

Department of Health & Human Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850



CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Enterprise Architecture and Strategy Group (EASG)

CMS Integrated Security Suite (CISS)

Release 8

User Guide

Version 7.08

June 18, 2007

Table of Contents

1.0	Introduction	1
1.1	Extended Scope/New Name	1
1.2	Interface Enhancements: The Treeview Interface	2
1.3	Navigating with the Keyboard	3
1.4	User Guide Screen Images	4
2.0	Getting Started	5
2.1	System Requirements	5
2.2	Selecting the Best Location for the CISS Database Files	5
2.2.1	Network Use	5
2.2.2	Local Use	6
2.3	Installation	6
2.3.1	Installing the CISS Application	6
2.3.2	Connecting to the Back-End Database	9
2.4	Managing Medicare Site Information	9
2.4.1	Managing Entity Information	9
2.4.2	Managing Self-Assessment Contract Information	11
2.5	Other Recommended Setup Activities	12
3.0	Interface Overview	13
3.1	Main Menu	15
3.1.1	Help	17
3.1.2	Check for Updates	18
3.1.3	Component Region	19
3.1.4	Application Control Region	19
3.1.5	Treeview Region	20
3.2	CISS Form Navigation Controls	25
3.3	CISS Form Modes	26
3.4	Accessing CISS Forms	28
3.4.1	Using Component Region Buttons to Access Forms	28
3.4.2	Using Treeview Region Nodes to Access Forms	29
3.5	CISS Form Drop-Down Menu Selections	30
3.6	CISS Form Required Fields	31
3.7	CISS “Busy” Message Displays	31
3.8	CISS Form Data Sensitivity	32
3.9	CISS Form Validation	33
3.10	CISS Form Spell-Check Button	34
3.11	Pivot Reports Button	34
3.11.1	Pivot Table Wizard	35
3.11.2	Pivot Table Report Fields	37
3.11.3	Pivot Report Example	39

CISS User Guide – Table of Contents

3.12	Adhoc (MS Access) Reports	41
3.12.1	Adhoc Report	42
4.0	Documentation	47
4.1	Opening the Supporting Documents Form	47
4.2	Adding New Supporting Documents	48
4.3	Add Available Documents	50
4.4	Remove Supporting Documents	51
4.5	Update Documents	53
4.5.1	Updating Supporting Documents	53
4.5.2	Updating Available Documents	56
4.6	Retire Documents	58
4.7	Documentation Errors	60
4.7.1	Correcting Missing Documentation Errors	60
4.8	Context Menus	62
5.0	Points-of-Contact (POCs)	65
5.1	Creating a New POC Record	65
5.2	Opening a POC Record	65
5.3	Editing a POC Record	66
5.4	Completing the POC Form	66
5.4.1	Last and First Name Fields	67
5.4.2	Email Field	67
5.4.3	Phone, Ext., and Fax Fields	67
5.4.4	Job Function Field	67
5.4.5	Notes Field	68
5.4.6	Finalizing the Form	68
5.5	POC Links or Associations	68
5.5.1	Adding Individual POC Links to Other Forms	69
5.5.2	Removing POC Links to Other Forms	71
5.6	Assigning a Primary POC	73
5.7	Deleting a POC Record	74
5.8	POC Reports	74
5.8.1	Print Current Point-of-Contact (MS Access)	75
5.8.2	Print All Points-of-Contact (MS Access)	76
5.8.3	Adhoc (MS Access)	77
6.0	Self-Assessments	78
6.1	Self-Assessments and Lower-Level CSR Nodes	78
6.2	Self-Assessment Form Navigation Controls	80
6.3	Unlocking Self-Assessment Records	81
6.3.1	Unlocking All Self-Assessment CSR Response Records	81
6.3.2	Unlocking Individual CSR Response Records	83
6.4	Creating a New Self-Assessment	83
6.5	Modifying Self-Assessment Information	84

CISS User Guide – Table of Contents

6.6	Opening Self-Assessments and CSRs	84
6.6.1	Opening a Self-Assessment	85
6.6.2	Opening a CSR Category or Response	85
6.7	Editing a Self-Assessment/CSR Record	85
6.8	New Self-Assessments/CSR Records	86
6.8.1	Creating a New Response Record	87
6.8.2	Entity Response Button	88
6.8.3	Baseline Self-Assessment	89
6.9	Completing the Self-Assessment/CSR Form	89
6.9.1	Self-Assessment Title and CSR Screen Areas	90
6.9.2	CSR Status and Response Areas	92
6.9.3	Finalizing the Form	98
6.10	Deleting a Self-Assessment or CSR Response Record	98
6.10.1	Deleting a Self-Assessment	98
6.10.2	Deleting a CSR Response Record	99
6.11	Self-Assessment/CSR Reports	100
6.11.1	Validate Current CSR	101
6.11.2	Validate Current Self-Assessment	102
6.11.3	Print Worksheet (Current CSR)	103
6.11.4	Print Worksheets (All CSRs)	104
6.11.5	Print Current CSR (MS Word)	104
6.11.6	Print All CSRs (MS Word)	105
6.11.7	Print Current CSR (MS Access)	105
6.11.8	Print All CSRs (MS Access)	106
6.11.9	Adhoc (MS Access)	106
7.0	Weaknesses	108
7.1	Creating a New Weakness Record	108
7.2	Opening a Weakness Record	109
7.3	Editing a Weakness Record	109
7.4	Completing the Weakness Form	110
7.4.1	Weakness Identifier	111
7.4.2	Weakness Title	112
7.4.3	Weakness Description	112
7.4.4	Weakness Category Selection	112
7.4.5	Action Plan Selection	112
7.4.6	Risk Selection	113
7.4.7	FISMA Severity Selection	113
7.4.8	Type Selection	113
7.4.9	Status Selection	114
7.4.10	Finalizing the Form	114
7.4.11	Validating Weaknesses	114
7.5	Weakness Links or Associations	115
7.5.1	Adding Weakness Links to Other Forms	116
7.5.2	Removing Weakness Links to Other Forms	117
7.6	Deleting a Weakness	120
7.7	Weakness Reports	120
7.7.1	Print Current Weakness (MS Access)	121
7.7.2	Print All Weaknesses (MS Access)	122
7.7.3	Adhoc (MS Access)	122

CISS User Guide – Table of Contents

7.7.4	Weakness POA&M (MS Access)	123
8.0	Action Plans	125
8.1	Creating a New Action Plan Record	125
8.2	Opening an Action Plan Record	125
8.3	Editing an Action Plan Record	126
8.4	Completing the Action Plan Form	127
8.4.1	Action Plan Title and Description Fields	128
8.4.2	Completion Dates and Target Implementation Costs Areas	128
8.4.3	Costs and Funding Sources Area Fields	128
8.4.4	Finalizing the Form	129
8.4.5	Validating Action Plans	129
8.5	Completing Milestones	129
8.5.1	Adding Milestones	130
8.5.2	Adding Projected Completion Dates	133
8.5.3	Adding Status Updates	136
8.5.4	Action Plan Completion Dates	138
8.6	Action Plan Links or Associations	139
8.6.1	Adding Action Plan Links to POCs	140
8.6.2	Removing Action Plan Links to POCs	141
8.7	Deleting an Action Plan Record	142
8.8	Action Plan Reports	143
8.8.1	Print Current Action Plan (MS Access)	144
8.8.2	Print All Action Plans (MS Access)	145
8.8.3	Adhoc (MS Access)	145
9.0	Systems	147
9.1	Risk Assessment and Contingency Planning Schedules	147
10.0	Audits	148
10.1	Creating a New Audit Record	148
10.2	Opening an Audit Record	148
10.3	Editing an Audit Record	148
10.4	Completing the Audits Form	149
10.4.1	Review/Audit Title Field	149
10.4.2	Performed By Field	149
10.4.3	Audit/Review Type Field	149
10.4.4	Review/Audit Date Field	150
10.4.5	Comments Field	150
10.4.6	Finalizing the Form	150
10.4.7	Validating Audits	150
10.5	Audit Links or Associations	151
10.6	Deleting an Audit Record	151
10.7	Audit Reports	152
10.7.1	Print Current Audit (MS Access)	152
10.7.2	Print All Audits (MS Access)	153
10.7.3	Adhoc (MS Access)	153

11.0	<i>Findings</i>	155
11.1	Creating a New Finding Record	155
11.2	Opening a Finding Record	155
11.3	Editing a Finding Record	156
11.4	Completing the Findings Form	157
11.4.1	Finding Identifier	158
11.4.2	Description Field	159
11.4.3	Weakness Link Selection	159
11.4.4	Audit Link Selection	159
11.4.5	Category Selection	159
11.4.6	Risk Selection	160
11.4.7	FMFIA (and CPIC) Severity Selection	160
11.4.8	Status Selection	161
11.4.9	Closed Pending and Closed Date Fields	161
11.4.10	Docs Buttons	161
11.4.11	Finalizing the Form	162
11.4.12	Validating Findings	162
11.5	Finding Links or Associations	163
11.5.1	Adding Finding Links to Other Forms	164
11.5.2	Removing Finding Links to Other Forms	164
11.6	Deleting a Finding Record	165
11.7	Finding Reports	166
11.7.1	Print Current Finding (MS Access)	167
11.7.2	Print All Findings (MS Access)	167
11.7.3	Adhoc (MS Access)	168
11.7.4	Finding POA&M (MS Access)	169
11.7.5	Universal CAP (MS Excel)	170
12.0	<i>Submissions to CMS</i>	171
12.1	POA&M Report	171
12.2	Self-Assessment Submission	172
12.2.1	Submission Date	173
12.2.2	Submission Validation	174
12.2.3	Submission File	175
12.3	POA&M Submission	176
12.3.1	Submission Date	177
12.3.2	Weakness Source Selection	178
12.3.3	Submission Validation	178
12.3.4	Submission File	179
13.0	<i>Database Administration</i>	181
13.1	Managing the Back-End Database	181
13.1.1	Back-end Database Connection Error	181
13.1.2	Changing the Back-end Database	181
13.1.3	Connecting to the Back-end Database	182
13.2	Database Administration Menu	188
13.2.1	Who's Logged On?	189
13.2.2	Compact/Repair Back-end	189
13.2.3	Backup Back-end	190
13.2.4	Encryption	190

CISS User Guide – Table of Contents

13.2.5	Missing Documents	197
13.2.6	Check for Updates	197
13.3	Updating the CISS Application	200
13.3.1	Installing a CISS Application Update	200
14.0	<i>CMS Administrative Functions (For CMS Use Only)</i>	204
14.1	Admin Tools	204
14.1.1	POA&M Admin Button	204
14.1.2	Output Docs to Folders Button	209
14.1.3	Import Data Button	215
14.1.4	Validate All POA&M Weaknesses Button	222
14.1.5	Pivot Reports Button	222
14.2	Validate Support Documents	222
14.3	Analysis Reports	224
14.4	Updating Imported Weaknesses	227
14.4.1	Assigning CMS Weakness Numbers	227
14.4.2	Updating CMS Projected Dates	228
14.5	Change CSR Version	228
14.5.1	Change CSRs	228
14.5.2	Non-Current CSR Version Warning	229

Table of Figures

Figure 1-1. CISS Treeview interface	2
Figure 2-1. Setup “Introduction” dialog	7
Figure 2-2. Setup “Copyright Information” dialog	7
Figure 2-3. Setup “Select the destination folder” dialog	8
Figure 2-4. Setup “Start copying files” dialog	8
Figure 2-5. Setup “Setup Complete” dialog	9
Figure 2-6. Treeview “Edit” Contractor node pop-up menu	10
Figure 2-7. Entity Information form	10
Figure 2-8. POC list error message	10
Figure 2-9. Treeview Self-Assessments (CAST) node	11
Figure 2-10. Treeview “Edit” Self-Assessments (CAST) node pop-up menu	11
Figure 2-11. Edit Self-Assessment dialog	11
Figure 3-1. CISS Files are missing! dialog message	13
Figure 3-2. CISS “WARNING” statement	14
Figure 3-3. CISS main menu	14
Figure 3-4. CISS main menu regions	16
Figure 3-5. CISS User Guide	17
Figure 3-6. CISS / CSR version information	18
Figure 3-7. Component Region Buttons	19
Figure 3-8. Application Control Region Buttons	19
Figure 3-9. Partially expanded Treeview region nodes	21
Figure 3-10. Major and Lower-Level Security Element Nodes	22
Figure 3-11. Example Treeview node pop-up menus	24
Figure 3-12. Treeview node pop-up menu summary	25
Figure 3-13. Record navigation buttons	25
Figure 3-14. Record navigation button use	26
Figure 3-15. CISS form READONLY mode	26
Figure 3-16. CISS form EDIT mode	26
Figure 3-17. CISS form ADD mode	26
Figure 3-18. CISS form modes	27
Figure 3-19. Component region buttons	28
Figure 3-20. Treeview node pop-up menus	29
Figure 3-21. Drop-down menu selection example	30
Figure 3-22. Example of required fields	31
Figure 3-23. Example of required fields notification message	31
Figure 3-24. Processing Request message	31
Figure 3-25. Example of sensitive form field	33
Figure 3-26. Sensitive information warning message	33
Figure 3-27. Highlighted example of “Validation” error message	34
Figure 3-28. Pivot Table Wizard form	35
Figure 3-29. Pivot Table Wizard form CSR Responses “Query Fields”	36
Figure 3-30. Pivot Table Wizard form Findings Data “Query Fields”	36
Figure 3-31. Pivot Table Wizard form Weakness Data “Query Fields”	37
Figure 3-32. Pivot Table Wizard form report area	38
Figure 3-33. Pivot Report example	38
Figure 3-34. Pivot Table Wizard form CSR Responses “Query Fields”	39
Figure 3-35. Example Pivot Report	40
Figure 3-36. Example Pivot Report field drop-down menu	40
Figure 3-37. Example Pivot Table revised report	41
Figure 3-38. Adhoc report type selection dialog	42
Figure 3-39. Adhoc Primary filter selection form	42
Figure 3-40. Adhoc report “Applicability” Primary and Secondary filters	43
Figure 3-41. Adhoc report “CSR” Primary and Secondary filters	43
Figure 3-42. Adhoc report “Reference” Primary and Secondary filters	44

CISS User Guide – Table of Contents

Figure 3-43. Adhoc report “Self-Assessment” Primary and Secondary filters	44
Figure 3-44. No records found message	45
Figure 3-45. Example CSR Adhoc report	45
Figure 3-46. MS Access® report Toolbar controls	46
Figure 4-1. Supporting Documents form	48
Figure 4-2. Supporting Documents dialog	49
Figure 4-3. Supporting Documents form displaying Supporting Documents	49
Figure 4-4. Supporting Documents form displaying Available Documents	50
Figure 4-5. Supporting Documents form displaying moved Available Documents	51
Figure 4-6. Supporting Documents form displaying Supporting Documents	52
Figure 4-7. Supporting Documents form displaying Supporting Documents	52
Figure 4-8. Supporting Documents form Update Document	53
Figure 4-9. Update Document dialog	54
Figure 4-10. Supporting Documents form displaying updated Supporting Documents	54
Figure 4-11. Supporting Documents form displaying updated document	55
Figure 4-12. Supporting Documents form displaying updated document	55
Figure 4-13. Supporting Documents form Update Document	56
Figure 4-14. Update Document dialog	57
Figure 4-15. Supporting Documents form displaying updated Supporting Documents	57
Figure 4-16. Supporting Documents form	59
Figure 4-17. Supporting Documents form displaying Retired Document	59
Figure 4-18. CISS Files are missing! dialog message	60
Figure 4-19. Database Administration dialog	60
Figure 4-20. Missing Documents dialog	61
Figure 4-21. Missing: [file name] Document dialog	61
Figure 4-22. Reinsert Missing File dialog	62
Figure 4-23. Missing Documents dialog	62
Figure 4-24. Supporting Documents form pop-up menu	63
Figure 4-25. Supporting Documents form pop-up menus	63
Figure 4-26. Supporting Documents form Open caution message	64
Figure 5-1. Points-of-Contact form EDIT mode	67
Figure 5-2. Points-of-Contact form READONLY mode	68
Figure 5-3. Assign Points-of-Contact dialog	69
Figure 5-4. Assign Responsibility dialog	70
Figure 5-5. Assign Points-of-Contact dialog with POC assignment	70
Figure 5-6. POC CSRs dialog window assignment	71
Figure 5-7. POC CSRs dialog window assignment	71
Figure 5-8. Assign Responsibility dialog	72
Figure 5-9. Delete Contact Assignment warning message	72
Figure 5-10. Action Plan form POCs dialog window assignment	73
Figure 5-11. Assign Points-of-Contact form	73
Figure 5-12. Assign Responsibility dialog without Primary assignment selected	74
Figure 5-13. Assign Responsibility dialog with Primary assignment selected	74
Figure 5-14. Delete Point of Contact warning message	74
Figure 5-15. Points-of-Contact Reports menu	75
Figure 5-16. Example Current POC report	76
Figure 5-17. Example All POCs report	76
Figure 5-18. Adhoc Points-of-Contact Reports dialog	77
Figure 6-1. Treeview Self-Assessment and CSR nodes	79
Figure 6-2. Self-Assessment form Self-Assessment Title drop-down menu	80
Figure 6-3. Goto CSR drop-down menu	80
Figure 6-4. Response Record and CSR Record navigation buttons	80
Figure 6-5. Locked Self-Assessment form record	81
Figure 6-6. Treeview Self-Assessment node “Unlock All Records” pop-up menu	82
Figure 6-7. Unlocked Self-Assessment form record	82
Figure 6-8. Treeview CSR node “Unlock Record” pop-up menu	83
Figure 6-9. Treeview Self-Assessments (CAST) node “Add” pop-up menu	83

CISS User Guide – Table of Contents

Figure 6-10. Add Self-Assessment form	84
Figure 6-11. Treeview Self-Assessments (CAST) lower-level nodes	84
Figure 6-12. New Self-Assessment form record	87
Figure 6-13. Self-Assessment form “Entity Response” button	88
Figure 6-14. Baseline Self-Assessment selection	88
Figure 6-15. Self-Assessment form EDIT mode	89
Figure 6-16. Self-Assessment form response status area	90
Figure 6-17. Self-Assessment form upper region	90
Figure 6-18. CSR Applicability dialog	91
Figure 6-19. CSR Protocols dialog	91
Figure 6-20. CSR Guidance and Related CSRs dialog	91
Figure 6-21. CSR References dialog	92
Figure 6-22. Self-Assessment form CSR response area in EDIT mode	92
Figure 6-23. Self-Assessment form CSR response area in READONLY mode	93
Figure 6-24. Self-Assessment Reports menu	95
Figure 6-25. Assign Points-of-Contact dialog	95
Figure 6-26. “Assignee” drop-down menu	96
Figure 6-27. Assign Weakness dialog	97
Figure 6-28. “Weakness” drop-down menu	97
Figure 6-29. Treeview “Delete” Self-Assessment node pop-up menu	98
Figure 6-30. Delete Self-Assessment form	98
Figure 6-31. Delete Self-Assessment warning message	99
Figure 6-32. Delete Record warning message	99
Figure 6-33. Self-Assessment Reports menu	100
Figure 6-34. Treeview Self-Assessment name node “Reports” pop-up menu	100
Figure 6-35. Treeview CSR control technique node “Reports” pop-up menu	101
Figure 6-36. MS Word® macro warning message	101
Figure 6-37. Treeview CSR number node “Validate” pop-up menu	102
Figure 6-38. CSR end of validation message	102
Figure 6-39. Example Word® single-CSR validation error report	102
Figure 6-40. Treeview Self-Assessment name node “Validate” pop-up menu	103
Figure 6-41. Treeview CSR number node “Create Worksheet” pop-up menu	103
Figure 6-42. Example Word® CSR Response worksheet	104
Figure 6-43. Treeview Self-Assessment name node “Create Worksheets” pop-up menu	104
Figure 6-44. Example MS Word® CSR report	105
Figure 6-45. Example MS Access® CSR report	106
Figure 6-46. Adhoc Self-Assessment Reports dialog	107
Figure 7-1. Weakness form locked fields	110
Figure 7-2. Weakness form EDIT mode	111
Figure 7-3. Weakness form “Category” selection	112
Figure 7-4. Weakness form “Action Plan” selection	112
Figure 7-5. Weakness form Risk “Likelihood” selection	113
Figure 7-6. Weakness form Risk “Impact” selection	113
Figure 7-7. Weakness form “FISMA Severity” selection	113
Figure 7-8. Weakness form “Type” selection	114
Figure 7-9. Weakness form “Status” selection	114
Figure 7-10. Treeview “Validate” all Weaknesses node pop-up menu	114
Figure 7-11. Weakness Validate confirmation message	115
Figure 7-12. Example Weakness validation error report	115
Figure 7-13. Weakness form READONLY mode	116
Figure 7-14. Assign Responsibility dialog	117
Figure 7-15. Weakness CSRs dialog window assignment	118
Figure 7-16. Findings form Weakness title field	119
Figure 7-17. Findings form Weakness title field	119
Figure 7-18. Delete Weakness warning message	120
Figure 7-19. Weakness Reports menu	120
Figure 7-20. Example Current Weakness report	121

CISS User Guide – Table of Contents

Figure 7-21. Example All Weaknesses report	122
Figure 7-22. Adhoc Weakness Reports dialog	123
Figure 7-23. Example Weakness POA&M report	124
Figure 8-1. Action Plan form locked fields	127
Figure 8-2. Action Plan form EDIT mode	128
Figure 8-3. Action Plan form “Costs” and “Funding Sources” area	129
Figure 8-4. Action Plan Validate confirmation message	129
Figure 8-5. Example Action Plan validation error report	129
Figure 8-6. Milestones disabled function message	130
Figure 8-7. Milestones root node before adding a Milestone	130
Figure 8-8. Action Plan disabled function message	130
Figure 8-9. Milestones node “Add Milestone” pop-up menu	130
Figure 8-10. Milestone node “Add Milestone” pop-up menu	131
Figure 8-11. Milestone sub-form method of adding Milestones	131
Figure 8-12. Action Plan form Milestone sub-form	132
Figure 8-13. Milestone node pop-up menu	133
Figure 8-14. Adding a subsequent Projected Completion Date	134
Figure 8-15. Action Plan form Projected Date sub-form	135
Figure 8-16. Preparing to add a subsequent Status Update	136
Figure 8-17. Action Plan form Status Update sub-form	137
Figure 8-18. Action Plan Completion Dates area	138
Figure 8-19. Status Update form Status field	139
Figure 8-20. Action Plan form READONLY mode	140
Figure 8-21. Assign Responsibility dialog	141
Figure 8-22. Assign Responsibility dialog	142
Figure 8-23. Delete Contact Assignment warning message	142
Figure 8-24. Delete Action Plan warning message	143
Figure 8-25. Action Plan Reports menu	143
Figure 8-26. Example Current Action Plan report	144
Figure 8-27. Example All Action Planes report	145
Figure 8-28. Adhoc Action Plan Reports dialog	146
Figure 10-1. Audits and Reviews form EDIT mode	149
Figure 10-2. Audit/Review Type drop-down selection menu	150
Figure 10-3. Audit Validate confirmation message	150
Figure 10-4. Example Audit validation error report	151
Figure 10-5. Audits and Reviews form Finding(s) dialog window	151
Figure 10-6. Delete Audit warning message	151
Figure 10-7. Audit Reports menu	152
Figure 10-8. Example Current Audit report	153
Figure 10-9. Example All Audits report	153
Figure 10-10. Adhoc Audit Reports dialog	154
Figure 11-1. Findings form locked fields	157
Figure 11-2. Findings form EDIT mode	158
Figure 11-3. Findings form “Weakness” selection	159
Figure 11-4. Findings form “Audit” selection	159
Figure 11-5. Findings form “Category” selection	160
Figure 11-6. Findings form Risk “Likelihood” selection	160
Figure 11-7. Findings form Risk “Impact” selection	160
Figure 11-8. Findings form “FMFIA (and CPIC) Severity” selection	161
Figure 11-9. Findings form “Status” selection	161
Figure 11-10. Findings form “Status” error message	161
Figure 11-11. Findings form “Docs” selections	162
Figure 11-12. Finding Validate confirmation message	162
Figure 11-13. Example Finding validation error report	163
Figure 11-14. Findings form READONLY mode	163
Figure 11-15. Assign Responsibility dialog	164
Figure 11-16. Assign Responsibility dialog	165

CISS User Guide – Table of Contents

Figure 11-17. Delete Contact Assignment warning message	165
Figure 11-18. Delete Finding warning message	166
Figure 11-19. Finding Reports menu	166
Figure 11-20. Example Current Finding report	167
Figure 11-21. Example All Findings report	168
Figure 11-22. Adhoc Finding Reports dialog	168
Figure 11-23. Example Finding POA&M report	169
Figure 11-24. Example Universal CAP report	170
Figure 12-1. Treeview Contractor node “POA&M Report” pop-up menu	172
Figure 12-2. Include old Weaknesses message	172
Figure 12-3. Example POA&M Report	172
Figure 12-4. Treeview Contractor node “Submit Self-Assessments” pop-up menu	173
Figure 12-5. Select Date dialog and submission confirmation message	173
Figure 12-6. Abnormal Date submission confirmation message	174
Figure 12-7. Self-Assessment validation error message	174
Figure 12-8. Example Self-Assessment validation error report	175
Figure 12-9. Save to dialog	175
Figure 12-10. Self-Assessment submission success message	176
Figure 12-11. Encrypt Submission File dialog	176
Figure 12-12. Treeview Contractor node “Submit POA&M” pop-up menu	177
Figure 12-13. Select Date dialog and submission confirmation message	177
Figure 12-14. Abnormal Date submission confirmation message	177
Figure 12-15. Include New Weaknesses form dialog	178
Figure 12-16. POA&M validation error message	178
Figure 12-17. Example POA&M error report	179
Figure 12-18. POA&M Save to dialog	179
Figure 12-19. POA&M submission success message	180
Figure 12-20. Encrypt Submission File dialog	180
Figure 13-1. Connection Error warning message	181
Figure 13-2. Connect to Back-end Database dialog	182
Figure 13-3. Back-end connection problem dialog	182
Figure 13-4. Connection Error warning message	182
Figure 13-5. First Data Link Properties dialog	183
Figure 13-6. Select Access Database dialog	183
Figure 13-7. Second Data Link Properties dialog	184
Figure 13-8. Testing the back-end file connection	184
Figure 13-9. Back-end database Version Error message dialog	185
Figure 13-10. Change back-end message	185
Figure 13-11. Exiting message	185
Figure 13-12. Default Save Back-end as dialog	186
Figure 13-13. Pre-existing file name message dialog	186
Figure 13-14. Company name Descriptive Information of New Database dialog	187
Figure 13-15. Company name Required Information dialog	187
Figure 13-16. Company abbreviation Descriptive Information of New Database dialog	187
Figure 13-17. Company name Required Information dialog	188
Figure 13-18. Cannot create back-end database dialog	188
Figure 13-19. Database Administration menu	188
Figure 13-20. Logged On Users dialog	189
Figure 13-21. Successful compaction message	189
Figure 13-22. Successful backup message	190
Figure 13-23. Encrypt a File dialog	191
Figure 13-24. Select the file to Encrypt dialog	191
Figure 13-25. Select a directory dialog	192
Figure 13-26. Encryption Input File/Output Path selections	192
Figure 13-27. Password Incorrect message	193
Figure 13-28. Password Strength Error message	193
Figure 13-29. Encrypt Now button	193

CISS User Guide – Table of Contents

Figure 13-30. Encryption Succeeded message	194
Figure 13-31. Compress Encrypted File dialog	194
Figure 13-32. Compression Succeeded message	194
Figure 13-33. Encrypt a File dialog	195
Figure 13-34. Decrypt a File dialog	195
Figure 13-35. Select the file to Decrypt dialog	195
Figure 13-36. Select a directory dialog	196
Figure 13-37. Decrypt Input File/Output Path selections	196
Figure 13-38. Password Incorrect message	197
Figure 13-39. Decryption Succeeded message	197
Figure 13-40. Checking for updates message	198
Figure 13-41. Version Update Info dialog message	198
Figure 13-42. Time to Update the CISS! dialog	198
Figure 13-43. File Download dialog	199
Figure 13-44. Save As dialog	199
Figure 13-45. WinZip® dialog	200
Figure 13-46. CISS / CSR version information	200
Figure 13-47. Update Warning dialog message	201
Figure 13-48. Setup “Introduction” dialog	201
Figure 13-49. Setup “Copyright Information” dialog	201
Figure 13-50. Setup “Start copying files” dialog	202
Figure 13-51. Setup “Setup Complete” dialog	202
Figure 13-52. Back-end database Version Error dialog message	202
Figure 13-53. Updating backend database message	203
Figure 14-1. CMS-only Component region buttons	204
Figure 14-2. Admin Tools menu	204
Figure 14-3. Entity Information dialog	205
Figure 14-4. Entity Information dialog “Select Data” drop-down menu	205
Figure 14-5. Entity Information dialog “System” drop-down menu	205
Figure 14-6. Entity Information “Weaknesses w/ System Family Assignment” dialog window	206
Figure 14-7. Please enter the Year dialog	206
Figure 14-8. Please enter the Quarter dialog	206
Figure 14-9. Browse for Folder dialog	207
Figure 14-10. Include old Weaknesses dialog	207
Figure 14-11. Entity Information “Findings” dialog window	208
Figure 14-12. Entity Information dialog “Weaknesses w/o System Family” selection	209
Figure 14-13. Select Entities for Adhoc Reporting dialog	210
Figure 14-14. Adhoc Admin Tools dialog	210
Figure 14-15. Finding Document Export Filters selection form	211
Figure 14-16. No records found message	211
Figure 14-17. Browse for Folder dialog	212
Figure 14-18. View Exported Supporting Document dialog	212
Figure 14-19. View Exported Supporting Document dialog	213
Figure 14-20. Self-Assessment Response Document Export Filters selection form	213
Figure 14-21. No records found message	214
Figure 14-22. Browse for Folder dialog	214
Figure 14-23. View Exported Supporting Document dialog	214
Figure 14-24. View Exported Supporting Document dialog	215
Figure 14-25. Import Data File dialog	215
Figure 14-26. “Import Type” drop-down menu	216
Figure 14-27. “Import Type” Self-Assessment selection	216
Figure 14-28. Self-Assessment Open file dialog	216
Figure 14-29. No File Selected message	217
Figure 14-30. Hot Fix error message	217
Figure 14-31. Validation success message	217
Figure 14-32. Self-Assessment validation table structure error message	217
Figure 14-33. Self-Assessment validation process field error message	218

CISS User Guide – Table of Contents

Figure 14-34. Self-Assessment Open file dialog	218
Figure 14-35. No File Selected message	218
Figure 14-36. Self-Assessment Import Process complete message	219
Figure 14-37. “Import Type” POA&M selection	219
Figure 14-38. POA&M Open file dialog	219
Figure 14-39. No File Selected message	220
Figure 14-40. Validation success message	220
Figure 14-41. POA&M validation table structure error message	220
Figure 14-42. POA&M validation process field error message	220
Figure 14-43. POA&M Open file dialog	221
Figure 14-44. No File Selected message	221
Figure 14-45. POA&M Import Process complete message	222
Figure 14-46. Weakness Validate confirmation message	222
Figure 14-47. Example Weakness validation error report	222
Figure 14-48. Database Administration dialog	223
Figure 14-49. Missing Documents dialog	223
Figure 14-50. Select Entities for Adhoc Reporting dialog	224
Figure 14-51. Adhoc CISS dialog	225
Figure 14-52. Average CSR Statistical Report Filters selection form	225
Figure 14-53. Average CSR Statistical Report Filters Secondary filters	226
Figure 14-54. Imported Weakness form	227
Figure 14-55. Database Administration menu	228
Figure 14-56. Swap CSRs dialog	228
Figure 14-57. Swap CSRs dialog version drop-down menu	228
Figure 14-58. Swap CSRs dialog CSR version display	229
Figure 14-59. Non-current CSRs Loaded warning message	229
Figure 14-60. CSRs Reset message	229

1.0 Introduction

The Centers for Medicare and Medicaid Services (CMS) has implemented an ongoing security initiative to address the systems security requirements mandated for Medicare data by a number of federal and CMS documents¹. Requirement statements have been collected from these documents and consolidated into a set of “CMS Core Security Requirements (CSRs).” Microsoft (MS) Access[®] has been used to condense and consolidate these requirement statements into an automated database that sorts captured requirement statements into Categories², General Requirements, and Control Techniques. Protocols describe suggested self-assessment procedures designed to verify that Business Partners comply with system security requirements.

1.1 Extended Scope/New Name

The application known as the Contractor Assessment Security Tool (CAST) has been used by CMS since 2001 to conduct annual self-assessments, the results of which are submitted and reviewed annually by CMS as part of its overall security improvement and compliance efforts.

New capabilities have been added to the CAST to address the evolving needs at CMS and its Business Partners. These changes address Business Partner requests for additional self-assessment functionality (resulting in an improved CAST component), while also meeting CMS requirements to track ongoing security issues and status information in response to federal law (resulting in the addition of an entirely new security oversight component), which includes:

- Plan of Action and Milestones (POA&M) and reporting
- Risk assessments and System Security Plans (SSPs) (future enhancement)
- System components and inventory (future enhancement)
- Audit/review of corrective actions
- Certification, accreditation, and testing (future enhancement).

The CMS Integrated Security Suite (CISS) (pronounced “kiss”) consists of the enhanced CAST module and additional security oversight functionality targeted at remediation improvement. The CAST module facilitates management of self-assessment compliance by ensuring consistency between actual security efforts and reported weaknesses and remediations. The remediation improvement component provides for tracking and reporting of security information derived from “Section 912”³ evaluations, Data Center reviews, Statement on Auditing Standards (SAS) No. 70, and Chief Financial Officer (CFO) audits. It also provides Business Partner support in meeting the federal requirements imposed by the Federal Information Security Management Act (FISMA).

¹ Federal and CMS mandates are listed in the *CMS/Business Partners Systems Security Manual (BPSSM)*.

² The six general and three application control categories in the *Federal Information System Controls Audit Manual (FISCAM)* were used as the initial categories for grouping the CSRs. One new category (“Networks”) was added based on information contained in Presidential Decision Directive (PDD) 63, and the Health Information Portability and Accountability Act (HIPAA).

³ The Medicare Prescription Drug, Improvement, and Modernization Act of 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors

Using the CISS, CMS and its Business Partners can:

- Develop, maintain, and issue uniform, enterprise-wide systems security policy
- Perform self-assessments in preparation for audits by specific federal and CMS organizations using standardized methods of data entry and reporting
- Develop, maintain, and evaluate a central repository for current and historical systems security program data
- Perform automated data entry of current systems security program data
- Perform automated reporting of current and historical systems security program data
- Perform concurrent data-entry or viewing by more than one qualified security representative
- Track the status of open issues.

1.2 Interface Enhancements: The Treeview Interface

The CISS enhancements also include significant changes to the user interface. A “Treeview” interface (Figure 1-1) has been incorporated as a visual, easy-to-use navigation tool for all the information contained within the CISS application. Treeviews are familiar to users of Microsoft products (such as MS Outlook® and MS Windows® Explorer).

Figure 1-1. CISS Treeview interface



Used extensively throughout the CISS application, the Treeview is useful for illustrating data interrelationships and navigating through data information structures and relationships. In the CISS application, the Treeview interface enables users to establish, track, and manage relationships among:

- Systems
- Audits
- Weaknesses
- Findings
- Self-Assessments (CAST)
- Responsible Persons/Owners
- POA&M
- C&A.

Clicking (specifically, double-clicking and right-clicking) on “nodes” in the Treeview provides a variety of functionality within the CISS, including:

- Pop-up menus
- Direct access to detail forms (Self-Assessments, Action Plans, Weaknesses, Systems, Findings, Points of Contact)
- Direct access to forms for manipulating data within the Treeview.

The Treeview interface and its functionality are explained in Chapter 3.0 as well as in applicable sections in the User Guide.

1.3 Navigating with the Keyboard

The CISS application uses the “Treeview” interface (Figure 1-1) to display data information structures and relationships as well as custom forms to display its database information. Users can use the following keyboard keys to navigate within the CISS interface and forms:

- Areas on CISS forms are separated using contrasting colors. The **Tab** key is used to navigate from one field or area to the next from left-to-right, then from top-to-bottom.
- The right/left arrow keys (→, ←) are used in the Treeview to expand/contract the active node. The up/down arrow keys (↑, ↓) are used to move up and down the Treeview.
- The arrow keys (←, ↑, →, ↓) are also used to navigate within a single color-coded area. Use these arrow keys to select/deselect radio buttons where only one radio button can be selected at any given time.
- The **Enter** or **Spacebar** keys activate (i.e., “click”) the currently selected (i.e., highlighted) form button, when applicable.
- The **Spacebar** also toggles between selecting and deselecting the active checkbox, when applicable.
- When nothing is selected or active on a form (i.e., making the form controls inaccessible to keyboard manipulation), the **Ctrl+Tab** key combination (i.e., keeping the **Ctrl** key depressed while depressing the **Tab** key) makes the form active again so that the keyboard can be used. This is the same as clicking a neutral area of the form with the mouse.
- The **Alt+↓** key combination (i.e., keeping the **Alt** key depressed while depressing the ↓ key) opens the selected drop-down menu, when applicable.
- The **Esc** key closes an open drop-down menu, when applicable.
- The **F1** key displays User Guide context help for the active form or field (refer to section 3.1.1).
- The **Enter** key selects the highlighted entry in a drop-down menu, when applicable.

WARNING: Pressing the **Esc** key while entering information into any CISS form deletes all the information entered since the form was opened and returns the form to its previous state. Use care not to press the **Esc** key unless closing an open drop-down menu or deliberately canceling all changes to an open form.

1.4 User Guide Screen Images

The User Guide was created using screen images from different CISS releases and MS Windows® versions. There may be some minor differences among the User Guide screen images and actual CISS screen displays. However, none of these differences affect the instructions provided in the User Guide. The User Guide will be updated to reflect up-to-date screen images, as necessary.

2.0 Getting Started

The CISS database is divided into several database files. The *front-end* database file (CISS.mde) contains the static code and interface components (forms, reports, etc.). The *back-end* database file (CISS_BE.mdb) contains the data that is unique to your individual organization (self-assessment data and Business Partner information). The tool suite places the CSRs and other relevant data into the back-end database. Other database files may be included to provide a historical reference to past CSR versions and support data for specific functionalities.

Note: The back-end database file name (CISS_BE.mdb) used as an example in the User Guide is the default file name when creating a new back-end database. Your back-end database may have a different file name.

2.1 System Requirements

The following are minimum suggested system requirements for the use of the CISS:

- Personal computer with Pentium 166-megahertz (MHz) or higher
- VGA or higher resolution monitor—preferably Super VGA
- 128 megabytes (MB) of RAM or above
- MS Windows[®] NT 4.0 with Service Pack 6 (SP6), 2000, XP, or later
- MS Access[®] 2000 or later
- MS Office[®] 2000 Professional
- Adobe Reader[®], Version 4 or later.

NOTE: The CISS is designed to function with MS Access[®] 2000 but will function with later versions (i.e., MS Access[®] 2003). However, the CISS will not function with earlier versions of MS Access[®].

2.2 Selecting the Best Location for the CISS Database Files

The CISS provides for local installation of the main tool components with either local or remote storage of the back-end data. The optimal location for the CISS back-end data varies with each organization's computer system design and CISS user requirements.

The front-end database and its associated files should be located locally on each applicable local workstation. The front-end database installation requires about 16 MB of local disk space and contains the data that remains static between CSR and CISS application updates.

2.2.1 Network Use

Storing the back-end database (CISS_BE.mdb) on a network allows for the most versatile use of the self-assessment data. Keep in mind that maintaining the data on a network drive provides both advantages and disadvantages.

Advantages:

- Multiple users can access CISS data concurrently; the system can accommodate up to 255 concurrent users.
- Sharing of back-end data on a network drive allows others to see "live" changes to the database in real-time (e.g., within 60 seconds).
- Locating back-end data files on a network server typically provides for a more frequent and scheduled backup of CISS back-end data.

Disadvantages:

- Connection to any MS Access[®] database via a network can slow database performance. The more users logged onto the database, the slower the database response time.
- Network access to the data may expose your security data to unauthorized access. It is recommended that network access to the self-assessment security data directory be restricted to only those authorized to view or modify the data.
- Network connection interruptions can result in corrupted MS Access[®] databases. Although the damage is often recoverable, the possibility of such corruption means that the database requires much more frequent and timely maintenance.

2.2.2 Local Use

Storing the back-end database (CISS_BE.mdb) on a local drive has its own advantages and disadvantages.

Advantages:

- Provides for quicker response time due to the absence of network traffic constraints.
- Reduces susceptibility to corruption due to network interruptions.
- May provide better protection from unauthorized access depending on local system settings.

Disadvantages:

- Restricts use to those with access to the local workstation/drive.
- Loss of local system may result in loss of both access to data and the data itself. Local drives are less likely to be backed up on a regular basis, resulting in the need to take measures to ensure that the database is properly backed up.

2.3 Installation

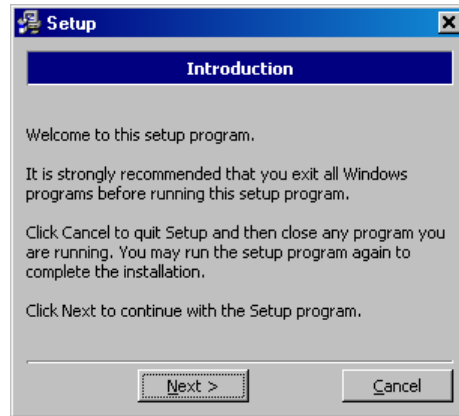
This section explains how to install the CISS application.

2.3.1 Installing the CISS Application

To install the CISS application for the first time:

- a. Double-clicking the CISS installation file (CISS_Vxxx.exe), where “xxx” is the version number, displays the following **Setup** “Introduction” dialog.

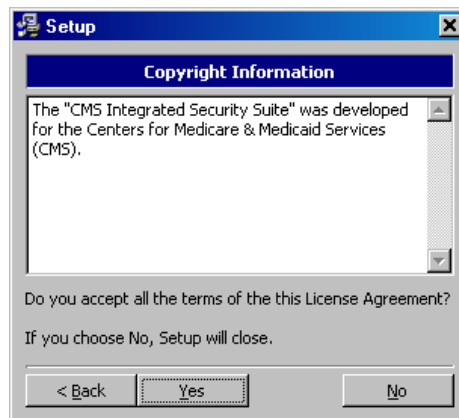
Figure 2-1. Setup “Introduction” dialog



NOTE: Since the purpose of these instructions is to install the CISS application, only the installation steps are explained. Canceling the installation process is self-explanatory.

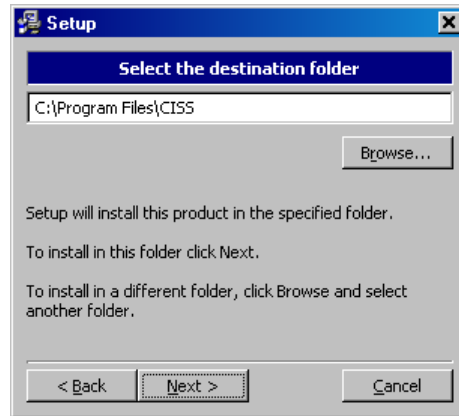
- b. Selecting terminates the installation process after displaying a confirmation dialog. Selecting continues the installation process and displays the following **Setup** “Copyright Information” dialog.

Figure 2-2. Setup “Copyright Information” dialog



- c. Selecting terminates the installation process, while selecting displays the following **Setup** “Select the destination folder” dialog which suggests the default installation folder.

Figure 2-3. Setup “Select the destination folder” dialog

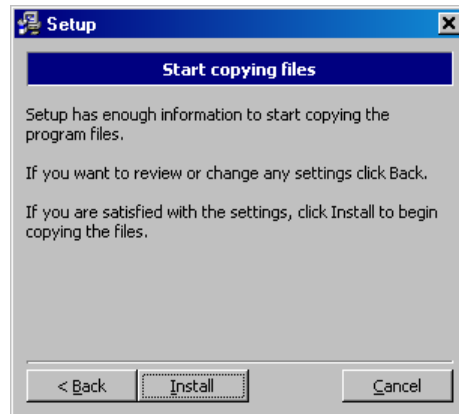


It is recommended (but not required) that the CISS be installed in the default installation folder. Selecting allows the user to specify a different folder.

WARNING: On some systems the user may not have sufficient privileges to install software. In such a case the default directory may be set to a system directory such as WinNT\System\CISS\. If this occurs, STOP immediately, and have your administrator install the CISS on your PC.

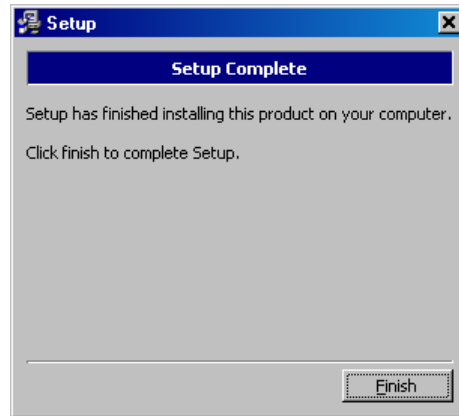
- d. Selecting displays the following **Setup** “Start copying files” dialog.

Figure 2-4. Setup “Start copying files” dialog



- e. Selecting starts the installation process, after which the following **Setup** “Setup Complete” dialog displays.

Figure 2-5. Setup “Setup Complete” dialog



- f. Selecting completes the installation process and closes the application. As part of the installation process, a “CMS Integrated Tool Suite” icon was placed on the Windows® desktop. Continue with the next section, 2.3.2, to link to the back-end database.

2.3.2 Connecting to the Back-End Database

The front-end (i.e., application data) and back-end (i.e., Business Partner data) database files must be linked to work properly. These links must be established the first time the CISS application is run, and whenever the back-end file name or location is changed or a new back-end database is created. Refer to section 13.1 for instructions on connecting to the back-end database.

2.4 Managing Medicare Site Information

The sections that follow describe the mechanics of using the CISS to manage Medicare entity information and manage contract information (i.e., number, type, name, description) for existing self-assessments.

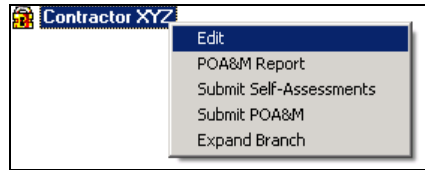
2.4.1 Managing Entity Information

The contractor name, abbreviation, and other organization-specific information are used throughout the CISS application. This information should be entered when initially setting up the CISS.

To assist in completing the following steps, refer to Figure 3-3 for an image of the CISS main menu when the application is first opened and no buttons have been selected or clicked. The contractor name shown in the Treeview top level node, or root node (i.e., “Contractor XYZ”), is the same name entered in section 13.1.3.3).

- a. To change the contractor name or input other contractor entity information, right-click the contractor name top-level, or root node (i.e., “Contractor XYZ”), to display the following pop-up menu.

Figure 2-6. Treeview “Edit” Contractor node pop-up menu



- b. Selecting “Edit” opens the following **Entity Information** form.

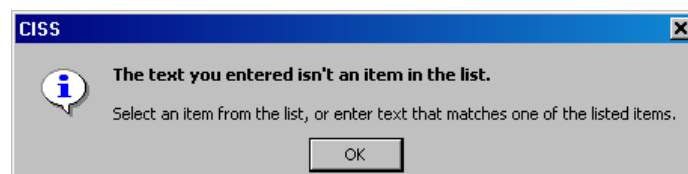
Figure 2-7. Entity Information form

- c. Note the **▶*** button at the end of the “VP Medicare” and “SSO” fields. The Points-of-Contact (POCs) for these two fields must be selected from a drop-down menu, as indicated by the **▼** drop-down menu button. Since both of these drop-down menus list only POCs that already exist in the database, new POCs cannot be input using the **▼** selection in these fields. If there are no POCs in the database (such as when using the CISS for the first time or when the desired POC is not already in the database), selecting **▶*** at the end of either field opens the **Points-of-Contact** form (Figure 5-1) so a new POC can be added to the database (refer to section 5.1).

NOTE: The **▶*** button can be selected to add new POCs. All POCs are contained in a common database and are not specific to either field or title.

- d. After the new POC(s) have been created or if the desired POC(s) already exists in the database, a POC can then be selected from the appropriate field drop-down menu. If any new information is entered into the VP Medicare or SSO fields instead of selecting a POC from the drop-down menu, the following error message displays when leaving the form.

Figure 2-8. POC list error message



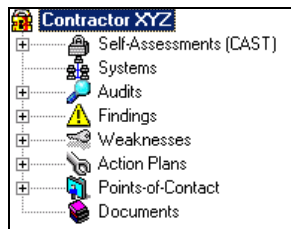
- e. To close the above error message, delete all information in the applicable field, leaving it blank, or select a POC from the drop-down menu before selecting **OK** to continue.
- f. Selecting **Save and Close** saves the information, while **Close w/o Saving** exits without saving the data. Either button returns the user to the CISS main menu.

2.4.2 Managing Self-Assessment Contract Information

To assist in completing the following steps, refer to Figure 3-3 for an image of the CISS main menu when the application is first opened and no buttons have been selected or clicked. The contractor name shown in the Treeview top level node, or root node (i.e., “Contractor XYZ”), is the same name entered in section 13.1.3.3).

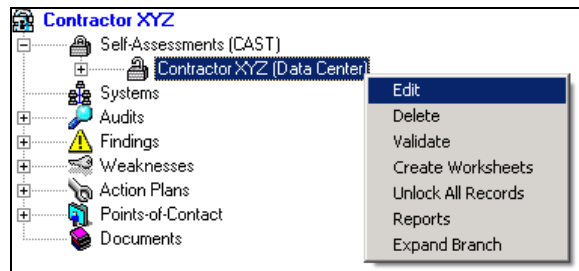
- a. Double-click the contractor name root node (i.e., “Contractor XYZ”) to expand the node and display its lower-level security oversight element nodes [i.e., Self-Assessments (CAST), Systems, Audits, Findings, Weaknesses, Action Plans, Points-of-Contact, Documents].

Figure 2-9. Treeview Self-Assessments (CAST) node



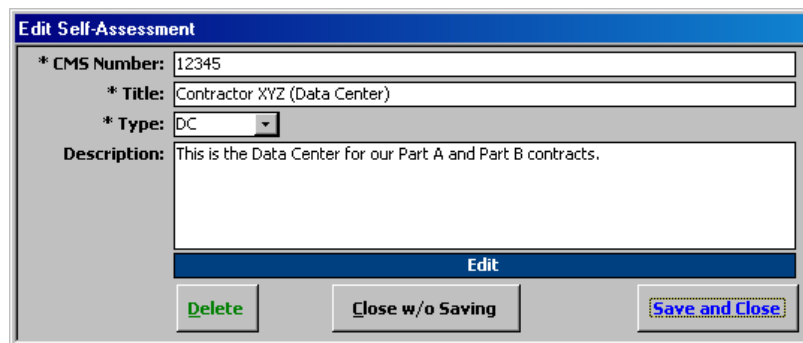
- b. Double-click the “Self-Assessments (CAST)” node or select its corresponding icon to expand the “Self-Assessments (CAST)” node and display the Self-Assessment names that exist in the back-end database. To edit a Self-Assessment name or other contract-related information in an existing Self-Assessment, selecting the desired Self-Assessment name node [i.e., “Contractor XYZ (Data Center)”] and right-clicking the Self-Assessment name node opens the following pop-up menu.


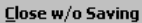
Figure 2-10. Treeview “Edit” Self-Assessments (CAST) node pop-up menu



- c. Selecting “Edit” from the pop-up menu opens the following **Edit Self-Assessment** dialog.

Figure 2-11. Edit Self-Assessment dialog



- d. After the Self-Assessment contract information has been updated, selecting  saves the information and closes the dialog. Selecting  exits the dialog and returns to the CISS main menu without saving the changes.

2.5 Other Recommended Setup Activities

The relational nature of the CISS application means that all security-related data are entered once and then linked together hierarchically. For example, Self-Assessments contain CSR responses, which contain links to one or more responsible parties known as POCs. Non-compliant CSR responses (i.e., response status other than “Level 3,” “Level 4,” “Level 5,” or “N/A”) link to Weaknesses, that link to Action Plans, and each of these link to responsible POCs.

Because POCs are such an integral (and required) part of the various security oversight elements tracked in the CISS, users are encouraged to refer to Chapter 5.0, and add their POC data to the database before entering other data. Then, the POCs are available for assignment when necessary. Otherwise, if a POC does not already exist in the database, the user must close the CISS element form to create the POC and re-enter the original element form before the POC can be assigned (or linked) to the security element.

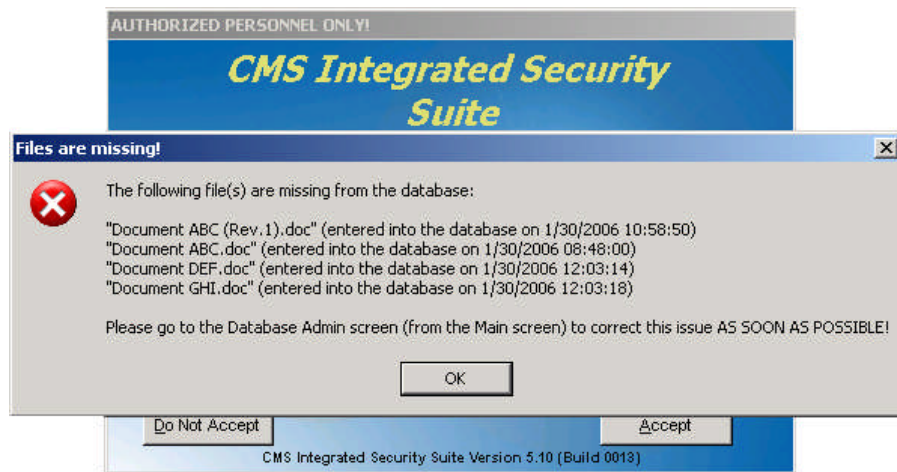
NOTE: The only CISS element form that allows POCs to be created and assigned within an entry form is the **Entity Information** form (Figure 2-7). All other element forms (except the POC form) require that POCs be selected from a drop-down menu and only pre-existing POCs appear on the drop-down menu.

3.0 Interface Overview

The CISS interface makes use of a Treeview interface, command buttons, drop-down menus, pop-up menus, and other conventional MS Windows® controls and behaviors. To open the CISS application, double-click the “CMS Integrated Security Suite” desktop icon that was created during installation (refer to section 2.3.1).

Upon opening, the CISS may display the following **Files are missing!** dialog message over the CISS “WARNING” statement. This dialog message displays whenever the CISS has determined that CAST or POA&M supporting documentation previously attach to the CISS (refer to Chapter 4.0) are missing or changed. Since this is a critical error, the CISS will continue to display this error message multiple times while accessing various program options. To correct this critical documentation error and stop this message from displaying, refer to section 4.7.

Figure 3-1. CISS Files are missing! dialog message



Otherwise, the CISS displays only the CISS “WARNING” statement dialog (Figure 3-2) indicating that the information contained in the database is sensitive and access to the information should be restricted to authorized personnel only. Information concerning the security readiness of the applicable systems should be treated as sensitive (possibly as company proprietary as well).

NOTE: If a CONNECTION ERROR message displays over the “WARNING” statement (such as when opening the CISS for the first time), refer to section 2.3.2 before proceeding.

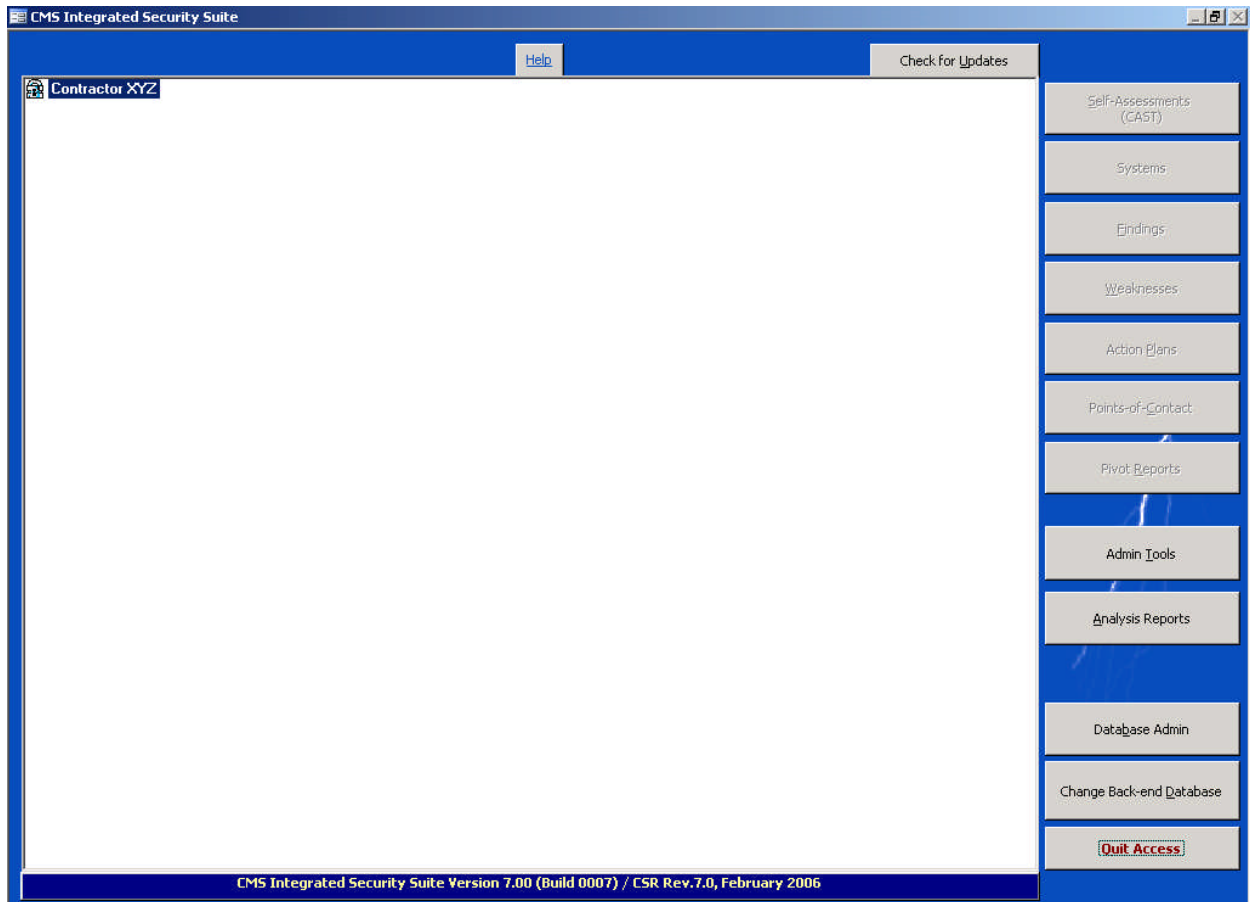
To proceed, the user must “Accept” the terms presented in the WARNING statement by selecting . Selecting closes the application.


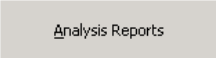
Figure 3-2. CISS “WARNING” statement



After acceptance, the CISS application opens to the following main menu.

Figure 3-3. CISS main menu



NOTE: The  and  buttons displayed on the main menu in Figure 3-3 and Figure 3-4 appear only on the CMS version of the CISS application. These buttons are used by CMS to import Business Partner Self-Assessment and POA&M submissions, and process the data in their master back-end database. Only the main menu features available in the contractor version of the CISS application are displayed and discussed in the remainder of the User Guide sections. The CMS-only button features are explained in Chapter 14.0.

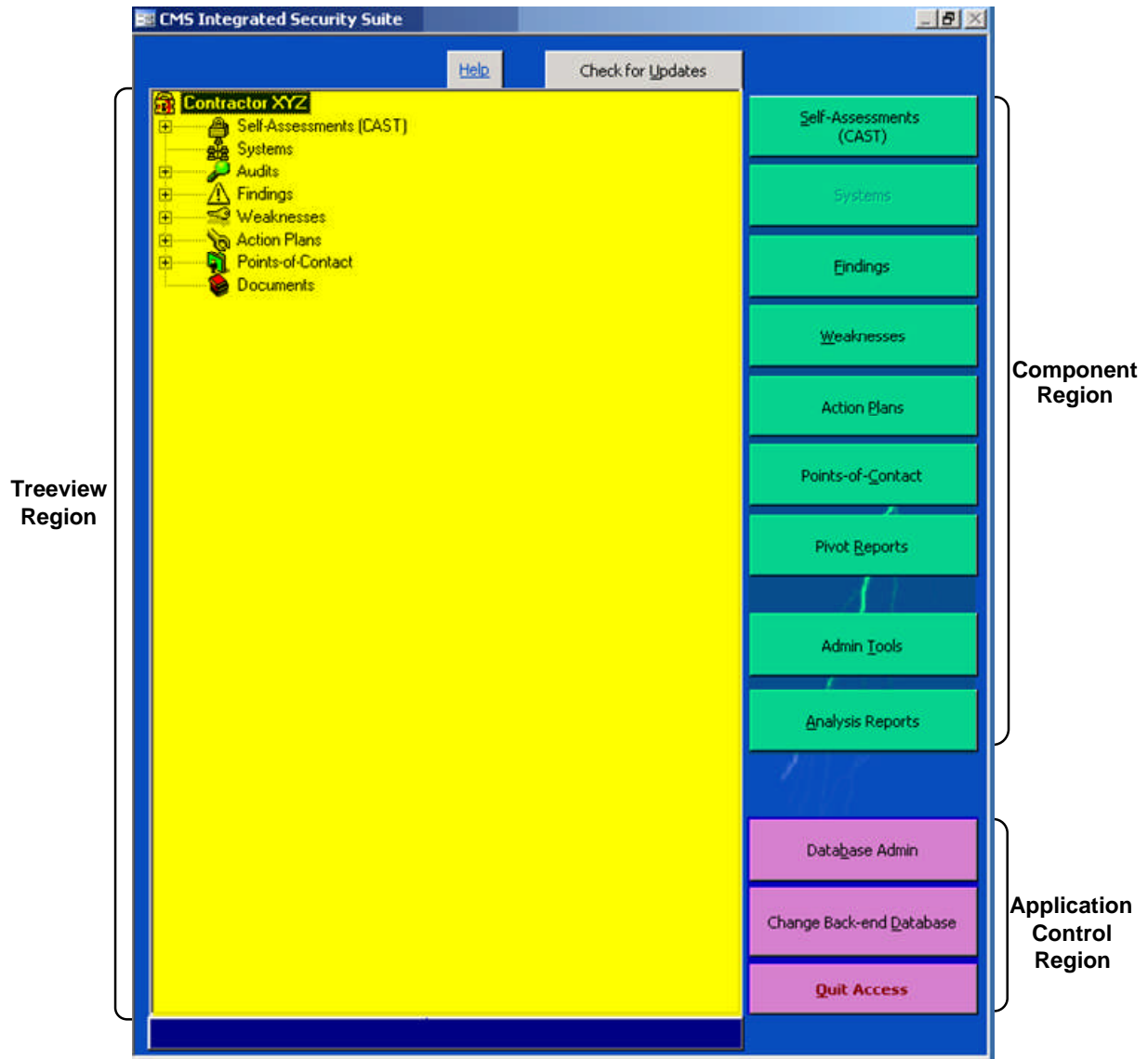
When the main menu initially opens, it displays a single root-level node representing the organization's name (i.e., "Contractor XYZ"). This root-level node is named when the database is initially configured (refer to section 13.1.3.3) but can be changed at any time (refer to section 2.4.1).

In addition, the security oversight element buttons on the right side of the main menu [i.e., Self-Assessments (CAST), Systems, Findings, Weaknesses, Action Plans, and Points-of-Contact] are not activated (i.e., not selectable) when the main menu initially opens. Double-clicking the Treeview root-level node (i.e., Contractor XYZ) expands the root-level node (refer to section 3.1.5 for an explanation of the Treeview region) and activates the security oversight element buttons (Figure 3-4).

3.1 Main Menu

For User Guide discussion purposes, consider the CISS main menu as having three regions (refer to Figure 3-4). This is only done to assist in distinguishing and explaining the differences between Treeview and button selection options.

Figure 3-4. CISS main menu regions



The Component region buttons are disabled when the CISS main menu initially opens but its buttons are enabled after the Treeview root-level node is expanded to display its major upper-level node contents. To expand the Treeview root-level node and activate the Component region buttons, double-click the root-level node name (i.e., Contractor XYZ).

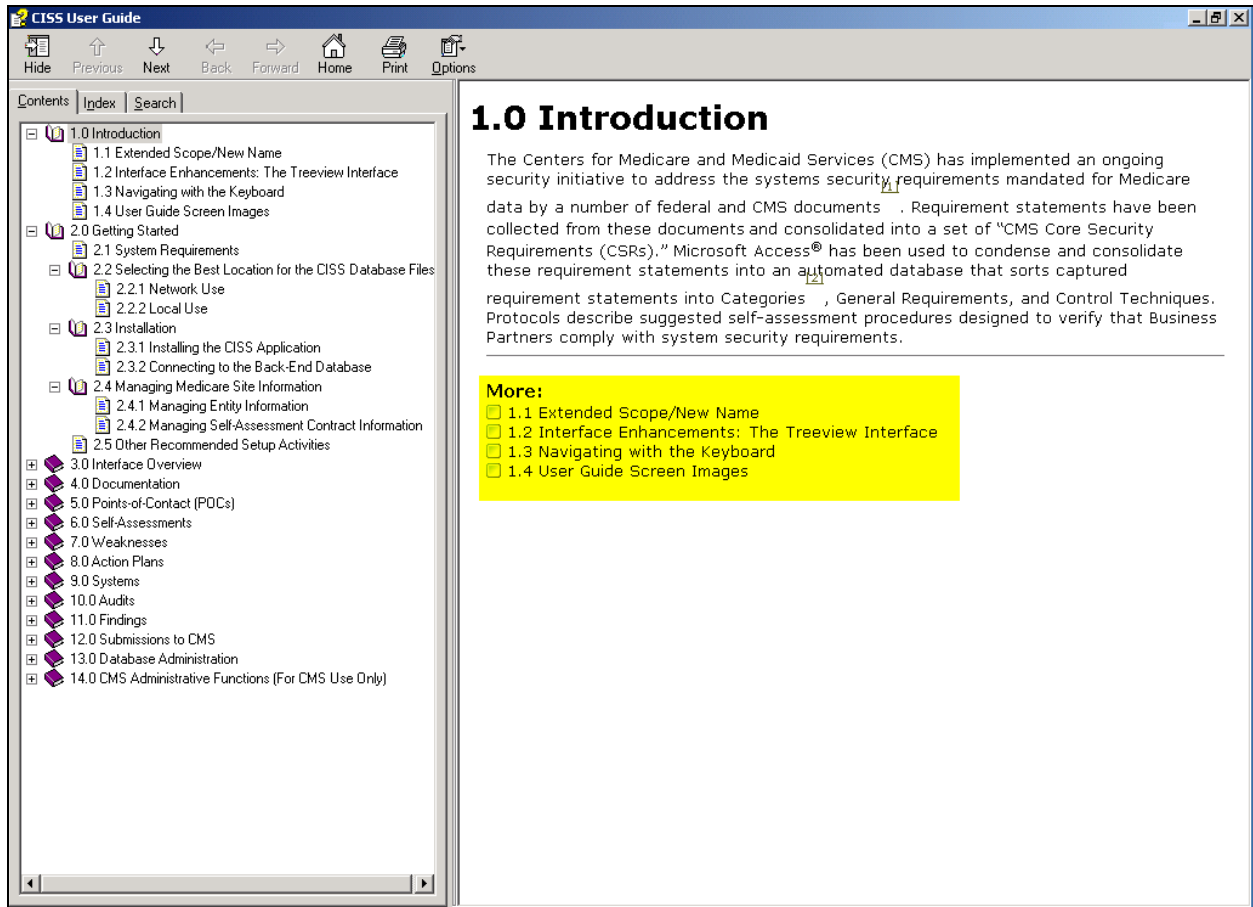
Each of the Component region buttons and Treeview major upper-level nodes in Figure 3-4 represent a different security oversight element (refer to section 3.1.5 for an explanation of the Treeview region). The Treeview region nodes and Component region buttons provide access to the same information contained in the back-end database. The information is simply accessed differently. The different CISS application components are explained in more detail in their applicable User Guide chapters.

It is important to note that all information relating to the same record entry (e.g., POC, System, Weakness, Audit) only has to be entered once. Form updates are automatically reflected in the corresponding record and all related or linked forms so multiple changes are not required.

3.1.1 Help



Located above the center portion of the main menu Treeview region (Figure 3-3) is a [Help](#) button. The [Help](#) button opens this html-based CISS User Guide which is included as part of the CISS application installation file. Selecting [Help](#) opens the following **CISS User Guide** dialog window for viewing or printing.

Figure 3-5. CISS User Guide



The User Guide includes tabs for Contents, Index (not functional in this release), and Search. The “Contents” tab lists the User Guide table of contents and it functions like the CISS Treeview regions (refer to section 3.1.5). The “Search” tab allows searches through the entire User Guide.

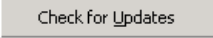
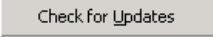
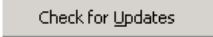
The “More” yellow highlighted area depicted in the above dialog window figure lists any lower-level sections or sections (if applicable) for the active “Contents” tab selection. Selecting any hypertext section number or heading text in the “More” area “jumps” to the selected link. To return to the previous section or section Treeview selection, use the [Back](#) button. To “jump” forward to the “More” hypertext link again, use the [Forward](#) button. Selecting these two buttons multiple times steps forward or back through all the hypertext section links previously selected.

Using the **Page Down** and **Page Up** keys does not scroll continuously from section to section. These keys only scroll through the active section or section. To scroll continuously from one section to the next, either forward or backward, use the **CISS User Guide** dialog window and  and  buttons.

The User Guide also includes interactive hypertext links to figures, chapters, and sections wherever they are referenced in User Guide chapters or section topics. Some of the hypertext links may not be functional in the current User Guide due to a bug in the help authoring application which is not part of the CISS. When/if this bug is fixed, the nonfunctional links will be corrected in a future CISS/User Guide release.

Using a html-based help system provides the capability to link topics within the User Guide to CISS forms, fields, and dialogs. Selecting the **F1** key while a dialog or entry form is active displays generic User Guide help for the active dialog or form. When the cursor is active in a form field or area, selecting the **F1** key displays User Guide help specific to the selected field or area. Using the **Tab** key to move the cursor focus to a form or dialog button displays User Guide help for the active button, if applicable.

3.1.2 Check for Updates

If the CISS is installed on a computer that has access to the Internet, the CISS can check for newer releases. Located above the right portion of the main menu Treeview region (Figure 3-3) is a  button. The CISS can be configured to automatically check for newer releases each time it is opened or the  button can be selected to manually check for updates. Refer to section 13.2.6 for this CISS configuration setting. However, for the  button to function, either automatically or manually as described here, the computer must have Internet access.

If the CISS is installed on a computer that does *not* have access to the Internet, the user is required to use a computer that has Internet access to check for, and download, the latest CISS release. The *CISS Info* web page (<http://cisstool.com/Info.aspx>) which is located at the *CISS Tool Support* web site (<http://cisstool.com/default.aspx>) maintains the latest release of the CISS tool. To update the CISS application, refer to section 13.3.

To determine which CISS version/build number and CSR version is currently installed, check the version information located in the lower area of the main menu below the Treeview region (Figure 3-6).

Figure 3-6. CISS / CSR version information



3.1.3 Component Region

The following CISS security oversight elements can be accessed using their respective buttons in the Component region of the main menu:

Figure 3-7. Component Region Buttons

Button	Function
Self-Assessments (CAST)	Invokes the Self-Assessment form (refer to Figure 6-7). Provides access to all the Self-Assessments in the back-end database.
Systems	When implemented, invokes the Systems form. Provides access to all the Systems in the back-end database.
Findings	Invokes the Findings form (refer to Figure 11-1). Provides access to all the Findings in the back-end database.
Weaknesses	Invokes the Weakness form (refer to Figure 7-1). Provides access to all the Weaknesses in the back-end database.
Action Plans	Invokes the Action Plan form (refer to Figure 8-1). Provides access to all the Action Plans in the back-end database.
Points-of-Contact	Invokes the Points-of-Contact form (refer to Figure 5-2). Provides access to all the POCs in the back-end database.
Pivot Reports	Invokes the Pivot Table Wizard form (refer to section 3.11). Provides access to user-configurable custom reports.
Admin Tools	For CMS use only—not displayed on the contractor version of the CISS application.
Analysis Reports	For CMS use only—not displayed on the contractor version of the CISS application.

3.1.4 Application Control Region

The following buttons are available in the Application Control region of the CISS main menu:

Figure 3-8. Application Control Region Buttons

Button	Function
Database Admin	Invokes the Database Administration menu (Figure 13-19) which permits the user to determine who is using the back-end database, compact/repair and backup the back-end database, and set the CISS update option to manual or automatic (refer to Chapter 13.0).
Change Back-end Database	Invokes the Connect to Back-end Database form (Figure 13-2), which permits the user to change the back-end database file (refer to section 13.1.3).
Quit Access	Closes the CISS application and exits from MS Access®.

3.1.5 Treeview Region

When the CISS main menu initially opens, it displays a single root-level node representing the organization's name (“Contractor XYZ” for User Guide examples) (refer to Figure 3-3). This root-level node is named when the database is initially configured (refer to section 13.1.3.3) but can be changed at any time (refer to section 2.4.1).

3.1.5.1 Expanding Treeview Nodes

If the Treeview root-level node is not already expanded, double-click the root-level node (i.e., “Contractor XYZ”). This activates the Component region buttons and expands the Treeview root-level node to display the major security oversight element nodes (Figure 3-4). Each of these major security element nodes (i.e., Self-Assessments [CAST], Systems, Audits, Findings, Weaknesses, Action Plans, Points-of-Contact, Documents) represents a different security oversight function within the CISS application. Each major security element node and its corresponding lower-level nodes are represented by different icons and icon colors (refer to section 3.1.5.2 for an explanation of the different Treeview node icons).




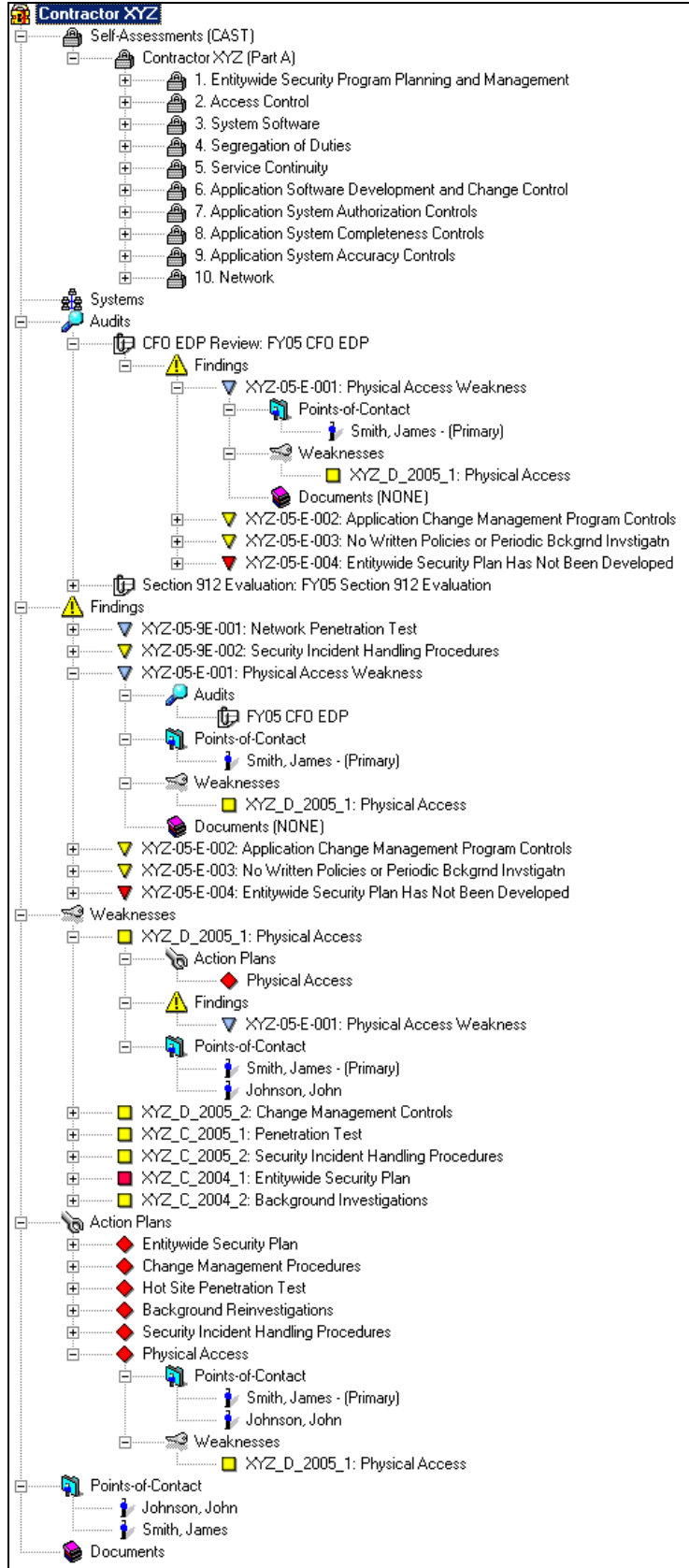


The presence of a  icon by a major security element node indicates that the node contains other lower-level nodes and related information. The major security element node, as well as all lower-level nodes, can be expanded by clicking the corresponding  icon, when present, to display other lower-level nodes or its contents (refer to Figure 3-9). If any node level does not display the  icon, it is already expanded to its lowest level—there are no lower-level nodes or other information to display. Each Treeview node level represents a collection of information (i.e., records) stored in the CISS back-end database, and the Treeview nodes present a hierarchical display and method of accessing all the information contained in the CISS database.

Figure 3-9. Partially expanded Treeview region nodes




Clicking an expanded node’s corresponding  icon collapses (i.e., closes) all lower-level nodes to the selected node level. However, clicking a node’s corresponding  icon only expands the selected node to the next lower-level node. It does not expand all lower-level nodes—it expands only one level below the selected node level. Also refer to section 3.1.5.3 for an explanation of Treeview node pop-menu options that can be used to expand and collapse nodes.

Note in Figure 3-9 that when major security element nodes and lower-level nodes are expanded to their lowest level, the lower-level nodes display the same information included in other nodes. For example, the POC names displayed in the lower-level POC nodes under the Audits, Findings, Weaknesses, and Action Plans major security element nodes display the same POC names that are included in the major-level Points-of-Contact node. In this example, the information related to a single POC is entered once in the applicable POC record but that POC record can be linked to as many CISS activities or elements, as necessary.









As mentioned earlier, the point to make here is that all information relating to the same record entry (e.g., Weakness, Audit, Finding, Weakness, POC) only has to be entered once. Any change made in any form or record, no matter how the user navigated to or accessed it, is updated wherever applicable, so that multiple changes are not required.




























3.1.5.2 Treeview Node Icons

The Treeview uses different icons to represent each of the major security element nodes (e.g., the Audits  icon). These same major security element icons are used to represent the security element (e.g. Audits) whenever it is displayed in other security element lower-level nodes (refer to Figure 3-9). In most cases, the Treeview also uses different colored icons or different icon representations to display the status of the lower-level node (refer to the individual Findings displayed under the Findings major security element in Figure 3-9 for examples). The different Treeview node icons and icon representations are explained in the following table.

NOTE: When a node is selected, its icon representation changes (e.g., enlarges) to indicate its selection. Also, the Self-Assessment “padlock” icon can display a locked or unlocked padlock icon based on the Self-Assessment status. These temporary and locked/unlocked node selection changes are depicted separately in the following table.

Figure 3-10. Major and Lower-Level Security Element Nodes

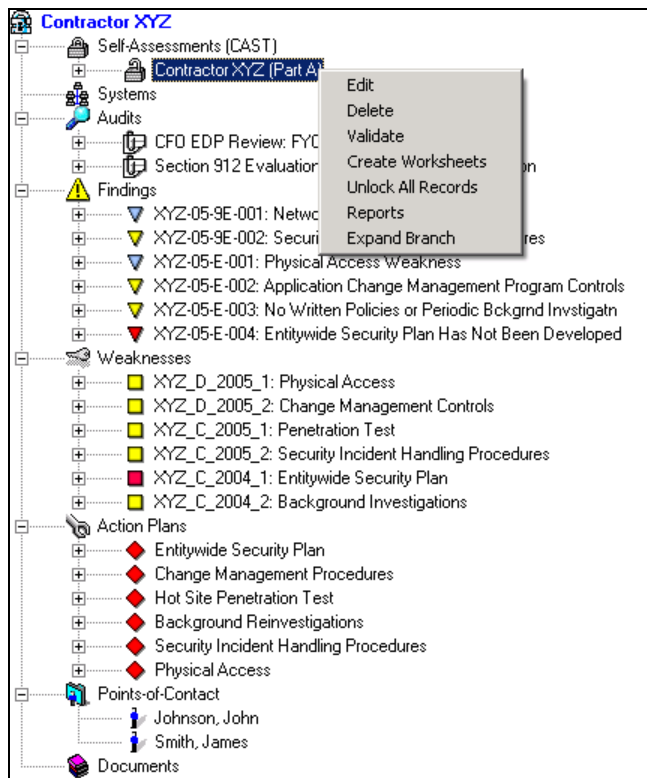
<i>Icon</i>	<i>Major and Lower-Level Security Element Nodes</i>
	<i>Self-Assessments (CAST)</i>
	CSR Level 0 status
	CSR Level 1 status
	CSR Level 2 status
	CSR Level 3 status
	CSR Level 4 status
	CSR Level 5 status
	CSR N/A status in agreement with Applicability matrix

	CSR N/A status in conflict with Applicability matrix
	CSR status not assigned
	Systems (Not functional in this release.)
	Audits
	Individual Audits
	Findings
	Closed status
	Closed Pending status
	Ongoing status
	Delayed status
	Status not assigned
	Weaknesses
	Closed status
	Closed Pending status
	Ongoing status
	Delayed status
	Status not assigned
	Action Plans (Note: Action Plan status is based on milestones.)
	Closed status
	Closed Pending status
	Ongoing status
	Delayed status
	Status not assigned
	Points-of-Contact
	Individual POCs
	Documents
	Individual documents

3.1.5.3 Treeview Node Pop-Up Menu

Right-clicking selected Treeview nodes activates a pop-up menu that allows specific functions to be performed (e.g., Add, Edit, Delete, Validate, etc.). The following figure depicts an example of a Treeview node pop-up menu expansion.

Figure 3-11. Example Treeview node pop-up menus



The Treeview pop-up menus are node-specific. The same pop-up menu options are not available at all node levels and to all node elements. All pertinent pop-up menu functions are explained in their respective sections in the User Guide. The following table summarizes the pop-up menu options and functions:

NOTE: The **Supporting Documents** form (Figure 4-1) uses different pop-up menu options than those available in the Treeview region, so those pop-up menu options are explained in section 4.8 and not included here.

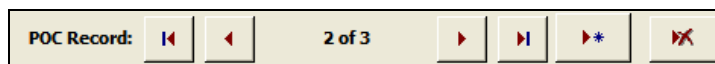
Figure 3-12. Treeview node pop-up menu summary

Pop-up Selection	Function
Add	Opens a dialog to add a new selected security element record
Collapse Branch	Collapses all expanded lower-level branches (displays only if a branch is expanded)
Create Worksheet	Creates a worksheet for the selected CSR
Create Worksheets	Creates worksheets for all CSRs in the selected Self-Assessment
Delete	Opens a dialog to delete the selected security element record
Disabled	This function is disabled in the current release
Edit	Opens a dialog to edit the selected security element record
Expand Branch	Expands the next three (3) lower-level branches, if available (displays only if branch is collapsed)
POA&M Report	Generates a POA&M Report for internal Business Partner use
Reports	Opens the selected security element reports menu
Submit POA&M	Prepares the POA&M report for submission to CMS
Submit Self-Assessments	Prepares all Business Partner Self-Assessments for submission to CMS
Unlock All Records	Unlocks all CSR response records in the selected Self-Assessment
Unlock Record	Unlocks the selected CSR response record
Validate	Performs a validation check on the selected security element

3.2 CISS Form Navigation Controls








The CISS application uses custom forms to display its information. Users can move through these form records using a mouse and the navigation buttons found in the bottom-left area of each form, such as the POC Record form navigation buttons shown in the following figure. These are the same navigation buttons used in most MS Access® applications.

Figure 3-13. Record navigation buttons



Refer to the following figure for a summary of how to use these navigation buttons to move through form records.

Figure 3-14. Record navigation button use

Tile	Function
	Move to first record
	Move to previous record
	Current record of total records
	Move to next record
	Move to last record
	Insert new record
	Delete current record

3.3 CISS Form Modes

The CISS application uses custom forms to display the information contained within its database. All CISS forms can be opened in READONLY (Figure 3-15), EDIT (Figure 3-16), or ADD (Figure 3-17) modes depending on the method employed to open the form (refer to section 3.4). In these examples, only the bottom portion of the **Points-of-Contact** form is included in the figures to illustrate the mode differences. The top portion of any CISS form is identical in all three modes and the modes in these examples apply to all CISS forms. The bottom portion of the **Self-Assessment** form differs from these examples but the modes function the same. Instructions for completing the various CISS forms are contained in separate sections in the User Guide.

Figure 3-15. CISS form READONLY mode

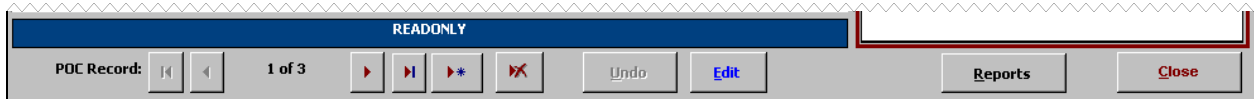


Figure 3-16. CISS form EDIT mode






























Figure 3-17. CISS form ADD mode



The following figure explains the functional differences among these form modes and how to change from one mode to another mode:

Figure 3-18. CISS form modes

Mode	Functional Capability
<p>READONLY (Figure 3-15)</p>	<p>READONLY mode is used to view an existing database record. In this mode, the form fields are not ready for user input or modification, and the  and  buttons are inactive. To change the form to EDIT mode and activate the  and  buttons, select  (refer to EDIT mode below).</p> <p>Selecting  before selecting  closes the form and returns to the CISS main menu. Selecting  changes the form to EDIT mode and selecting  while in EDIT mode returns the form to READONLY mode. Selecting  closes the form and returns to the CISS main menu.</p> <p>The  button is active to open the form’s report menu.</p> <p>The record navigation buttons at the bottom of the form are active. These navigation buttons allow movement through all existing POC records (refer to section 3.2).</p> <p>The  and  buttons are active. Selecting  opens a new blank record in ADD mode (refer to ADD mode below) while selecting  deletes the active record after a warning confirmation message.</p>
<p>EDIT (Figure 3-16)</p>	<p>EDIT mode is used to modify form fields in an existing database record. In this mode, the form is ready for user input or modifications, and the  and  buttons are activated. Selecting  closes the form and returns to the CISS main menu.</p> <p>The  button is active to open the form’s report menu.</p> <p>Some form fields are “locked” (i.e., no longer editable) by the CISS when their data is submitted to CMS. When this condition applies to a form, it is explained in the applicable User Guide sections.</p> <p>The record navigation buttons at the bottom of the form are inactive. This ensures that the user cannot exit the form except through the  and  buttons.</p>
<p>ADD (Figure 3-17)</p>	<p>ADD mode is used to add a new record to the database. In this mode, a blank form is opened and the form fields are ready for user input, and the  and  buttons are activated. Selecting  closes the form and returns to the CISS main menu.</p> <p>The  button is inactive.</p> <p>The record navigation buttons at the bottom of the form are inactive. This ensures that the user cannot exit the form except through the  and  buttons.</p>

3.4 Accessing CISS Forms

This section explains how to access CISS forms and explains why one method might be better to use than another in certain situations. It is always the same information presented in the CISS forms no matter how the form is accessed, but one method (Treeview region nodes) provides quicker, direct access while the other (Component region buttons) is better for browsing through security element record forms.

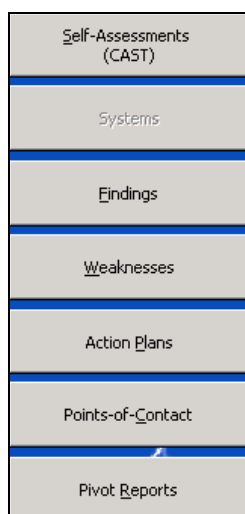
As shown on the CISS main menu (Figure 3-4), some Component region buttons [i.e., Self-Assessments (CAST), Action Plans, Weaknesses, Systems, and Points-of-Contact] include both Treeview major-level nodes and Component region buttons. However, “Audits” has a Treeview major-level node but no Component button. All security oversight elements can be accessed directly from a corresponding Treeview region node when the nodes are fully expanded. For example, in Figure 3-9, individual Findings are listed under the “Audits” and “Weaknesses” major-level nodes.





Most CISS forms can also be accessed from within other forms but the explanations in this section refer to using Component region buttons or Treeview region nodes to access CISS forms. How, as well as where, a CISS security element is accessed determines what mode the element form is opened in and the form’s functionality (refer to section 3.3).

3.4.1 Using Component Region Buttons to Access Forms

Using a Component region button (Figure 3-19) to access a CISS security oversight element *always* opens the selected form in READONLY mode (refer to Figure 3-18 for an explanation of READONLY mode). If records already exist in the selected security element, the form opens at record 1 of x (where x equals the total number of existing records within the form type). It also opens the form with active record navigation buttons to allow the user to navigate to all existing records (refer to section 3.2) in the selected security element (e.g., all POC records).

Figure 3-19. Component region buttons



If no records exist in the selected security element, the form opens at record 0 of 0 with only the  and  buttons activated. Selecting  opens a blank form (record 1 of 1) in ADD mode. Selecting  closes the form and returns to the CISS main menu (refer to Figure 3-18 for an explanation of ADD mode).

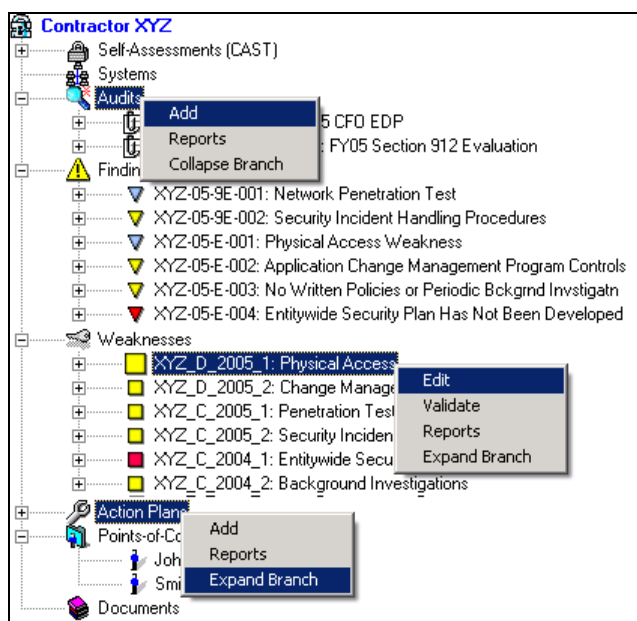
Using a Component region button offers the quickest method to open the CISS security oversight element form, but the user is then required to navigate to the desired form record and change the form mode before any modifications can be made. For example, if the back-end database contains 24 POC records and the POC record the user wishes to edit is record 15, using the “Points-of-Contact” button opens the form at record 1 of 24 in READONLY mode. The user then has to navigate to record 15 and change to EDIT mode before the record can be revised. While not a difficult task to perform, this is not the quickest method to use when trying to locate a specific record, especially if there are many such records. The next section, 3.4.2, explains how to select a specific record and open it in the desired mode.

Although the Component region buttons do not provide direct access to a specific record, using these buttons to open a security element form provides the best method to open a form and browse through all existing records in the selected form type. For example, if the user wished to review and confirm all the POC job functions, this would be the best way to browse and review all existing POC records. If a modification is necessary while browsing, the user can change from READONLY mode to EDIT mode to modify the record.


3.4.2 Using Treeview Region Nodes to Access Forms

Using the Treeview region nodes to open a CISS security element form (refer to section 3.1.5) offers the flexibility of selecting a specific record to open as well as the capability of selecting a specific function to be performed when the selected record is opened (refer to the Treeview node pop-up menus in section 3.1.5.3). For example, when the Treeview node pop-up menu “Add” is selected, the selected record is opened in ADD mode (refer to section 3.3) and when “Edit” is selected, the selected record is opened in EDIT mode (refer to section 3.3).

Figure 3-20. Treeview node pop-up menus



NOTE: Figure 3-20 is not a valid Treeview menu representation because multiple node selections cannot be made simultaneously. It is shown only to illustrate different pop-up menu options.

Treeview region nodes can be expanded to their next lower level by selecting any node’s corresponding  icon (if available) or by double-clicking any node to expand its lower-level contents (if available) (refer to Figure 3-20). Treeview nodes can also be expanded by selecting the Treeview node pop-up menu “Expand Branch” (if activated) (refer to section 3.1.5.3). Using any of these Treeview controls allows the expansion of all available lower-level security element records under each major-level node so a specific record can be selected. Use any of these techniques to expand and select the appropriate security element node or record in the User Guide Chapter explanations.

Using a Treeview node to access any CISS security element form opens only the selected record. The mode the form opens in depends on how the form was opened and what pop-up menu option was selected. Double-clicking any node that represents a security element record in the CISS opens the selected record form in READONLY mode (refer to section 3.3).

Forms accessed using Treeview region nodes always open the selected form at record 1 of 1 (unless adding a new record) no matter how many records of that form type exist in the database. It also opens the form with inactive record navigation buttons so the user is unable to navigate to other existing records in the selected security element (e.g., all POC records). Since a specific record was selected, only the selected record is opened.

Using the same examples provided in section 3.4.1, selecting a Treeview region node to open a specific POC record to edit is quicker than opening all the POC records using the Component region button and navigating to record 15 to locate the same POC. However, if the user wishes to review and confirm all POC job functions, selecting each record individually to review from Treeview region nodes would not be as easy as using the Component region button to browse through all the records.

3.5 CISS Form Drop-Down Menu Selections


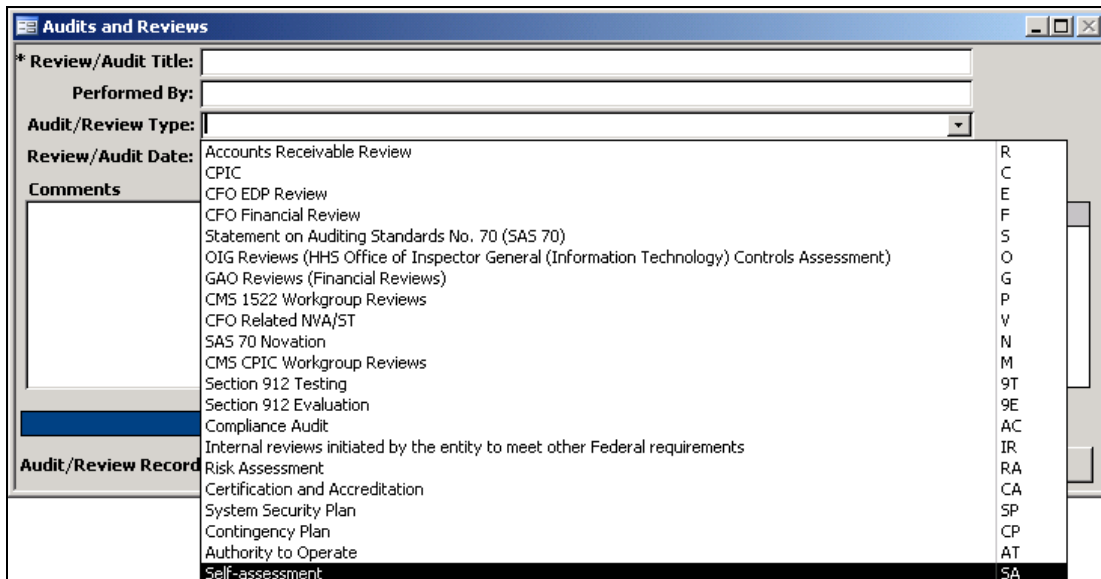
Some CISS forms use drop-down menu selections to fill-in certain fields. When a drop-down menu selection option is available, as indicated by the  button at the right end of the field, selecting this button opens a drop-down menu of valid selections.

Figure 3-21. Drop-down menu selection example

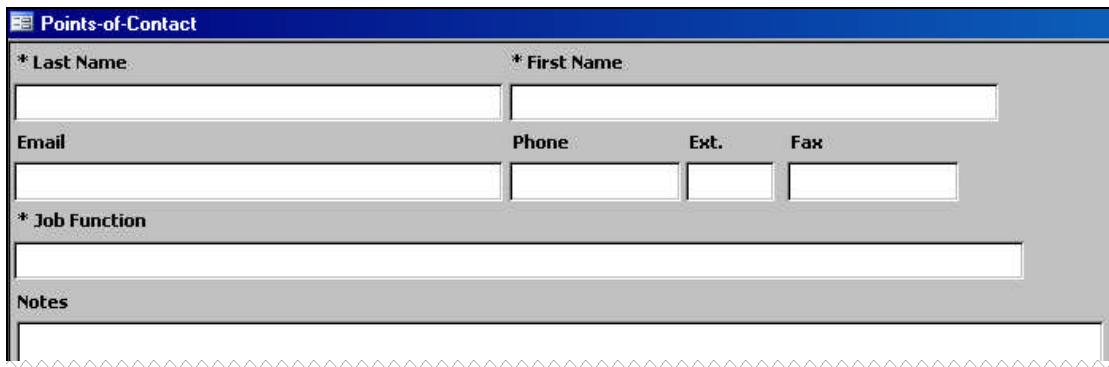


When drop-down menu selections are available, these menu selections are the only valid entries allowed in that field. The user can only select from the drop-down menu choices and cannot input other data in that field. In some cases, such as selecting a POC name from a POC drop-down menu, the user can add POCs to the database so they will be selectable from the drop-down menu. In other cases, such as in the Figure 3-21 example, the audit/review type selections are coded into the application and cannot be changed or added to by the user.

3.6 CISS Form Required Fields

Some CISS form fields require that they be filled-in before the form can be saved or the user can leave the form. Fields that display an “*” before the field name in any form are required fields (i.e., must be filled-in). In the following *Points-of-Contact* form, the “Last Name,” “First Name,” and “Job Function” are required fields.

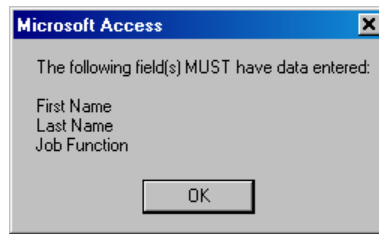
Figure 3-22. Example of required fields



The screenshot shows a web form titled "Points-of-Contact". It contains several input fields: "* Last Name", "* First Name", "Email", "Phone", "Ext.", "Fax", "* Job Function", and "Notes". The asterisk indicates that the Last Name, First Name, and Job Function fields are required.

If the user attempts to save or exit a form with blank required fields, the CISS application displays a screen message specifying which required fields are missing.

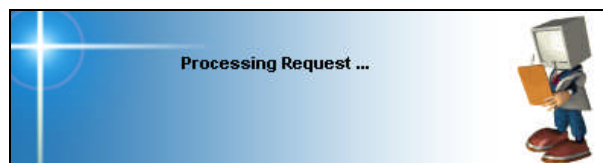
Figure 3-23. Example of required fields notification message



3.7 CISS “Busy” Message Displays

While the CISS processes certain user requests (e.g., reports, worksheets, submissions, etc.), various, and sometimes multiple, “busy” messages similar to the following message display to alert the user that the CISS is processing their request. Since these messages are self-explanatory and vary among CISS processes, they are not shown in the remainder of the User Guide.

Figure 3-24. Processing Request message



3.8 CISS Form Data Sensitivity

One of the primary purposes of the CISS application is to assist Business Partners maintain and report Weakness and Action Plan Milestone information in POA&M format to CMS. CMS uses this information to prepare and submit their annual POA&M report to the Department of Health and Human Services (DHHS) where it is combined with their report and submitted to OMB in accordance with FISMA reporting requirements.

Since some CISS form fields contain data that is reported to CMS and that data is ultimately reported outside CMS in their POA&M report, Business Partners need to be aware of which form text fields are reported outside CMS. As with all sensitive information in CMS, DHHS, and OMB, access to POA&M data is limited to those officials and staff that have an explicit business purpose for their use. However, contractor-, location-, or system-specific information, or other sensitive and identifying information should not be used in certain form text fields. If this type of weakness-related sensitive information were to be obtained by someone not permitted to access the system or someone outside the organization, the system may be exposed to unnecessary risk.

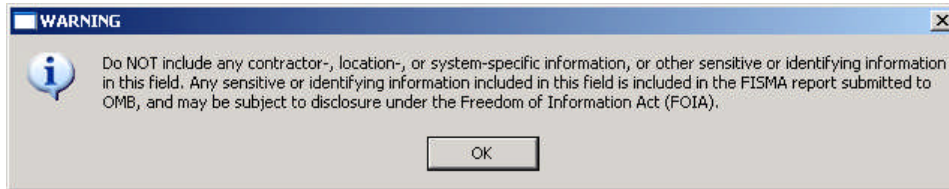
All form fields that contain text that are reported outside CMS in their POA&M report include a blue field background instead of the normal white field background (e.g., the “Title” field in Figure 3-25). The sensitive data restriction applies only to the following form/text fields that include the blue field background:

- Weakness “Title”
- Action Plan Milestone “Title”
- Action Plan Milestone Projected Date “Note”
- Action Plan Milestone Status Update “Description”

Figure 3-25. Example of sensitive form field

In addition, whenever exiting the form’s ADD or EDIT modes, the following warning message displays to alert the user about the sensitive data restriction. Selecting closes the warning message and returns to the applicable form.

Figure 3-26. Sensitive information warning message



3.9 CISS Form Validation

The data in some CISS forms are validated automatically against program criteria when the selected form is opened. If a validation error exists, the form displays an error message in red text such as the error message highlighted in yellow in the following figure.

The form’s data can also be validated by selecting the applicable form’s button (refer to the following figure). If there are errors, the CISS creates and displays a MS Word® error report that identifies the validation error(s) that need to be corrected. If there are no validation errors, a self-explanatory message dialog displays.

Figure 3-27. Highlighted example of “Validation” error message

The screenshot shows a 'Weakness' form with the following details:

- Entity:** XYZ
- Quarter:** B
- Year:** 2004
- Number:** 1
- Title:** Programmers Have Inappropriate Access
- Description:** Programmers have access to network-based applications (including production code) and network-based production data. Includes access to both older and new application code and data that includes read, write, and delete access rights. This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.
- Category:** Configuration Management
- Action Plan:** Programmer Access Restriction
- Risk:** High
- Type:** Program
- Status:** Delayed
- Likelihood:** Medium
- Impact:** High
- FISMA Severity:** Weakness



A yellow error box in the center of the form states: "There are errors on this form. Click 'Validate' to see the errors!".

The right sidebar contains the following sections:

- POCs:** Brown, William - (Primary), Davis, David
- Findings:** XYZ-05-E-001: Programmers Have Inappropriate Access
- CSRs:** 3.1.4 - Contractor XYZ (Data Center), 3.3.1 - Contractor XYZ (Data Center), 3.3.3 - Contractor XYZ (Data Center), 6.8.2 - Contractor XYZ (Data Center)
- Systems - (Disabled):**

At the bottom of the form, there is a 'Validate' button, a 'Reports' button, and a 'Close' button. A 'Weakness Record: 1 of 1' indicator is also present.

3.10 CISS Form Spell-Check Button

The primary CISS forms include a spell-check button,  (refer to Figure 3-27). This button is activate in EDIT and ADD modes (refer to section 3.3) so user input areas can be spell checked. Whenever the user is finished entering narrative-type data (e.g., titles, descriptions, responses) into a form, the user should select the  button to spell check the input fields and corrected any errors as necessary.

3.11 Pivot Reports Button

Every CISS security element report menu includes a MS Access[®] adhoc report selection (refer to section 3.12). Each of these adhoc reports requires that a MS Excel[®] report form be created and added to the CISS to provide the necessary adhoc report functionality. Consequently, the adhoc report format and filter selections must be “hard-coded” into the CISS, and the adhoc reports do not provide the report flexibility requested by the CMS and Business Partners. To provide the requested report flexibility, the CISS now includes access to the PivotTable function included in MS Excel[®].

The PivotTable function is a form of report that works by rearranging the fields and records in the contractor’s back-end database into a different format. The user can rotate (i.e., pivot) the columns in a PivotTable to display data summarized in different ways, easily sort the database in various ways, filter data, and collapse and expand the level of information displayed.

Creating and manipulating the PivotTable does not change the contents or layout of the backend database, so the user can safely use a PivotTable to experiment with contractor data without worrying about corrupting the data or needing to restore the database’s layout afterwards. A PivotTable also enables the user to perform what would otherwise be relatively complex calculations by using its built-in features.

For the near-term, the MS Access® adhoc report type and selections in each CISS security element report menu will remain in the CISS and this User Guide, but new adhoc report functionality will not be added. Instead, Business Partners should become familiar with, and use, the MS Excel® PivotTable functionality to generate their own unique reports. This User Guide provides only a brief overview of PivotTable functionality and does not provide an in-depth tutorial on how to use PivotTables. Help with using PivotTables can be found in MS Excel® Help and there is a “PivotTable Reports 101” located at the following MS web site: <http://office.microsoft.com/en-us/assistance/HA010346321033.aspx>.

3.11.1 Pivot Table Wizard

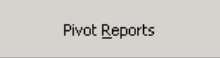
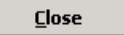
To access the MS Excel® PivotTable functionality, select the  button located in the Component region (Figure 3-3) of the CISS main menu. Selecting this button opens the following *Pivot Table Wizard* form.

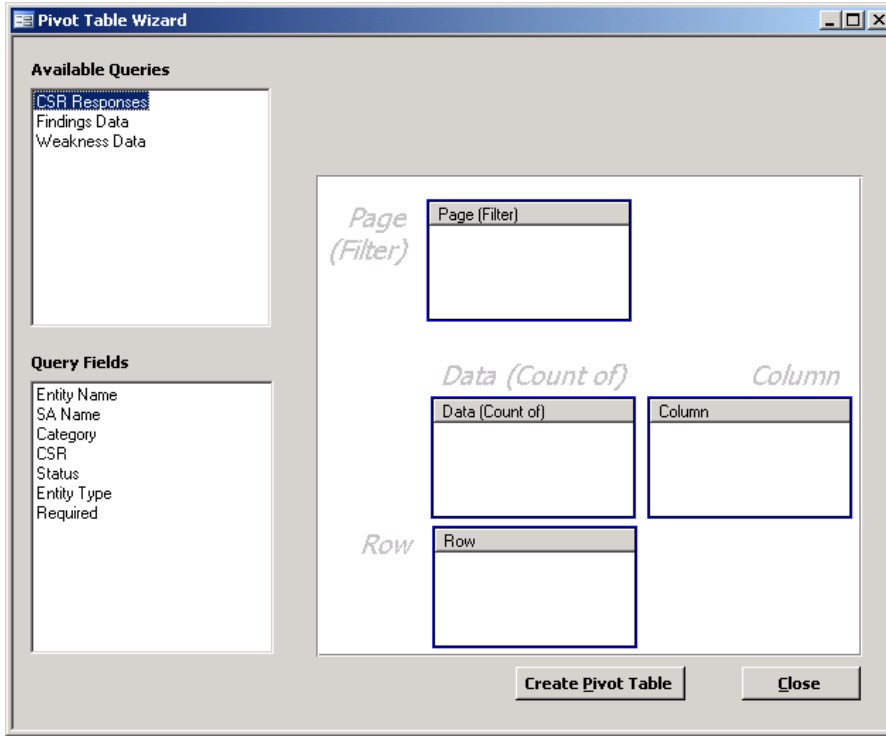
Figure 3-28. Pivot Table Wizard form

Available Queries		
CSR Responses Findings Data Weakness Data		
Query Fields		
	<i>Page (Filter)</i>	
	Page (Filter)	
	<i>Data (Count of)</i>	<i>Column</i>
	Data (Count of)	Column
	<i>Row</i>	
	Row	
	<input type="button" value="Create Pivot Table"/>	<input type="button" value="Close"/>

Selecting  closes the form and returns to the CISS main menu.

Selecting “CSR Responses” under *Available Queries* in the *Pivot Table Wizard* form displays the following report fields available under *Query Fields*:

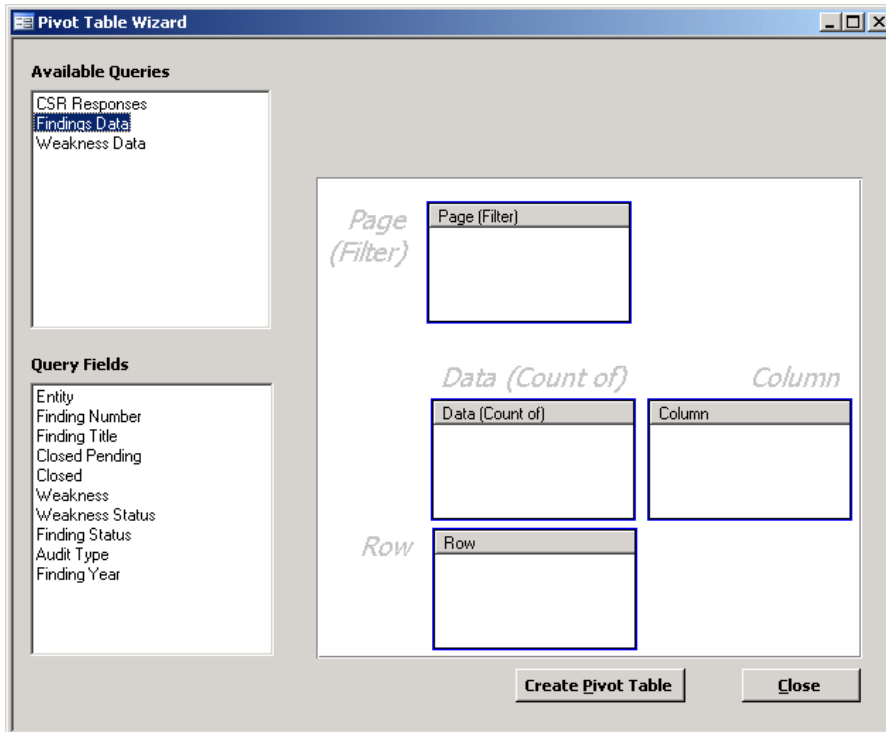
Figure 3-29. Pivot Table Wizard form CSR Responses “Query Fields”



Selecting **Close** closes the form and returns to the CISS main menu.

Selecting “Findings Data” under **Available Queries** in the **Pivot Table Wizard** form displays the following report fields available under **Query Fields**:

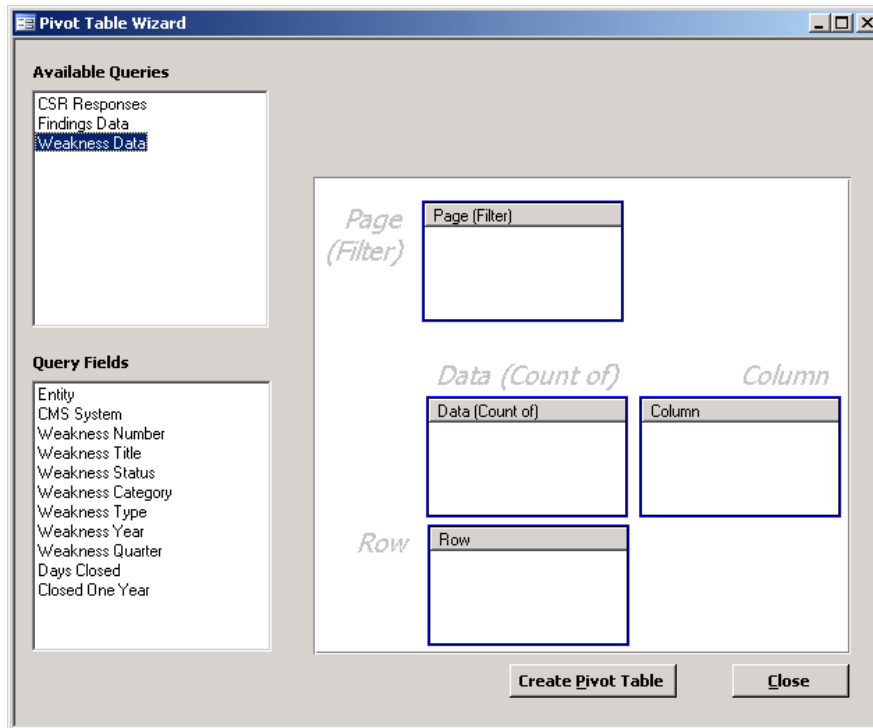
Figure 3-30. Pivot Table Wizard form Findings Data “Query Fields”



Selecting **Close** closes the form and returns to the CISS main menu.

Selecting “Weakness Data” under **Available Queries** in the **Pivot Table Wizard** form displays the following report fields available under **Query Fields**:

Figure 3-31. Pivot Table Wizard form Weakness Data “Query Fields”



Selecting **Close** closes the form and returns to the CISS main menu.

Although the **Pivot Table Wizard** form includes only three selections under “Available Queries,” each of these queries and their associated “Query Fields” encompass most of the data available in the back-end database. With these query selections and fields, almost every type of “ad hoc” report can be created. If additional query choices or fields are deemed necessary, they will be added in subsequent CISS releases.

3.11.2 Pivot Table Report Fields

The right area of the **Pivot Table Wizard** form encompasses the report formation area where “Query Fields” are “dragged” into different report field boxes (i.e., Page, Data, Column, Row) to create the desired report (see below).

Figure 3-32. Pivot Table Wizard form report area

The diagram shows a form with four main sections:

- Page (Filter):** A box labeled "Page (Filter)" containing a smaller box labeled "Page (Filter)".
- Data (Count of):** A box labeled "Data (Count of)" containing a smaller box labeled "Data (Count of)".
- Column:** A box labeled "Column" containing a smaller box labeled "Column".
- Row:** A box labeled "Row" containing a smaller box labeled "Row".

The **Pivot Table Wizard** form report fields and the resultant Pivot Report terms are depicted in the following example and are explained after the figure:

Figure 3-33. Pivot Report example

	A	B	C	D	E
1	Year	2003			
2					
3	Sum of Sales		Type		
4	Region	Salesperson	Beverages	Dairy	Meat
5	East	Buchanan	1,132		16,191
6		Davolio	8,334	14,474	1,441
7		Dodsworth	1,898		
8		Suyama	7,538	4,356	265
9	East Total		18,902	18,830	17,897
10	North	Buchanan	3,522	4,562	
11		Davolio	8,725	9,291	

- (1) **Page (Filter) Field** – A source data field that you assign to a page (or filter) orientation in a Pivot Report. For example, “Year” is a page field. You can use the “Year” field to display summarized data for only 2003, only 2004, and so on.
- (2) **Data (Count of) Field** – A source data field that contains values to be summarized. For example, “Sum of Sales” is a data field. For most types of source data, you can choose how to summarize data (for example, by sum, average, or count). A data field usually summarizes numbers, but it can also summarize text. For example, you can count the number of times a specific text entry (such as “Yes” or “No”) appears in a field.
- (3) **Column Field** – A source data field that you assign to a column orientation in a Pivot Report. For example, “Type” is a column field.
- (4) **Item** – A subcategory of a row, column, or page field. For example, the “Type” field contains the following items: Beverages, Dairy, and Meat. The “Salesperson” field contains these items: Buchanan, Davolio, Dodsworth, and Suyama.

- (5) **Row Field** – A source data field that you assign to a row orientation in a Pivot Report. For example, “Region” and “Salesperson” are row fields.
- (6) **Data Area** – The cells in a Pivot Report that contain summarized data. For example, the value in cell C5 summarizes Buchanan's beverage sales for the East region in 2003. In other words, it is a summary of the sales figures for every row in the source data that contains the items Buchanan, Beverage, East, and 2003.

3.11.3 Pivot Report Example

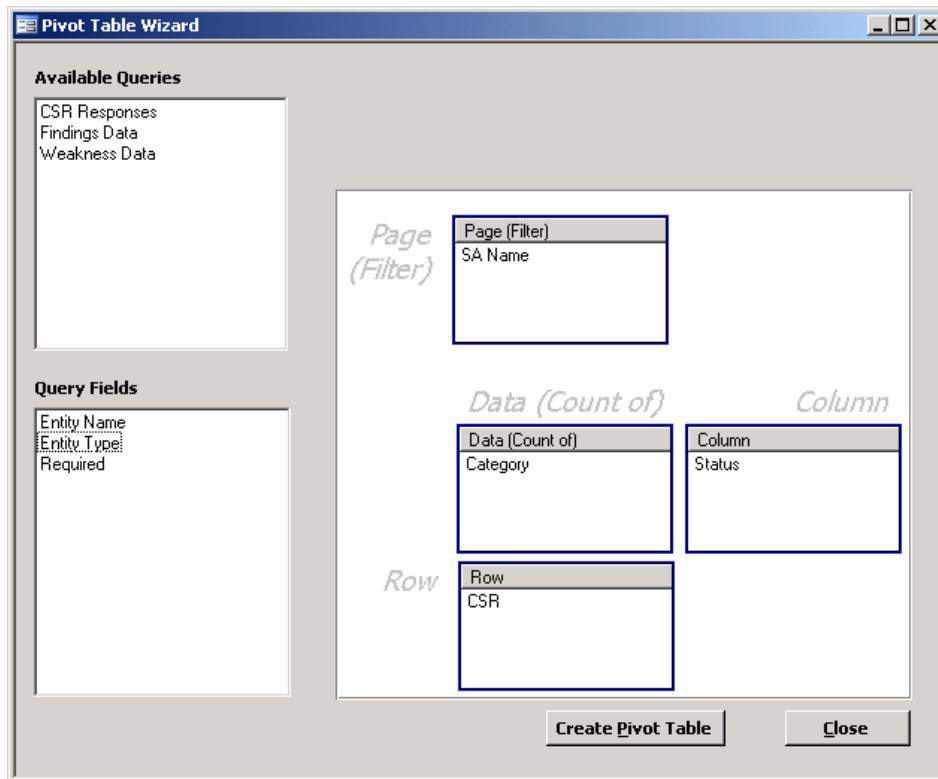
The following Pivot Report is only one example of the many report possibilities that are available when using the **Pivot Table Wizard** form to create your own unique report. The purpose of this example is only to demonstrate how to use the Wizard to create an adhoc report and is not meant to teach MS Excel® PivotTable nor to be all inclusive of other Pivot Report possibilities.

Using the “CSR Responses” query fields shown in the Figure 3-29 **Pivot Table Wizard** form, perform the following:

- a. Drag “SA Name” to the “Page (Filter)” drop box,
- b. Drag “Category” to the “Data (Count of)” drop box,
- c. Drag “Status” to the “Column” drop box, and
- d. Drag “CSR” to the “Row” drop box.

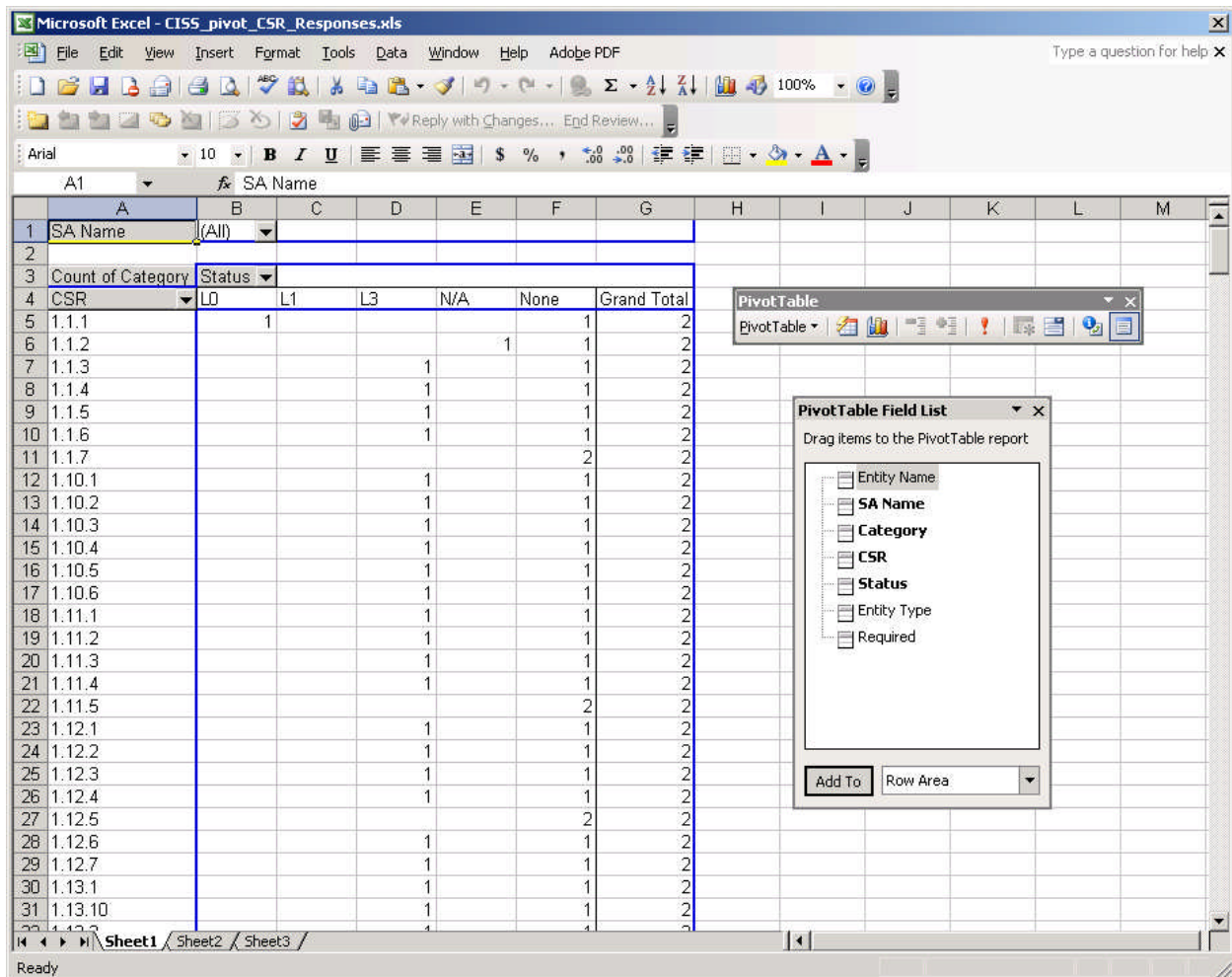
The end result of dragging these “Query Fields” is shown below:

Figure 3-34. Pivot Table Wizard form CSR Responses “Query Fields”



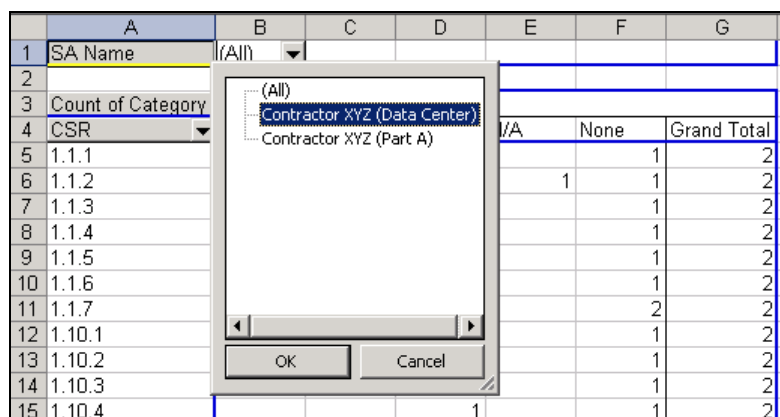
Selecting **Close** closes the form and returns to the CISS main menu. Selecting **Create Pivot Table** creates the desired report and opens the resultant report in MS Excel®:

Figure 3-35. Example Pivot Report



While in MS Excel®, the user can continue to customize the report. For example, this report includes two Self-Assessment. Selecting the “SA Name” drop-down menu displays the included Self-Assessment names.

Figure 3-36. Example Pivot Report field drop-down menu



Selecting “Contractor XYZ (A)” and , revises the report to include only “Contractor XYZ (A)” data as follows:

Figure 3-37. Example Pivot Table revised report

	A	B	C
1	SA Name	Contractor XYZ (Part A)	
2			
3	Count of Category	Status	
4	CSR	None	Grand Total
5	1.1.1		1
6	1.1.2		1
7	1.1.3		1
8	1.1.4		1
9	1.1.5		1
10	1.1.6		1
11	1.1.7		1
12	1.10.1		1
13	1.10.2		1
14	1.10.3		1

There are many other report possibilities available even with this simple example. Pivot Reports can be as simple or complex as the user is knowledgeable enough to create. As stated earlier in this Chapter, the intent of this User Guide is to provide a brief overview of MS Excel® PivotTable functionality and not to provide an in-depth tutorial on how to use it. Since creating and manipulating Pivot Reports does not change the contents or modify the layout of the backend database, experiment with the *Pivot Table Wizard* form to create various types of Pivot Reports and learn its functionality.

3.12 Adhoc (MS Access) Reports

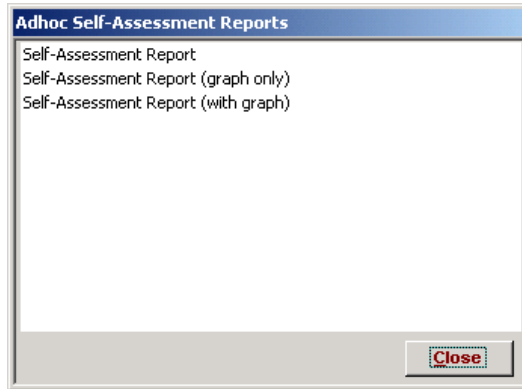
All CISS security element report menus include a MS Access® adhoc report selection (i.e., button) in their reports menu (refer to the report menu section in each security element Chapter). The adhoc report allows users to create reports that include user-specified information based on user-selected parameters (or filters). However, each of the available adhoc reports requires that a MS Excel® report form be created and added to the CISS to provide the necessary adhoc report functionality. Consequently, the adhoc report format and filter selections must be “hard-coded” into the CISS. Because of this, adhoc reports do not provide the same report flexibility provided by the Pivot Table reports described in section 3.11. However, an adhoc report may still provide the desired information in a pre-formatted report without having to use a Pivot Table report.

The creation and contents of adhoc reports is based on user-selected parameters (or filters). The selection of Primary and Secondary adhoc filters is performed in the same manner for all security element adhoc reports even if the filter selections may be different. For that reason, the selection of Primary and Secondary filters is explained here, and any selection filter specifics are explained in the applicable security element sections. The examples shown here refer to Self-Assessment/CSR adhoc reports, but the same filter selection process applies to all other security elements.

3.12.1 Adhoc Report

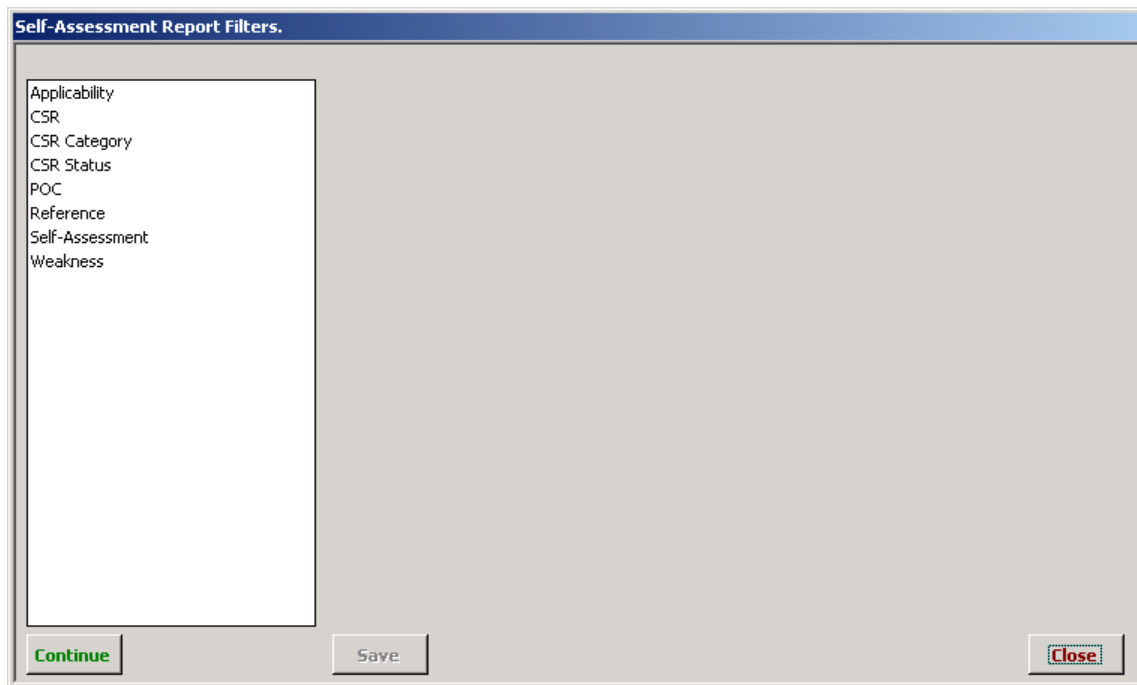
To generate an adhoc report, select the **Adhoc (MS Access)** on the applicable security element reports menu. This opens an adhoc report type selection dialog such as the following **Adhoc Self-Assessment Reports** dialog. Some security elements may display only one report type while others may display multiple report types.

Figure 3-38. Adhoc report type selection dialog



Selecting **Close** closes the reports type dialog and returns to the security element reports menu. Double-clicking a report type such as the “Self-Assessment Report” selection in the above dialog opens a Primary filter selection form such as the following **Self-Assessment Report Filters** form. The Primary filters displayed and available in the selection form are based on the security element and report type selected, so they will differ among security elements and report types.

Figure 3-39. Adhoc Primary filter selection form



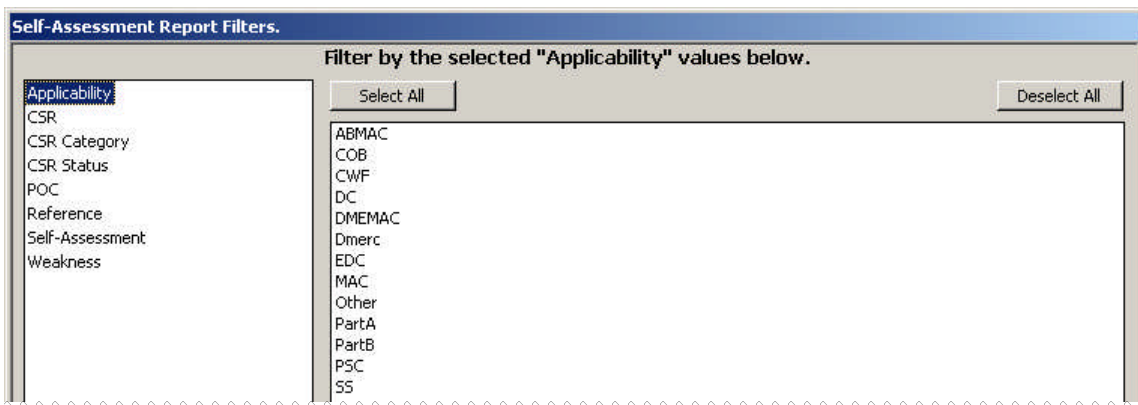
Selecting **Close** closes the Primary filter selection form and returns to the security element adhoc report type selection dialog (Figure 3-38). Selecting **Continue** before selecting any Primary filters listed on the left side of the form generates an unfiltered report that includes all available filter selections and form elements.

3.12.1.1 Adhoc Report Primary and Secondary Filters

The left side of the filters form lists the Primary filters that are available for selection. Selecting any of the Primary filters opens additional selection-based Secondary filters in a separate window on the right side of the form.

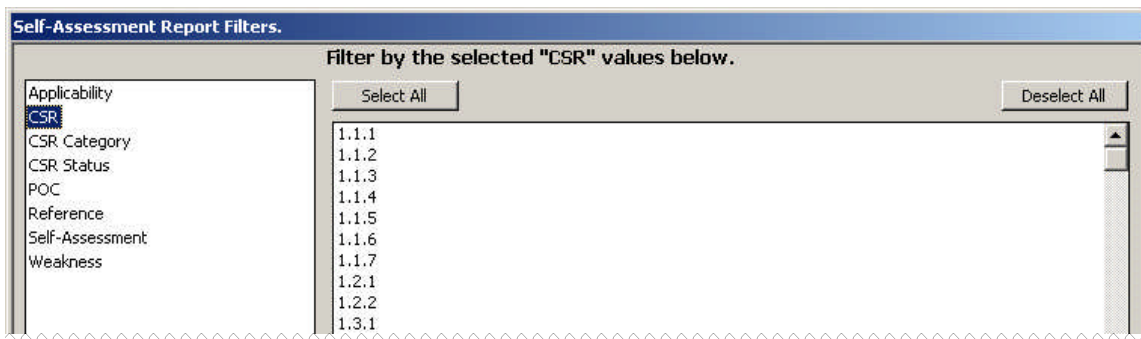
For example, selecting the “Applicability” Primary filter opens the following Secondary filter selections dialog.

Figure 3-40. Adhoc report “Applicability” Primary and Secondary filters



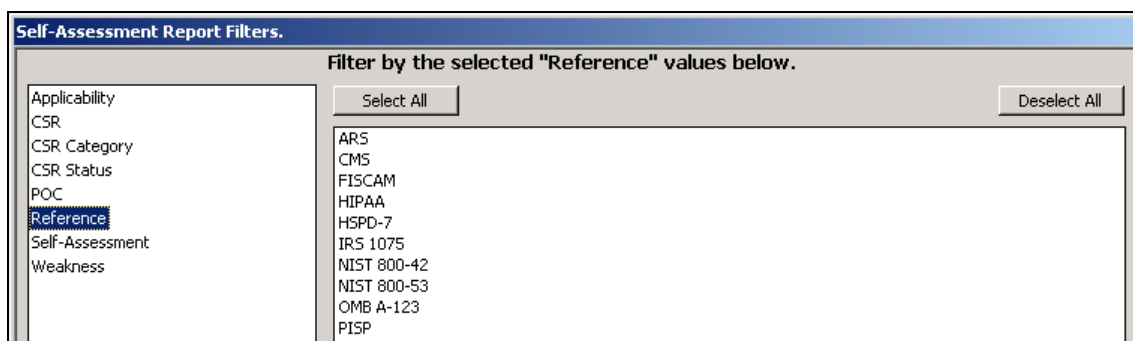
Selecting the “CSR” Primary filter opens the following Secondary filter selections dialog.

Figure 3-41. Adhoc report “CSR” Primary and Secondary filters



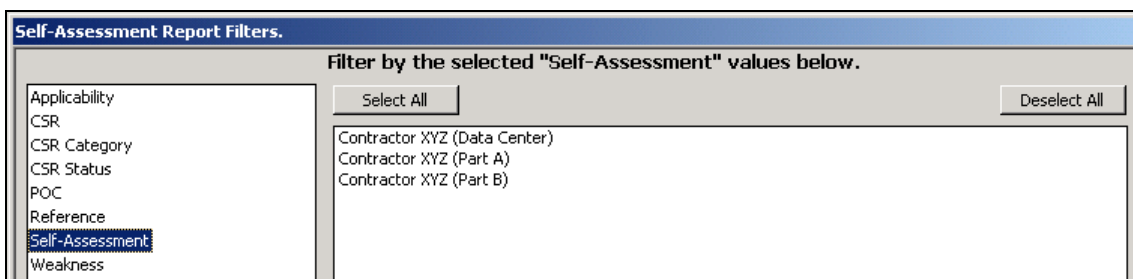
Selecting the “Reference” Primary filter opens the following Secondary filter selections dialog.

Figure 3-42. Adhoc report “Reference” Primary and Secondary filters



The above examples include CISS “hard-coded” Secondary filter selections because they are the same for all Business Partners. Other Secondary filter selections are based on Business Partner-specific data, such as POC, Self-Assessment, Weakness, Action Plan, and Finding names and/or numbers. For example, selecting the “Self-Assessment” Primary filter opens a Secondary filter selections dialog similar to Figure 3-43 which displays Secondary filters based on Business Partner-specific Self-Assessments.

Figure 3-43. Adhoc report “Self-Assessment” Primary and Secondary filters



3.12.1.2 Adhoc Report Multiple Filter Selection

After selecting a Primary filter from the left side of the filters selection form, select one or more Secondary filters (i.e., multiple filters can be selected) from the right side of the form. To select a Secondary filter, highlight the filter(s) by single-clicking the desired filter(s). To select multiple Secondary filters, highlight the filter(s) by using the **Ctrl+Single Click** key/mouse combination (i.e., keeping the **Ctrl** key depressed while single-clicking the left mouse button). To remove a selected Secondary filter(s), click the filter again to deselect it. To select all the Secondary filters, select and to deselect all Secondary filters, select .

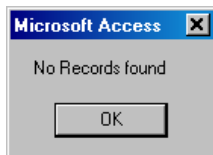
When finished selecting the Secondary filter(s) for a selected Primary filter, selecting saves the filter selection(s), while exits *without* saving the Secondary filters. Both selections return to the security element Primary filter selection form (Figure 3-39).

Additional Primary and Secondary filters can be selected by repeating the above procedures until all desired filters are selected. After the filter selections are completed, selecting generates a report based on the specified filter selections, while exits *without* creating a report. Once is selected, whether it results in a report or no records being found, all filters are reset and must be reselected to generate another report.

3.12.1.3 Adhoc Report Example

Some ad-hoc report filter selection combinations may result in no records being found that meet all of the specified criteria. When that is the case, the following message displays instead of a report.

Figure 3-44. No records found message



Once created, a report similar to the following Contractor XYZ (Data Center) Self-Assessment example (i.e., report type: “Self-Assessment Report,” Primary filter: “CSR Status,” Secondary filter: “N/A”) is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 3-45. Example CSR Adhoc report

CMS		CSR Self-Assessment for Contractor XYZ (Data Center)		
		Type: DC		
Category: 1	Entitywide Security Program Planning and Management			
General Req: 1.3	Handling, storage, and destruction of sensitive information shall be formally controlled.			
CSR: 1.3.1	Business Partners transmitting FTI from a mainframe computer to another computer need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies only to the COB contractor.)			
Applicability: COB	Status: N/A		Rev of 04/18/05	
Current Response:	This is a generic response for CSR 1.3.1 in the self-assessment for Test SA for ABC (D). This response was created on Monday, April 18, 2005.			
Web Addresses:	None assigned			
GUIDANCE	PROTOCOLS	RELATED CSRs	REFERENCES	POC
Transmission of Federal Tax Information must be accompanied by appropriate records that will determine who released the information and what was released.	For a complete document being washed from the IRS, observe handling of receipt of sensitive information for compliance with established procedures. Review relevant policies and procedures for inclusion of the required logging process elements. Interview possible individual(s) to confirm understanding of the required procedure. Review which system list for entities indicating that the documented process has been followed.	1.3.8	IR.1075-13.3@2.2	Erwin, William - (Primary) §8C
CSR: 1.3.8	Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)			
Applicability: COB	Status: N/A		Rev of 04/18/05	
Current Response:	This is a generic response for CSR 1.3.8 in the self-assessment for Test SA for ABC (D). This response was created on Monday, April 18, 2005.			
Web Addresses:	None assigned			
GUIDANCE	PROTOCOLS	RELATED CSRs	REFERENCES	POC
A formal security program should be established with a policy and procedure. A good approach when returning FTI information to CMS is to obtain a receipt and provide a notification which contains when and why the information was obtained, to whom and for what reason(s) it was used, and when it was returned so as to make the FTI information usage traceable.	Review audit data confirming compliance and use of the required procedure. Review relevant policies and procedures for inclusion and directed use of the required process. Confirm by inspection that facility has latest version of IR.8 Publication 1075.	1.3.1	IR.1075-13.3@4.1 IR.1075-13.3@4.2 IR.1075-8.1	Erwin, William - (Primary) §8C

3.12.1.4 Adhoc Report File Controls

Depending on the adhoc report type selected, the reports are created and displayed as either a MS Word®, Excel®, or Access® report. MS Word® and Excel® reports create and open a new document or spreadsheet with their respective Toolbar file controls. Whereas, MS Access®



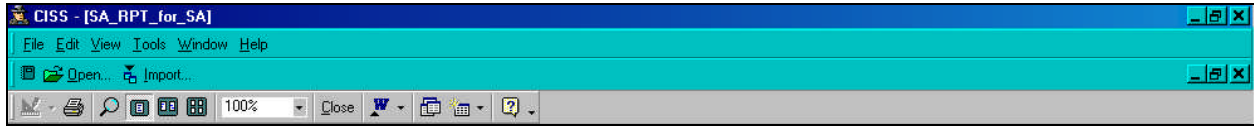
reports open as a sub-form inside the CISS. To manipulate MS Access® reports, use the non-blue highlighted report Toolbar controls depicted in the following figure to print () and close () the report.

Figure 3-46. MS Access® report Toolbar controls



4.0 Documentation


CMS requires that supporting documentation be included with Self-Assessment and POA&M submissions to corroborate certain non-compliant CSR responses and to corroborate closed audit or review Findings. Currently, documentation is required under the following conditions or circumstances:

- **CSR “N/A” Status Counter to Applicability Matrix** – CMS approval documentation is required for all CSR “N/A” responses that are not corroborated by the CSR Applicability matrix. That is, the CSR should be applicable for the contract type but the Business Partner does not agree.
- **Risk-Based Decision Non-Compliant CSR** – CMS concurrence documentation and updated Risk Assessment for all non-compliant CSR responses is required where a risk-based decision was made that no Weakness/Action Plan combination is required nor desired.
- **“Closed Pending” and “Closed” Finding Status** – Appropriate documentation is required to substantiate a “Closed Pending” and “Closed” Finding status, including the letter from CMS confirming the closure status.

NOTE: Review BPSSM Appendix A for other reporting requirements pertaining to the above situations.

This Chapter explains the general mechanics of using the CISS documentation feature. Chapters 6.0 and 11.0 include any documentation functions specific to those sections and forms.

4.1 Opening the Supporting Documents Form

Only two CISS forms include the supporting documents function: **Self-Assessment** and **Findings**. The  button in these two forms is only activated when one of the three conditions explained in section 4.0 are met. There is also a Treeview region major-level “Documents” node (Figure 3-4).

To open the **Supporting Documents** form (Figure 4-1), use either of the following methods:




- Expand the Treeview region “Documents” major-level node (refer to section 3.1.5.1) and double-click the lowest-level node below the desired supporting document to open the applicable CISS form. Then select the  button on the **Self-Assessment** form (Figure 6-7) or **Findings** form (Figure 11-2).
- Select the  button on the **Self-Assessment** form (Figure 6-7) or **Findings** form (Figure 11-2). For example, selecting the  button on the **Self-Assessment** form opens the following **Supporting Documents** form.

Figure 4-1. Supporting Documents form

NOTE: The **Supporting Documents** form shown in Figure 4-1 depicts a blank form, such as when no other supporting documents have been assigned to other Findings or CSRs (i.e., the “Available Documents” area on the left side of the form is blank) and when initialing assigning supporting documents to CSR 1.1.2 (i.e., the “Supporting Documents” area on the right side of the form is blank).

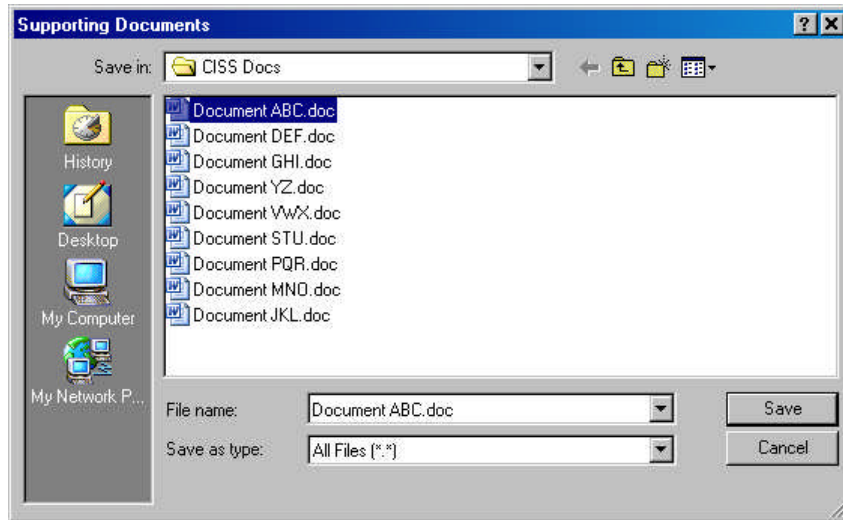
The top portion of the **Supporting Documents** form indicates the security element that the documents will be supporting. In this example, the supporting documents will corroborate CMS’ decision to accept a risk-based decision relating to non-compliant CSR 1.1.2.

Selecting **Save and Close** closes the **Supporting Documents** form and returns to the calling security element form (e.g., **Self-Assessment** form). Note that the **Close w/o Saving** button is not active at this point because no changes have been made to the form or the listed documents. This button is only active when changes are made. Otherwise, there is no reason for the user to exit the form without saving the form, so only the **Save and Close** button is active.

4.2 Adding New Supporting Documents

To add new “Supporting Documents” to the right side of the form when there are none listed or when the correct document is not listed in “Available Documents” on the left side of the form, select the **New Document** button. This opens the following **Supporting Documents** dialog.

Figure 4-2. Supporting Documents dialog



Navigate to the folder where the document you want to add is stored, select the document file name, and select the **Save** button. To select multiple documents, select and save each document individually. The original copy of all selected documents remains in its original location—untouched. The CISS saves a *copy* of the selected document in a separate location for its use and for submission to CMS.

After one or more documents have been selected and saved, the **Supporting Documents** form is automatically updated to display the selected document(s) on the “Supporting Documents” side of the form (Figure 4-3). The “Status” column under “Supporting Documents” displays the date the document was added.

Figure 4-3. Supporting Documents form displaying Supporting Documents

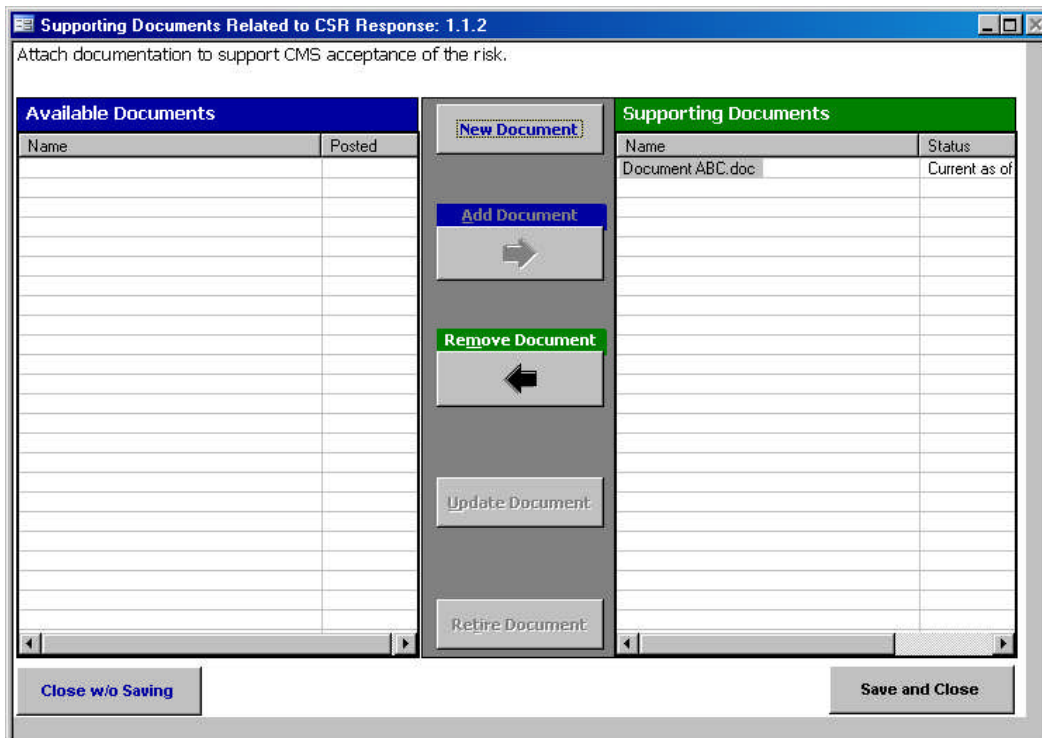


Figure 4-5. Supporting Documents form displaying moved Available Documents

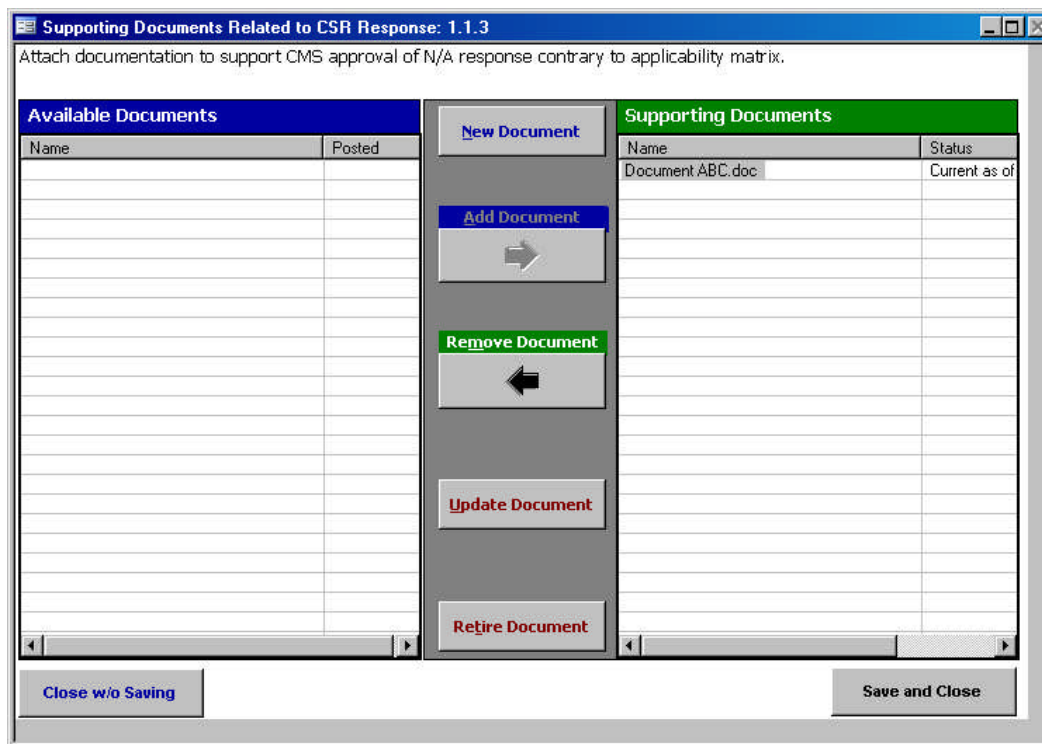


Figure 4-5 now displays the former “Available Documents” (i.e., Document ABC.doc) under “Supporting Documents.” It is no longer listed under “Available Documents” for this CSR example because it is already being used under “Supporting Documents.” However, this document (i.e., Document ABC.doc) will continue to display under “Available Documents” for other security elements that do not use this document under “Supporting Documents.”

Since changes were made in the form, the **Close w/o Saving** button is now active. Selecting **Close w/o Saving** exits the form without saving the supporting document addition(s). Selecting **Save and Close** saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

4.4 Remove Supporting Documents

Once a document has been selected to support a security element (e.g., CSR, Finding), such as in the previous examples, that document is listed under “Supporting Documents” for the applicable security element. To remove a documents listed under “Supporting Documents” (e.g., wrong document selected), highlight the document to be removed under the “Supporting Documents” listing and select the **Remove Document** button (Figure 4-6).

Figure 4-6. Supporting Documents form displaying Supporting Documents

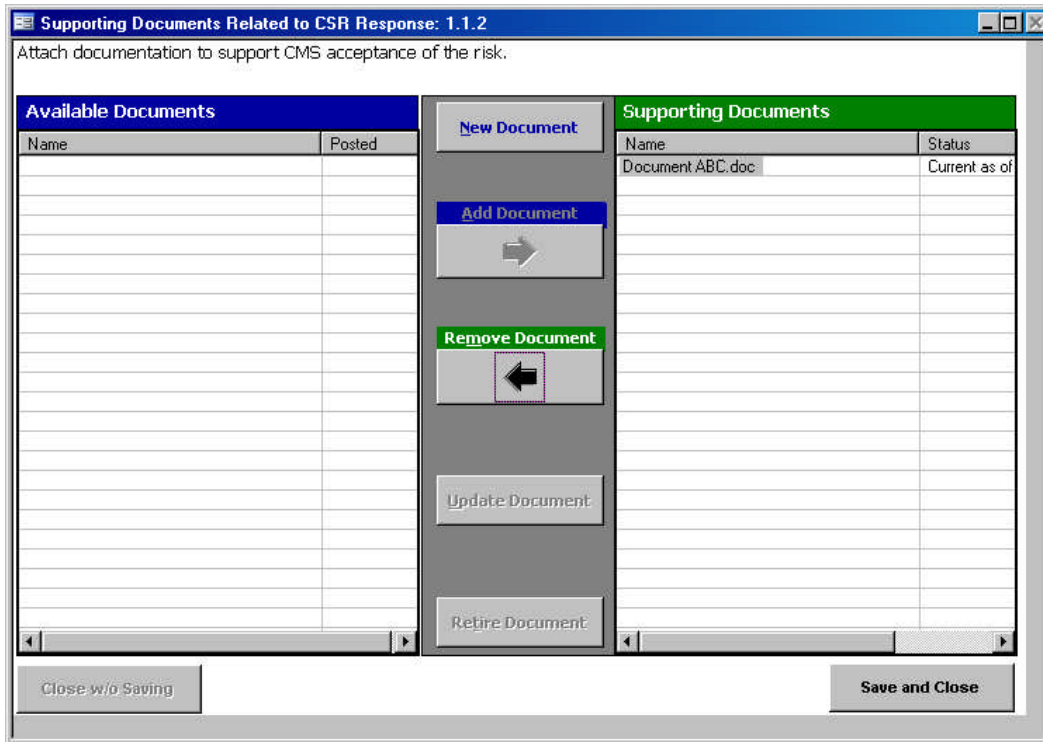
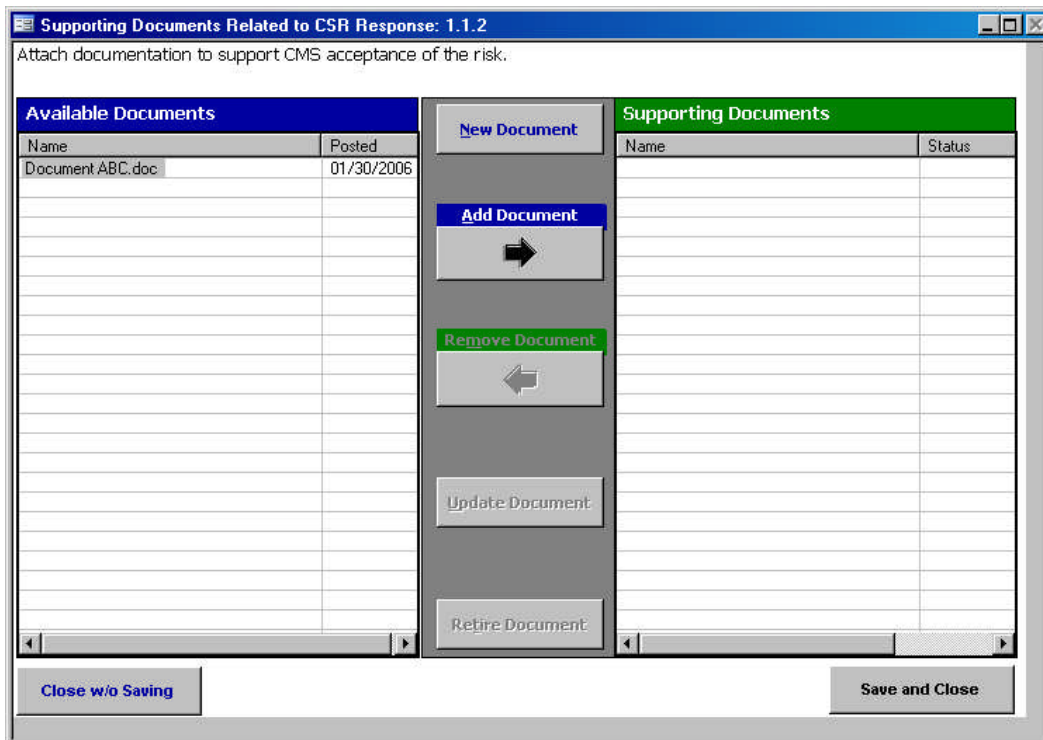


Figure 4-7 now displays the former “Supporting Documents” (i.e., Document ABC.doc) under “Available Documents.” It is no longer listed under “Supporting Documents” for this CSR example because it was removed from the “Supporting Documents” listing.

Figure 4-7. Supporting Documents form displaying Supporting Documents



Since changes were made in the form, the **Close w/o Saving** button is now active. Selecting **Close w/o Saving** exits the form without saving the supporting document addition(s). Selecting **Save and Close** saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

4.5 Update Documents

When a “supporting” or “available” document is updated with a newer version, the source file referenced within the CISS must also be updated. A document can be updated either under the “Available Documents” or “Supporting Documents” listing. What happens depends under which listing the document is updated.

4.5.1 Updating Supporting Documents

To update a document under “Supporting Documents,” select the document file name and select the **Update Document** button (Figure 4-8).

Figure 4-8. Supporting Documents form Update Document

Supporting Documents Related to CSR Response: 1.1.2

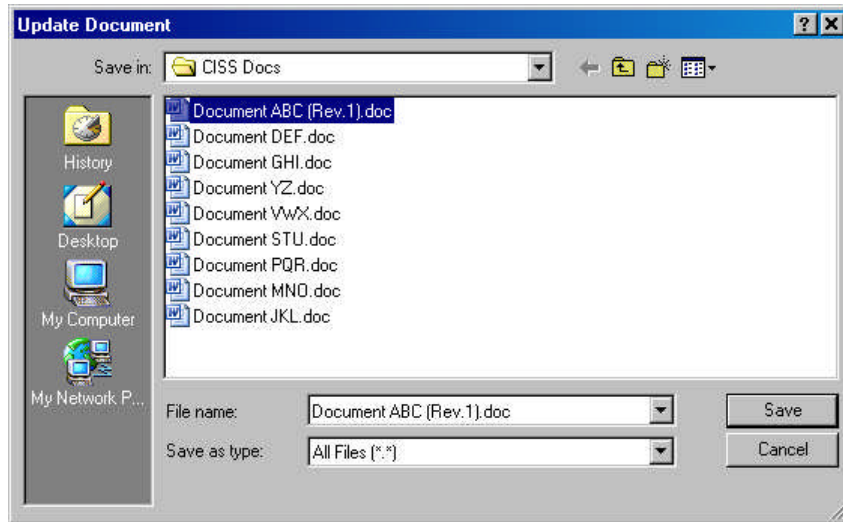
Attach documentation to support CMS acceptance of the risk.

Available Documents		New Document	Supporting Documents	
Name	Posted		Name	Status
		Add Document →	Document ABC.doc	Current as of
		Remove Document ←		
		Update Document		
		Retire Document		

Close w/o Saving Save and Close

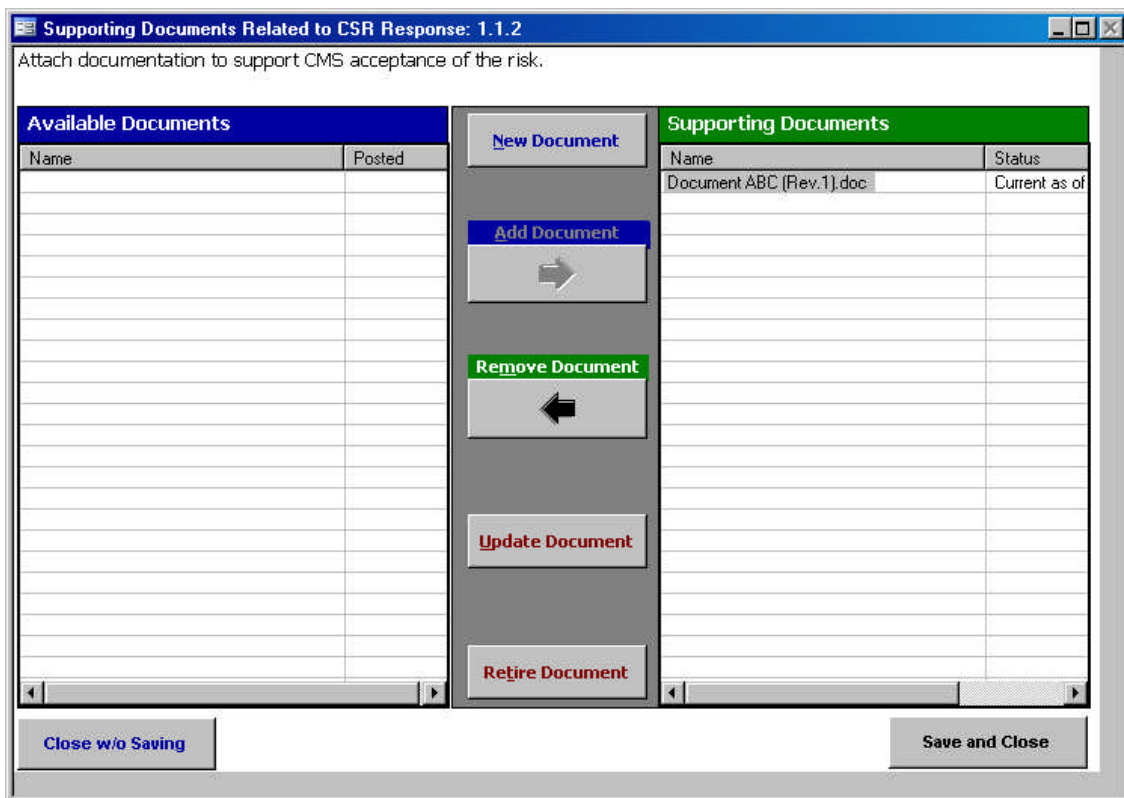
This opens the following **Update Document** dialog.

Figure 4-9. Update Document dialog



Navigate to the folder where the updated document is stored, select the document file name, and select the **Save** button. After the updated document has been selected and saved, the **Supporting Documents** form is automatically updated to display the updated document on the “Supporting Documents” side of the form (Figure 4-10).

Figure 4-10. Supporting Documents form displaying updated Supporting Documents

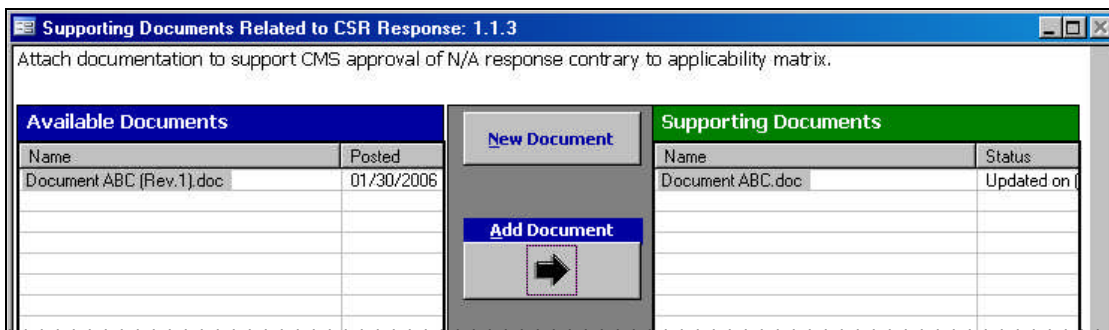


Since changes were made in the form, the **Close w/o Saving** button is now active. Selecting **Close w/o Saving** exits the form without saving the supporting document addition(s). Selecting **Save and Close** saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

In the previous CSR 1.1.2 “Update Documents” example, “Document ABC.doc” was updated to “Document ABC (Rev.1).doc” under “Supporting Documents” (Figure 4-10). However, only the document listing for CSR 1.1.2 under “Supporting Documents” was updated because the previous version of this document (i.e., before the revision) may still be a valid document under “Supporting Documents” for other security elements. Conversely, since this document was revised, the older version can no longer be selected to provide corroboration for new security elements, so only the revised version will be listed under “Available Documents.”

Refer to Figure 4-11 to view how this works for the CSR 1.1.3 example. CSR 1.1.3 used the same “Supporting Document” as CSR 1.1.2, “Document ABC.doc.” Although this document was updated for CSR 1.1.2 (Figure 4-10), it was not automatically updated for CSR 1.1.3. However, the updated version of this document is listed under “Available Documents.” The “Status” column under “Supporting Documents” displays the date the documented was updated.

Figure 4-11. Supporting Documents form displaying updated document



To update the existing CSR 1.1.3 “Document ABC.doc” listed under “Supporting Documents” with the updated version, select the **Add Document** ➔ button (Figure 4-11).

Figure 4-12. Supporting Documents form displaying updated document

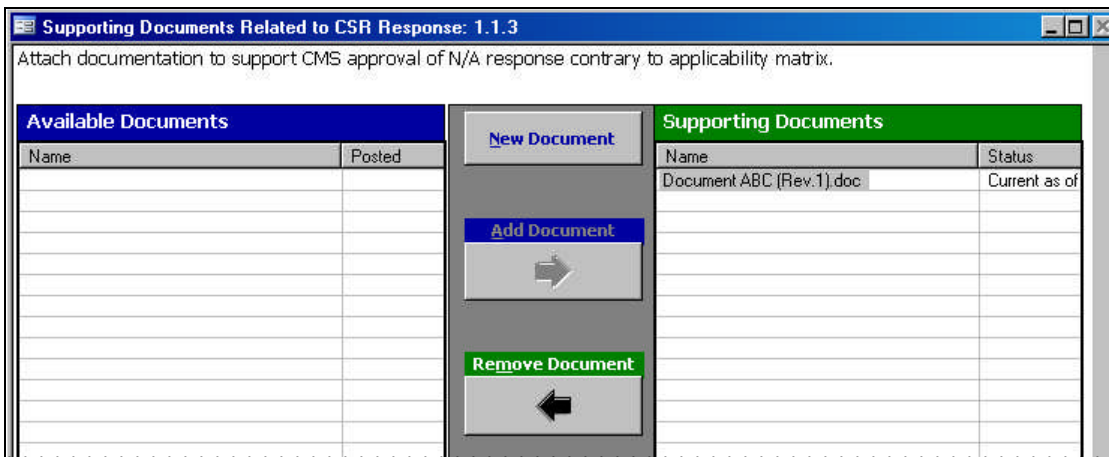


Figure 4-12 now displays the updated CSR 1.1.3 “Document ABC (Rev.1).doc” under “Supporting Documents.” It is no longer listed under “Available Documents” for this CSR example because it is already being used under “Supporting Documents.” However, the “Document ABC (Rev.1).doc” will continue to display under “Available Documents” for other security elements that do not use this document under “Supporting Documents.”

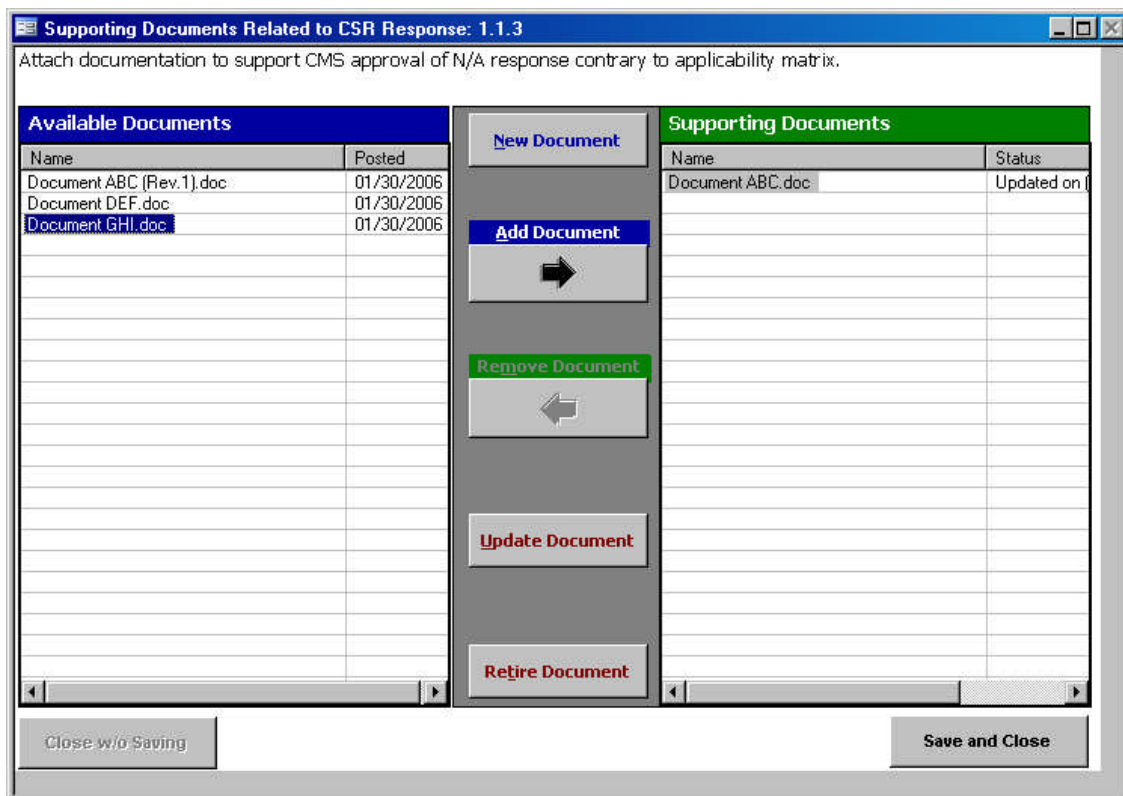
Since changes were made in the form, the **Close w/o Saving** button is now active. Selecting **Close w/o Saving** exits the form without saving the supporting document addition(s). Selecting **Save and Close** saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

4.5.2 Updating Available Documents

When the user updates a document listed under “Available Documents,” the CISS presumes that the user also wants to add the updated document to “Supporting Documents” for that security element. So do not update documents listed under “Available Documents” unless you also want to add the updated document to “Supporting Documents.” Use the previous section, 4.5.1, to update documents in “Supporting Documents.”

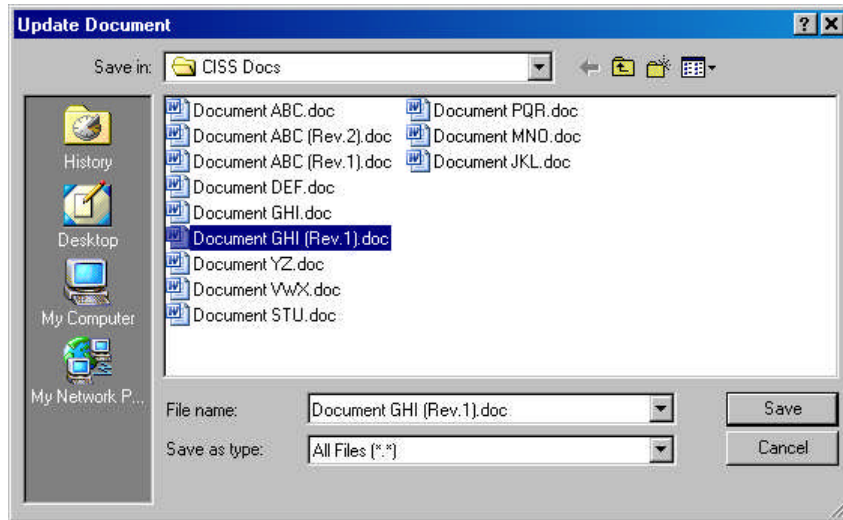
To update a document under “Available Documents” and have the updated document added to “Supporting Documents,” select the document file name and select the **Update Document** button (Figure 4-13).

Figure 4-13. Supporting Documents form Update Document



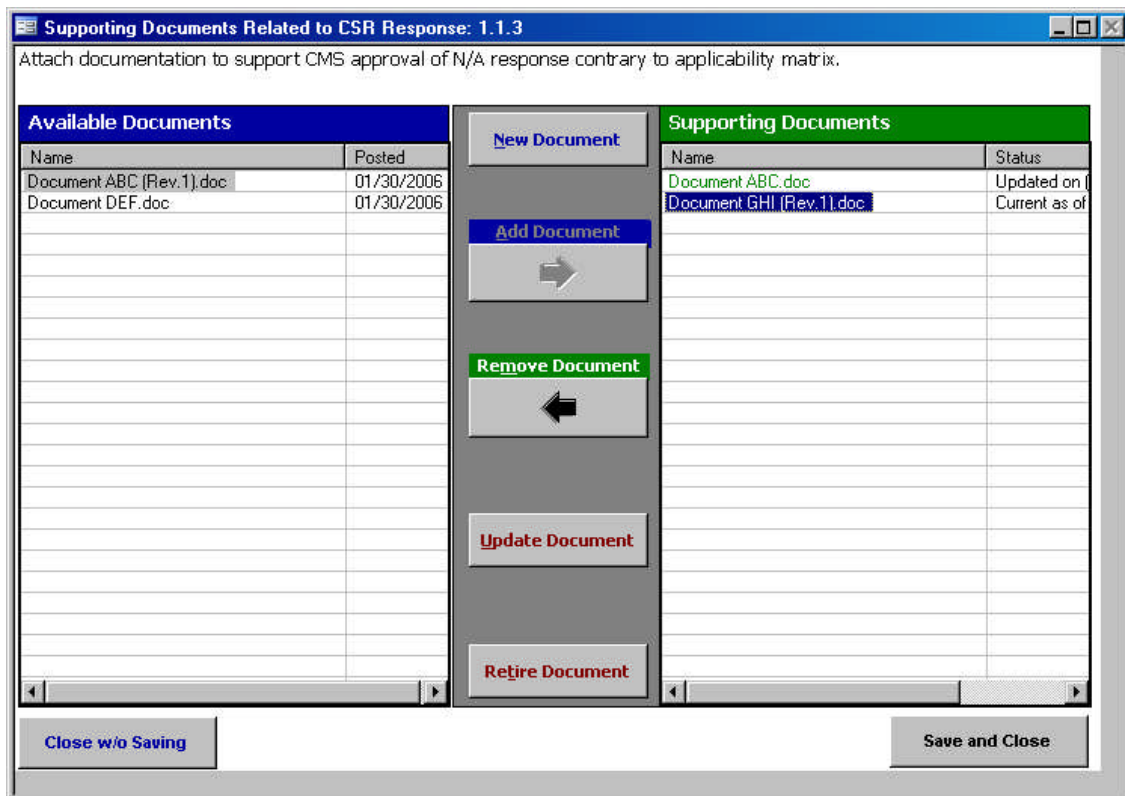
This opens the following **Update Document** dialog.




Figure 4-14. Update Document dialog



Navigate to the folder where the updated document is stored, select the document file name, and select the **Save** button. After the updated document has been selected and saved, the **Supporting Documents** form is automatically updated to display the updated document, “Document GHI (Rev.1).doc” under “Supporting Documents” but is not listed under “Available Documents” (Figure 4-15). Note that the older version of the document, “Document GHI.doc” is also not listed anywhere.

Figure 4-15. Supporting Documents form displaying updated Supporting Documents




Since changes were made in the form, the  button is now active. Selecting  exits the form without saving the supporting document addition(s). Selecting  saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

4.6 Retire Documents

Documents are “retired” when they are no longer relevant as a supporting document and can not be used as “Supporting Documents.” “Retired” documents are removed from the “Available Documents” listing so they cannot be selected elsewhere but they remain listed as “Supporting Documents” where previously selected. That is, if the “retired” document was previously selected as a supporting document, it will remain listed as a “Supporting Documents.”

An example for “retiring” a document might be an organizational-level policy that was originally used as a supporting document and it was replaced by a Medicare claims-specific policy. The former organizational-level policy is not “updated” but is “retired” and the new Medicare claims-specific policy is added as a new supporting document. The former organizational-level policy remains listed under “Supporting Documents” for the applicable security element but it is no longer selectable from the “Available Documents.”

Any document listed under “Available Documents” or “Supporting Documents” can be selected for “retirement.” Documents “retired from “Available Documents” will no long be listed as available for selection. However, when a document listed under “Supporting Documents” is retired, it is automatically removed from the “Available Documents” listing for other security elements but it will remain listed under “Supporting Documents” for the applicable security element. A future upgrade to the CISS will use different colored file name entries to designate if a support document is an original, revised, or retired copy.

To “retire” a document, select the applicable document under the “Available Documents” or “Supporting Documents” listing and select the  button (Figure 4-16).



WARNING: There is no confirmation notice after selecting the  button. Selecting it “retires” the document selection immediately. However, if that was not your intent, selecting the  button exits the form without saving the changes.

Figure 4-16. Supporting Documents form

Supporting Documents Related to CSR Response: 1.1.3
Attach documentation to support CMS approval of N/A response contrary to applicability matrix.

Available Documents		New Document	Supporting Documents	
Name	Posted		Name	Status
Document ABC (Rev.1).doc	01/30/2006	Add Document	Document ABC.doc	Updated on (
Document DEF.doc	01/30/2006		Document GHI.doc	Retired on (0
		Remove Document		
		Update Document		
		Retire Document		

Close w/o Saving Save and Close

Figure 4-16 shows the **Supporting Documents** form with the selected document retired and removed from the “Available Documents” listing. The “Status” column under “Supporting Documents” displays the date the documented was retired.

Figure 4-17. Supporting Documents form displaying Retired Document

Supporting Documents Related to CSR Response: 1.1.3
Attach documentation to support CMS approval of N/A response contrary to applicability matrix.

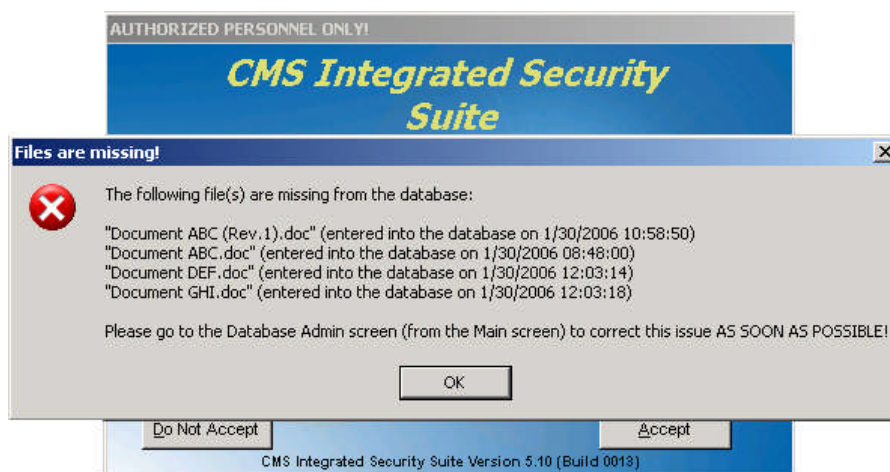
Available Documents		New Document	Supporting Documents	
Name	Posted		Name	Status
Document DEF.doc	01/30/2006	Add Document	Document ABC.doc	Retired on (0
			Document GHI.doc	Retired on (0

Since changes were made in the form, the **Close w/o Saving** button is now active. Selecting **Close w/o Saving** exits the form without saving the supporting document addition(s). Selecting **Save and Close** saves the document addition(s) and exits the form. Both buttons return the user to the original calling security element form (e.g., **Self-Assessment** form).

4.7 Documentation Errors

As mentioned in the Chapter 3.0 introduction, upon opening, the CISS may display the following **Files are missing!** dialog message over the CISS “WARNING” statement. This dialog message displays whenever the CISS has determined that supporting documentation previously attach to the CISS are missing (e.g., files are moved or deleted from their original CISS stored location). Since this is a critical error, the CISS will continue to display this message multiple times while accessing various program options.

Figure 4-18. CISS Files are missing! dialog message



4.7.1 Correcting Missing Documentation Errors

To correct missing documentation errors and stop the **Files are missing!** dialog message from displaying:

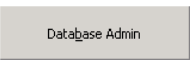
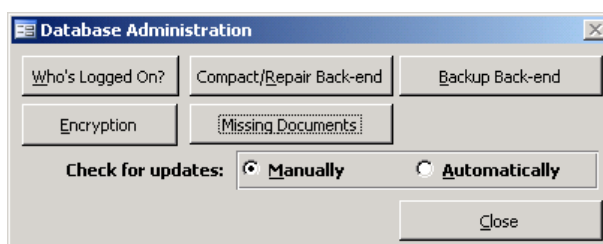

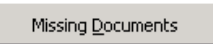
- a. Selecting the  button from the Application Control region of the main menu (Figure 3-3) displays the following dialog.

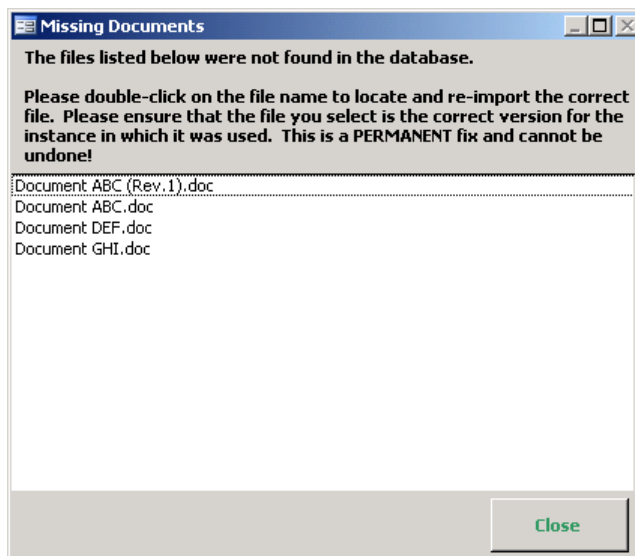
Figure 4-19. Database Administration dialog



- b. Selecting  returns to the main menu, while selecting  opens the following **Missing Documents** dialog.

NOTE: The remainder of the **Database Administration** dialog/menu buttons and options are explained in Chapter 13.0.

Figure 4-20. Missing Documents dialog




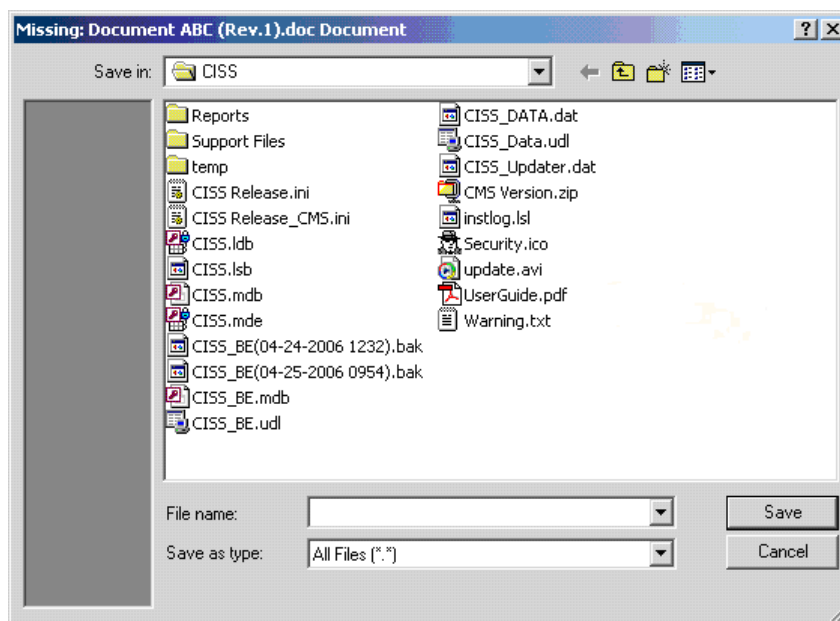
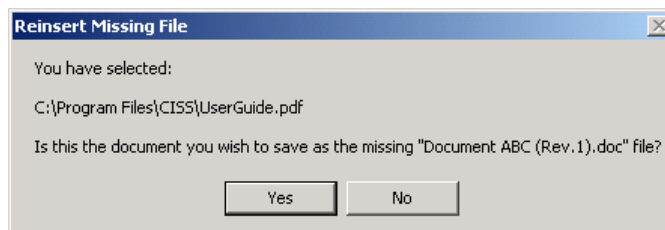
- c. Selecting  returns to the **Database Administration** dialog (Figure 4-19). Double-clicking on a file name listed in the dialog, selects it and opens the following **Missing: [file name] Document** dialog with the selected document file name included in the dialog title area (i.e., “Document ABC (Rev.1).doc”).

Figure 4-21. Missing: [file name] Document dialog



- d. Selecting  returns to the **Missing Documents** dialog (Figure 4-20). Otherwise, locate and select the desired file name. Selecting  opens the following dialog.

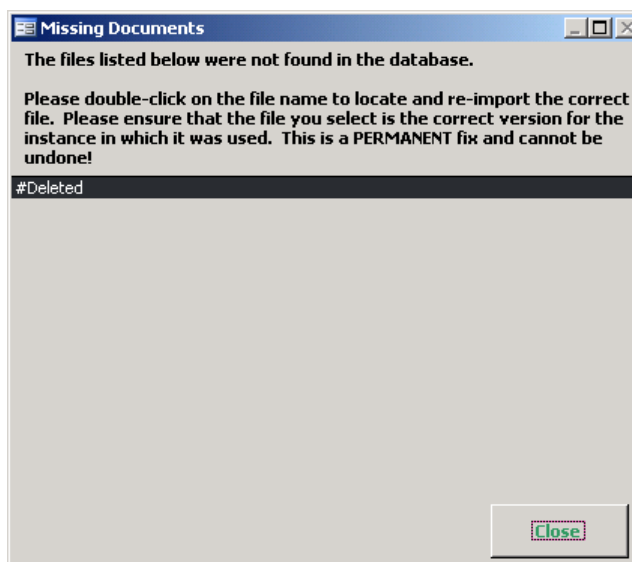
Figure 4-22. Reinsert Missing File dialog



WARNING: The document file name displayed in the above dialog replaces the missing document. This selection cannot be undone once it has been confirmed with , so review this file name before confirming the selection.

- e. Selecting returns to the **Missing Documents** dialog (Figure 4-20). Selecting imports the selected document into the CISS and returns to the **Missing Documents** dialog.
- f. Return to step c. above to continue locating and reinserting all missing document files. When all files have been reinserted into the CISS, the **Missing Documents** dialog no longer displays any missing document file names and the CISS will no longer display the **Files are missing!** dialog message.

Figure 4-23. Missing Documents dialog

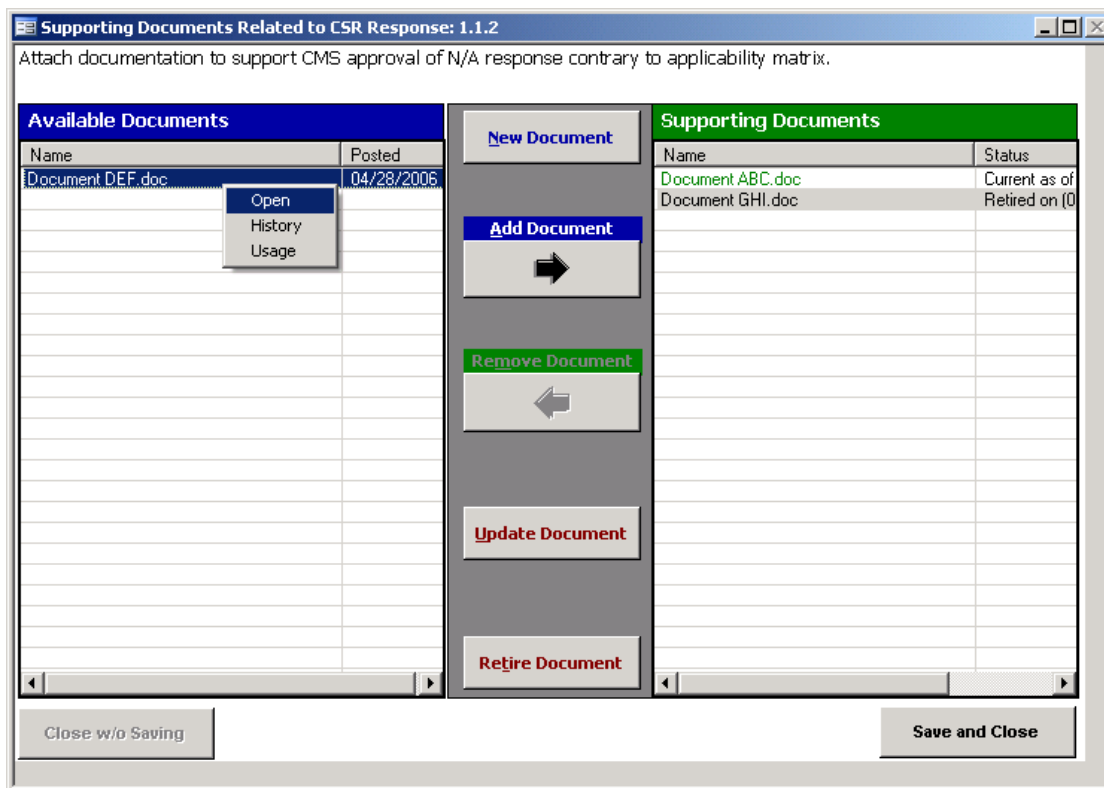


- g. Selecting in the above dialog returns to the **Database Administration** dialog (Figure 4-19).

4.8 Context Menus

The **Supporting Documents** form uses its own pop-up context menu options. Right-clicking on any document name in either the “Available Documents” or “Supporting Documents” area displays the following pop-up menu:

Figure 4-24. Supporting Documents form pop-up menu



These pop-up menu options are specific to the **Supporting Documents** form and are not the same menu options explained in section 3.1.5.3. The **Supporting Documents** form menu options and functions are the same in both the “Available Documents” and “Supporting Documents” areas. However, the pop-up menu options are not activated for any new document(s) until after **Save and Close** is selected to save the document.

The following summarizes the **Supporting Documents** form pop-up menu options and functions:

Figure 4-25. Supporting Documents form pop-up menus

Pop-up Selection	Function
Open	Opens the selected supporting document (see CAUTION below).
History	Displays a chronicle of the selected document, including any updates to the selected document.
Usage	Displays a listing of which Findings and/or CSRs the selected document supports.

CAUTION: Attempting to “Open” some file extension types (e.g., exe, com, bat, js) executes (i.e., runs) the selected file instead of opening it. This is a potentially dangerous situation if the wrong file (i.e., executable file) was added to the **Supporting Documents** form and then the “Open” option was selected for that file. Whenever an executable file type is selected to be opened, the following caution displays:

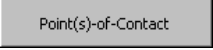
Figure 4-26. Supporting Documents form Open caution message



Selecting returns to the **Supporting Documents** form while selecting may potentially execute the selected file. To remove an executable supporting document file, refer to section 4.4.



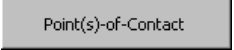

5.0 Points-of-Contact (POCs)






Each POC record in the CISS contains all the information relating to a specific individual, no matter what CISS security oversight element is linked to that individual. However, before any POC(s) can be linked to any CISS security element (i.e., Self-Assessments, Audits, Weaknesses, Findings, Action Plans), the POC record must already exist in the CISS. POCs can always be linked to (or associated with) CISS security elements after the fact, but the preferred method is to create all potential POCs before working on other CISS activities. POC assignments should be included for all individuals responsible for, or assisting with the completion, review, or approval of any CISS-related security element action or activity.

As described in section 3.1, one of the major-level nodes in the Treeview region is a “Points-of-Contact” node (Figure 3-4). In addition, the Component region of the main menu includes a  button (Figure 3-4). Either of these CISS main menu interfaces can be used to open POC records in the CISS application. This Chapter explains the mechanics of maintaining POC records and links in the CISS.

5.1 Creating a New POC Record

To create a new POC record, use either of the following methods to open the **Points-of-Contact** form (Figure 5-2):


- a. Right-click the Treeview region “Points-of-Contact” major-level node and select “Add” from the pop-up menu (refer to section 3.4.2). This opens a new blank form in ADD mode (refer to section 3.3). Selecting  and  closes the form *without* saving the new record and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  opens a new blank form in ADD mode.



Selecting  before selecting  closes the form *without* saving the new record and returns to the CISS main menu. After selecting  to open a new record, selecting  returns the form to READONLY mode *without* saving the new record. Selecting  closes the form and returns to the CISS main menu.

To complete the **Points-of-Contact** form, proceed to section 5.4.

5.2 Opening a POC Record







To open an existing POC record, use either of the following methods to open the **Points-of-Contact** form (Figure 5-2):

- a. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.1.5.1). Double-click the desired POC name node to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

5.3 Editing a POC Record

To edit an existing POC record, use either of the following methods to open the *Points-of-Contact* form (Figure 5-1):

- a. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.4.2). Right-click the desired POC name node and select “Edit” from the pop-up menu. This opens the selected POC form in EDIT mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.1.5.1). Double-click the desired POC name node to open the form in READONLY mode (refer to section 3.3). Selecting  changes the form to EDIT mode. Selecting  closes the form and returns to the CISS main menu.
- c. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired POC record (refer to section 3.2). Selecting  changes the form to EDIT mode. Selecting  closes the form and returns to the CISS main menu.

To modify the *Points-of-Contact* form data, proceed to the next section, 5.4.

5.4 Completing the POC Form

Refer to section 3.3, to ensure that the *Points-of-Contact* form is in the proper mode. To add a new POC record, the form must be in ADD mode; to edit an existing POC record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified.

Although the following figure displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes. In READONLY mode, the form fields cannot be modified. Only the form fields in the non-blue highlighted area depicted in the following figure can be edited or modified while in EDIT or ADD mode. And, the information in the blue highlighted area can only be edited or modified while in READONLY mode (refer to section 5.5).

Figure 5-1. Points-of-Contact form EDIT mode

5.4.1 Last and First Name Fields

The “Last Name” and “First Name” fields are required fields, so they must be completed before the form can be saved.

5.4.2 Email Field

The “Email” field is not required but when filled-in, it is formatted as an Email address link. Double-clicking this Email link uses the system default Email application to create a new message addressed to that individual. No validity checks can be performed on this field, so it is up to the user to ensure the Email address is correct before sending any messages using this field.

5.4.3 Phone, Ext., and Fax Fields

The “Phone” and “Fax” fields are not required but when filled in are preformatted for telephone numbers [i.e., (123) 555-1212] and the “Ext.” field is a maximum 5-digit field.

5.4.4 Job Function Field

The “Job Function” field is a required field that must be completed before the form can be saved. This field should specify the job function, position, title, or role the POC fulfills at the Business Partner (e.g., SSO, Security Administrator, VP of Medicare Operations, Programmer, etc.). There are no CISS-specific terms or job functions for this field. The job function must be determined by the Business Partner.

5.4.5 Notes Field

The “Notes” field is not required, but input whatever descriptive notes are deemed necessary for the POC. These notes are not reported outside the Business Partner and are there for informational purposes only.

5.4.6 Finalizing the Form

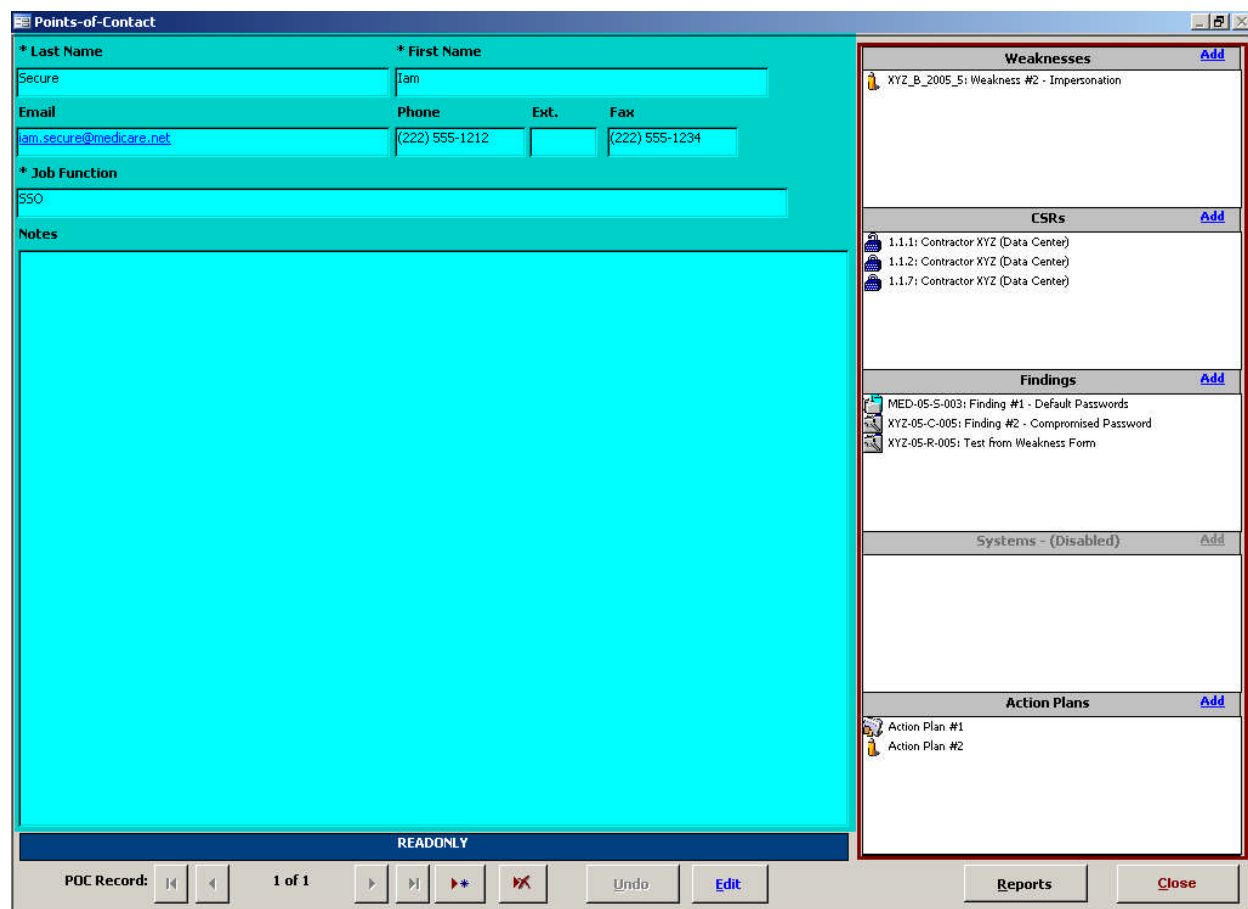
When done completing the form fields, selecting **Save** saves the form information, while selecting **Undo** closes the form *without* saving any of the new or modified information. There is no confirmation or warning message if **Undo** is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode. To make changes to the selected POC links or associations, proceed to the next section, 5.5.

Selecting **Close** closes the *Points-of-Contact* form and returns to the CISS main menu.

5.5 POC Links or Associations

Figure 5-2 displays a *Points-of-Contact* form in READONLY mode. In READONLY mode, the form fields in the blue highlighted area depicted in Figure 5-2 cannot be modified. Only the non-blue highlighted dialog window areas are selectable. These dialog windows display all existing links between the selected POC and Weakness, CSR, Finding, and Action Plan security element records, if any.

Figure 5-2. Points-of-Contact form READONLY mode



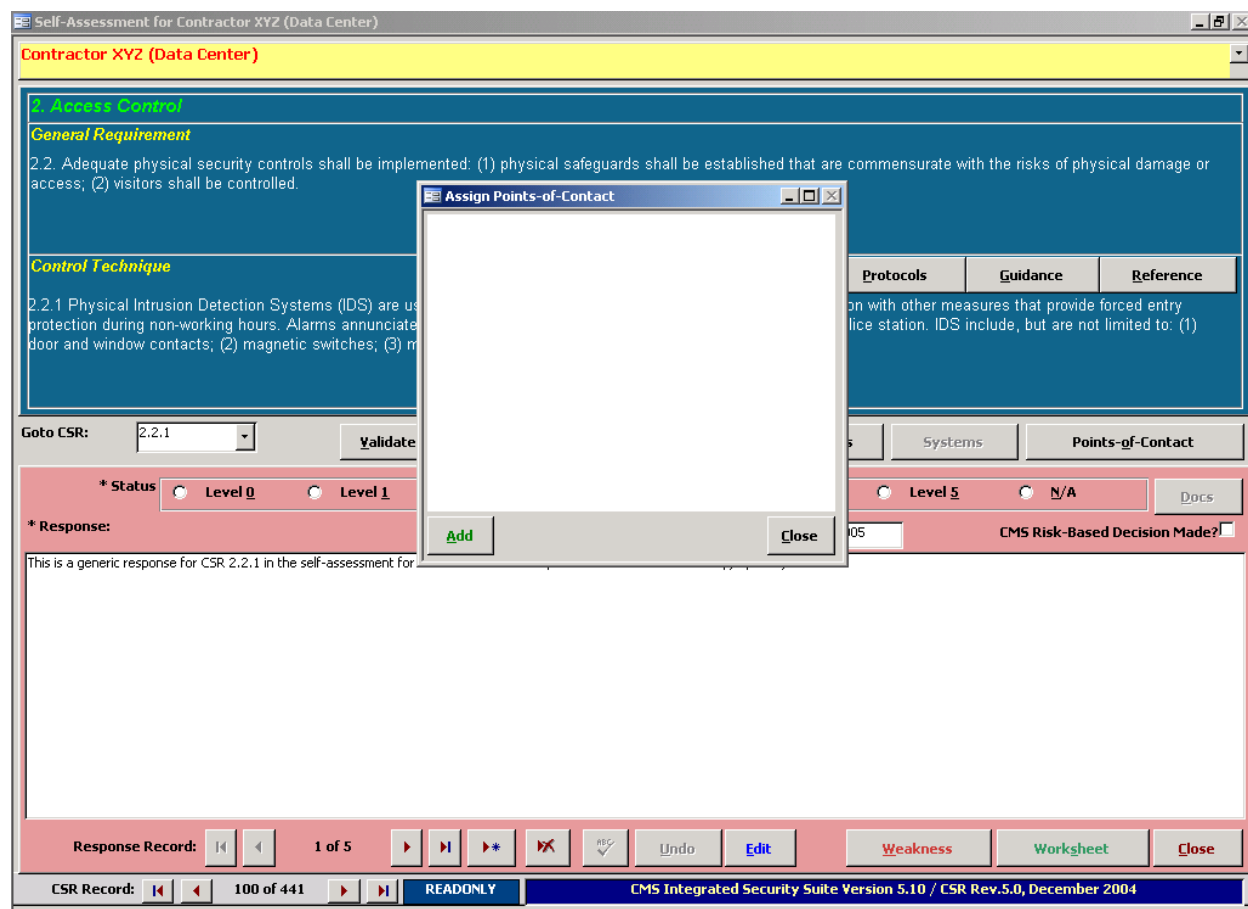
POC links or assignments can be added to individual security elements by following the instructions in next section, 5.5.1.

5.5.1 Adding Individual POC Links to Other Forms

POC links can be made to other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). POC links can also be made from the **Points-of-Contact** form dialog windows using the **Add** link in the dialog windows. Clicking the **Add** link in any of these dialog windows while in READONLY mode opens the selected security element form.

For example, clicking the **CSRs** dialog window **Add** link opens the **Self-Assessment** form in READONLY mode at CSR 1.1.1. After using the record navigation controls (or for CSR only, the “Goto CSR” drop-down dialog window) to navigate to the desired record (e.g., CSR 2.2.1), selecting **Point(s)-Of-Contact** from the respective form opens the following **Assign Points-of-Contact** dialog.

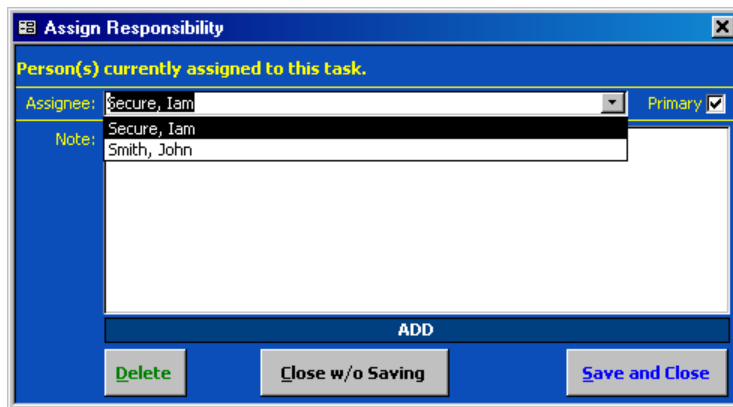
Figure 5-3. Assign Points-of-Contact dialog



Selecting **Close** closes the **Assign Points-of-Contact** dialog and returns to the original calling security element form (e.g., **Self-Assessment** form). Selecting **Add** opens the **Assign Responsibility** dialog where selecting the “Assignee” drop-down menu allows the user to select a POC from a list of available POCs (i.e., all existing POC records) (Figure 5-4). In this example,

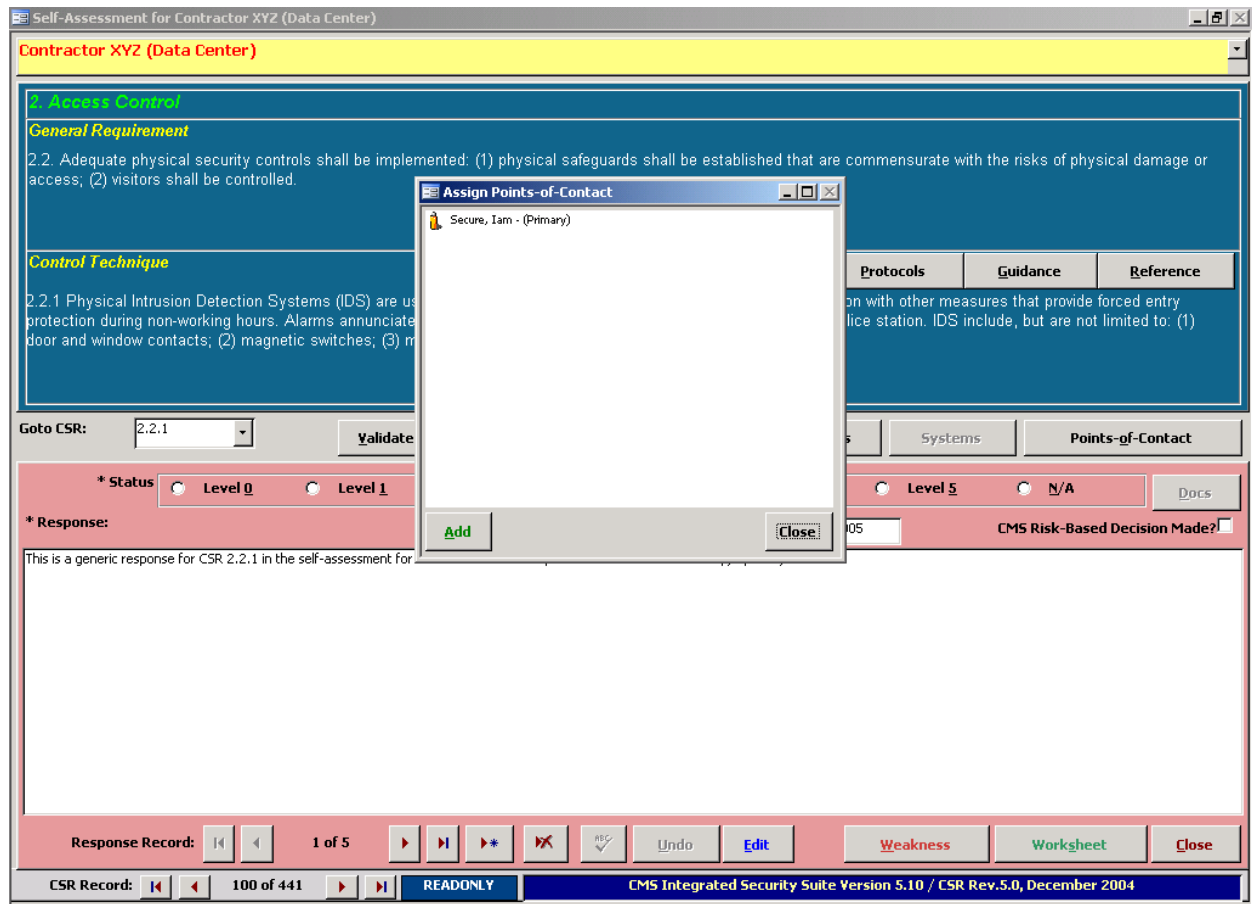
“Iam Secure” was selected for assignment to the applicable CSR (e.g., CSR 2.2.1). Note that the “Primary” field check box is also selected (refer to section 5.6, for information on this field).

Figure 5-4. Assign Responsibility dialog



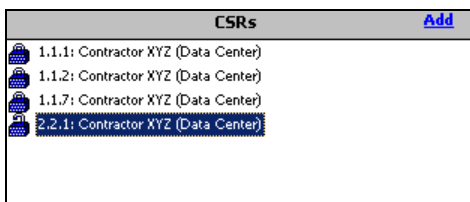
After the POC selection is made, selecting **Save and Close** saves the POC link assignment and closes the **Assign Responsibility** dialog. Selecting **Close w/o Saving** closes the dialog *without* making the POC link assignment. Both buttons return to the following **Assign Points-of-Contact** dialog with the new POC assignment displayed in its dialog window, if applicable.

Figure 5-5. Assign Points-of-Contact dialog with POC assignment



Selecting **Close** closes the *Assign Points-of-Contact* dialog and returns to the original calling security element form (e.g., *Self-Assessment* form). Selecting **Close** closes the security element form and return to the *Points-of-Contact* form (Figure 5-7). Note that the following *CSRs* dialog window now includes the new link assignment to CSR 2.2.1.

Figure 5-6. POC CSRs dialog window assignment

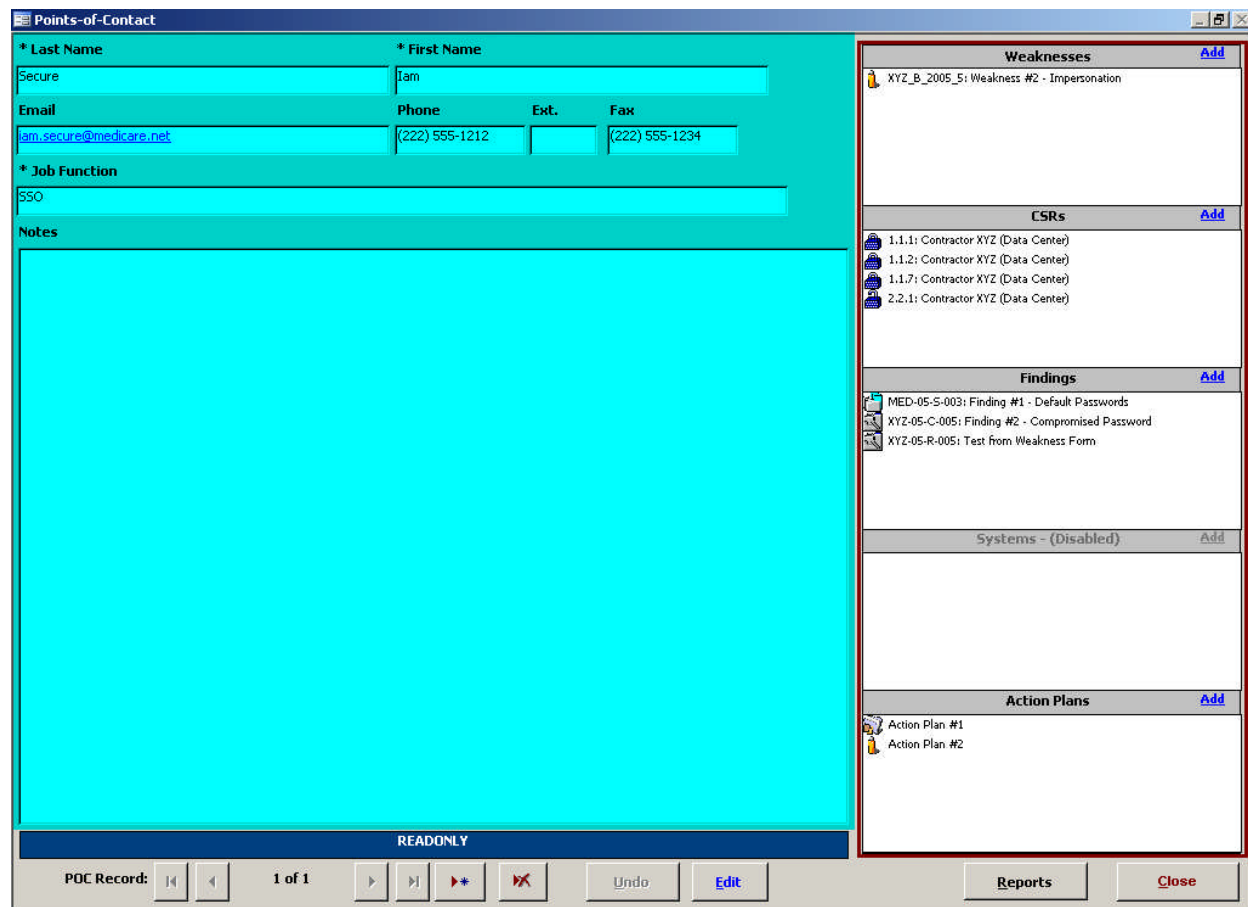


Selecting **Close** closes the *Points-of-Contact* form and returns to the CISS main menu.

5.5.2 Removing POC Links to Other Forms

POC links can be removed from other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). POC links that are listed in any *Points-of-Contact* form dialog window (Figure 5-7) can also be removed. Double-clicking the desired security element title in any dialog window while in READONLY mode selects the security element and opens its respective form.

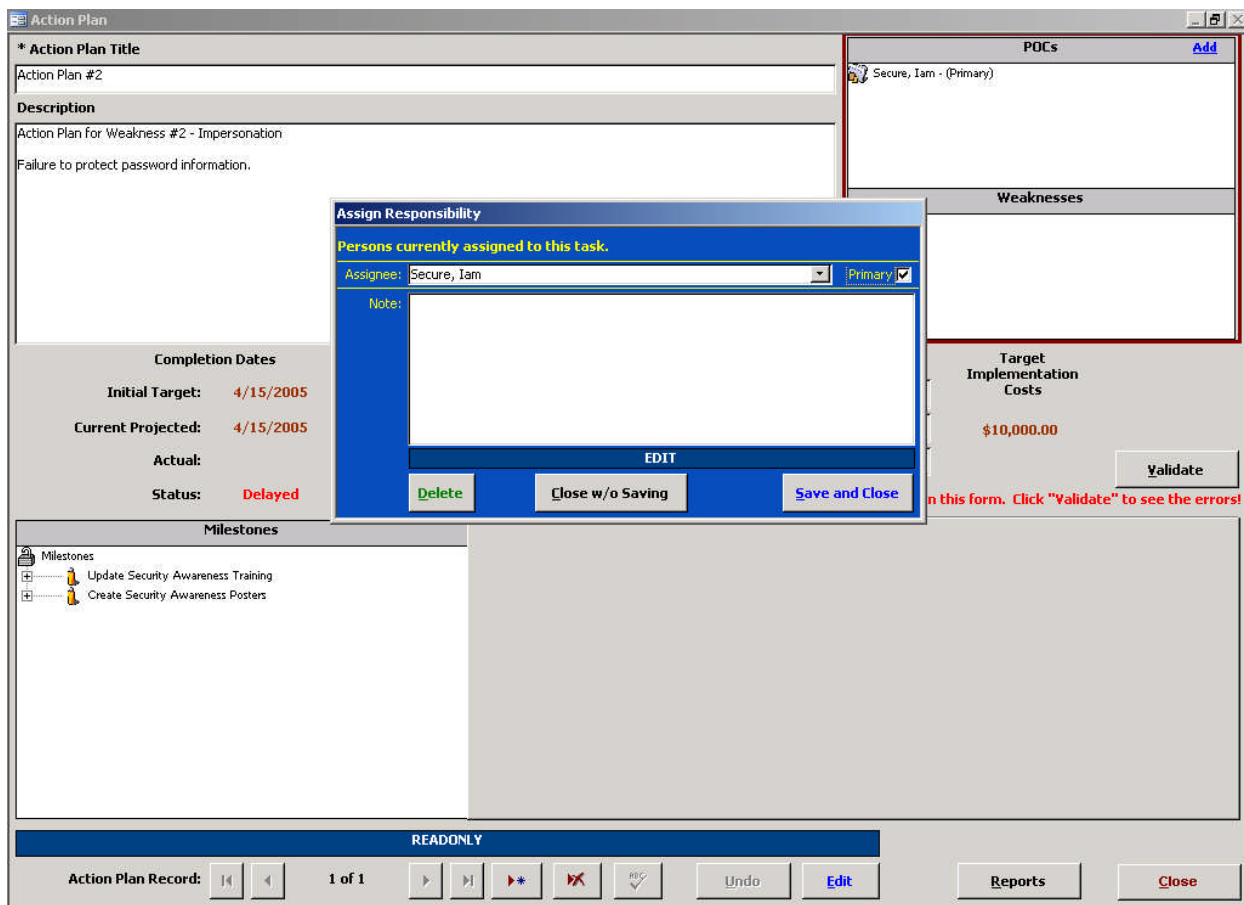
Figure 5-7. POC CSRs dialog window assignment



For example, double-clicking the “Action Plan #2” title in the **Action Plans** dialog window link opens the respective **Action Plan** form in READONLY mode. Double-clicking the “Secure, Iam” name in the **POCs** dialog window opens the selected POC **Assign Responsibility** form (Figure 5-8).

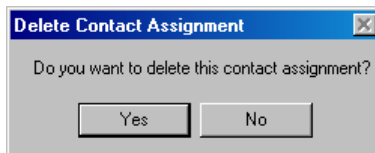
Selecting either **Close w/o Saving** or **Save and Close** closes the form *without* making any POC link assignment changes. Both buttons return to the original calling security element form (e.g., **Action Plan** form). Selecting **Close** closes the security element form and returns to the **Points-of-Contact** form.

Figure 5-8. Assign Responsibility dialog



Selecting **Delete** displays the following warning message.

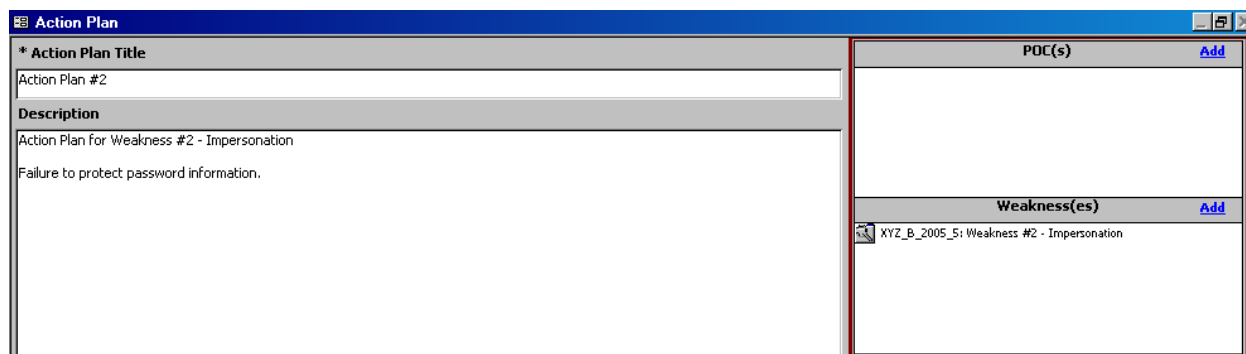
Figure 5-9. Delete Contact Assignment warning message



Selecting **No** exits the warning dialog and returns to the selected security element form (e.g. Action Plan #2) *without* removing the POC link. Selecting **Yes** *removes* the POC link *without* any further warnings or confirmations, and exits to the selected security form. Note that

the “Secure, Iam” POC link assignment has been deleted from the following Action Plan #2 POCs dialog window.

Figure 5-10. Action Plan form POCs dialog window assignment



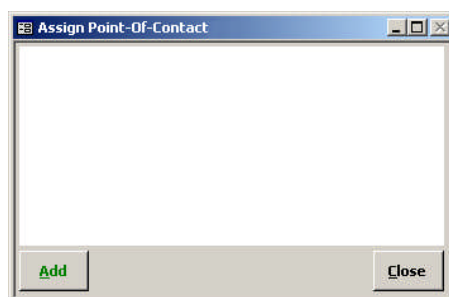
Selecting **Close** closes the original calling security element form and returns to the **Points-of-Contact** form. Selecting **Close** again closes the **Points-of-Contact** form and returns to the CISS main menu.

5.6 Assigning a Primary POC

Since multiple POCs may be assigned to CISS activities or functions, one of the POCs must be designated as the Primary POC. If only one POC is assigned to a CISS activity or function, that POC must be designated the Primary POC. This should be the person or job function that has overall responsibility for completing any required actions.

Selecting **Point(s)-Of-Contact** on any security element form where it is available displays the following **Assign Points-of-Contact** form.

Figure 5-11. Assign Points-of-Contact form



Selecting **Add** opens the **Assign Responsibility** dialog. Selecting the Assignee drop-down menu allows the user to select a POC from a list of available POCs (i.e., POC records that already existed.). In the Figure 5-12 example, John Smith was selected and is being assigned to this task. Note that the Primary “check box” is not filled-in. To designate this POC as the Primary POC for this task, click in the Primary box area.

Figure 5-12. Assign Responsibility dialog without Primary assignment selected

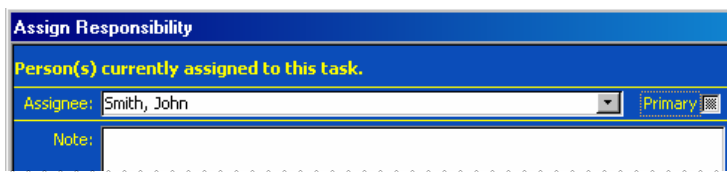
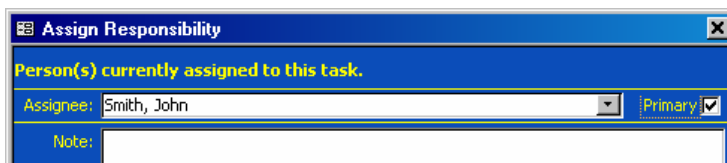


Figure 5-13. Assign Responsibility dialog with Primary assignment selected



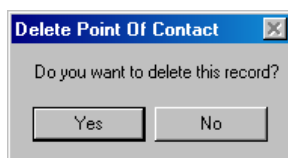
After completing the POC selection process, selecting the **Save and Close** completes the POC assignment.

5.7 Deleting a POC Record

To delete a POC, open the desired POC record using either of the following methods to open the **Points-of-Contact** form (Figure 5-2):

- a. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.1.5.1). Double-click the desired POC name node to open the form in READONLY mode (refer to section 3.3). Selecting **Close** closes the form and returns to the CISS main menu. Selecting **X** displays the **Delete Point of Contact** warning message (Figure 5-14).
- b. Select the Component region **Point(s)-of-Contact** button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired POC record (refer to section 3.2). Selecting **Close** closes the form and returns to the CISS main menu. Selecting **X** displays the following Delete Point of Contact warning message.

Figure 5-14. Delete Point of Contact warning message



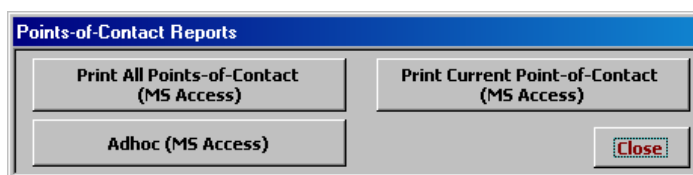
Selecting **No** in this warning message exits from the **Delete Point of Contact** warning and returns to the **Points-of-Contact** form *without* deleting the POC. However, selecting **Yes** *deletes* the selected POC, as well as all links to the selected POC, *without* any further warnings or confirmations. Selecting **Close** in the resultant form exits to the main menu.

5.8 POC Reports

MS Excel® PivotTable reports (refer to section 3.11) can be accessed by selecting the **Pivot Reports** button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Points-of-Contact Reports** menu can be accessed from the Treeview

region using pop-up menus or from the *Points-of-Contact* form using the **Reports** button (Figure 5-1).

Figure 5-15. Points-of-Contact Reports menu



NOTE: The **Print Current Point-of-Contact (MS Access)** button (Figure 5-15) is active only if the report selection is based on a single POC selection. For example, double-clicking a specific POC or selecting the “Reports” pop-up menu from a specific POC results in an active button because a “current” POC has been identified. However, when selecting the “Reports” pop-menu from the “Points-of-Contact” major-level node, the button is inactive because no “current” POC has been identified.

Any of the following methods can be used to open the *Points-of-Contact Reports* menu (Figure 5-15):

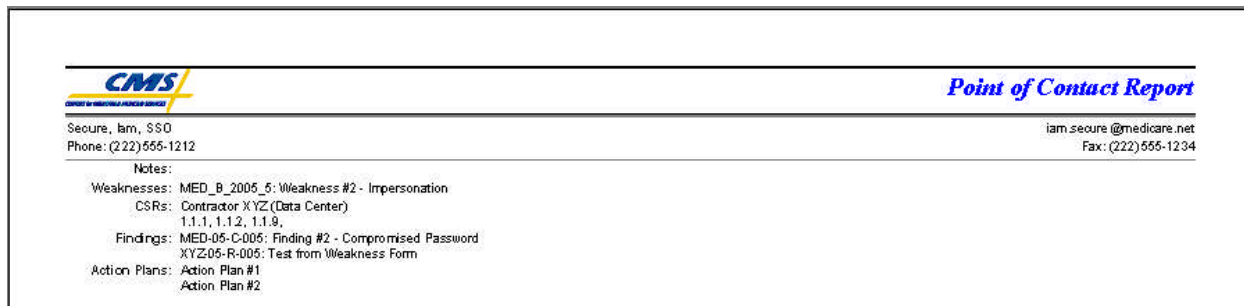
- a. If the *Points-of-Contact* form is already open, use the form record navigation buttons to navigate to the desired POC record (refer to section 3.2), if necessary. Then selecting **Reports** (Figure 5-1) opens the report menu.
- b. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.1.5.1). Double-click the desired POC name node to open the POC record. Then selecting **Reports** (Figure 5-1) opens the report menu.
- c. Expand the Treeview region “Points-of-Contact” major-level node or any security element node with a lower-level “Points-of-Contact” node (refer to section 3.4.2). Right-click the “Points-of-Contact” node or any POC name node in any security element to display a pop-up menu that includes a “Reports” option. (Refer to Figure 3-11 for an expansion of all Treeview nodes and their available pop-up menu options.) Selecting “Reports” from the pop-up menu opens the report menu.

5.8.1 Print Current Point-of-Contact (MS Access)

Selecting **Print Current Point-of-Contact (MS Access)**, if activated, from the *Points-of-Contact Reports* menu (Figure 5-15) generates a report that includes the selected POC’s information, and links or responsibilities to CISS security elements. Only the current or selected POC is included in the report.

Once created, a report similar to following example is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 5-16. Example Current POC report



Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 5-15).

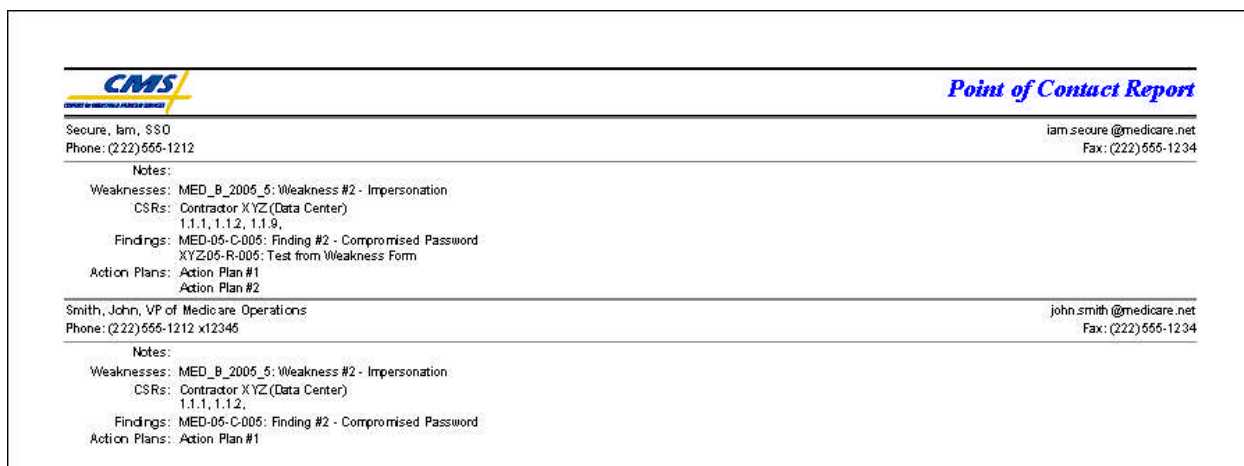
Selecting **Close** in the *Points-of-Contact Reports* menu closes the menu and returns to the original starting point (i.e., CISS main menu or *Points-of-Contact* form).

5.8.2 Print All Points-of-Contact (MS Access)

Selecting **Print All Points-of-Contact (MS Access)** from the *Points-of-Contact Reports* menu (Figure 5-15) generates a report that includes all POCs contained in the database. The report includes all POC information, and their links or responsibilities to CISS security elements. This POC report is formatted so each POC starts printing on a new page.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 5-17. Example All POCs report



Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 5-15).

Selecting **Close** in the *Points-of-Contact Reports* menu closes the menu and returns to the original starting point (i.e., CISS main menu or *Points-of-Contact* form).

5.8.3 Adhoc (MS Access)

The Adhoc reports feature allows the user to generate a customized report that is based on user-selected filters (or parameters) and includes only user-specified information. For example, an Adhoc report can be created that includes only the POCs assigned to specific security elements (e.g., Finding, Weakness) or a report can be created that includes only the POCs assigned to specific CSRs. These examples are only a small sample of how reports can be customized to meet specific needs. Although these reports include only the POCs based on user-specified filters, all of the contact information is included for each POC included in the report. The POCs are printed one after the other with no page breaks between each POC.

5.8.3.1 Adhoc Report Selection

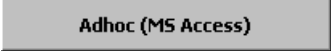
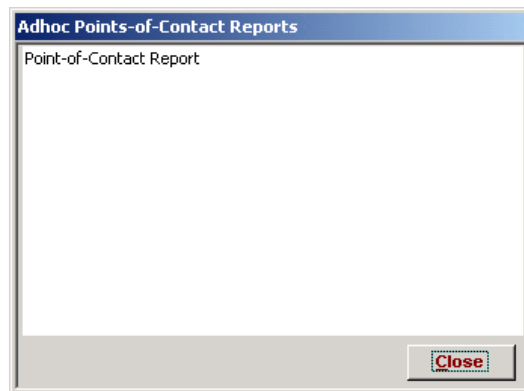

Selecting  from the *Points-of-Contact Reports* menu (Figure 5-15) opens the following *Adhoc Points-of-Contact Reports* dialog with the following Adhoc report selection.

Figure 5-18. Adhoc Points-of-Contact Reports dialog



Selecting  closes the dialog and returns to the *Points-of-Contact Reports* menu (Figure 5-15).

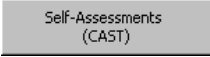
5.8.3.2 Adhoc Report Filter Selection

The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

6.0 Self-Assessments


An important element of ensuring an organizations’ IT security health is performing routine Self-Assessments of the Business Partners’ security program. The CISS application facilitates the performance and maintenance of annual Self-Assessments, especially when multiple Self-Assessments are required (e.g., one per Medicare contract).

New with the CISS versus the former CAST application is that all non-compliant CSRs result in a security Weakness and a corresponding Action Plan and Milestones to remediate the Weakness (versus creating Safeguards in the former CAST). In addition, all Weaknesses resulting from Audit or Review Findings must be linked (associated) with a corresponding non-compliant CSR. The progress towards completing the Action Plans associated with each Weakness is updated and submitted to CMS using the POA&M reporting process in the CISS application (refer to Chapters 7.0, 8.0, and 12.0).

As described in section 3.1, one of the major-level nodes in the Treeview region is a “Self-Assessments (CAST)” node (Figure 3-4). In addition, the Component region of the main menu includes a  button (Figure 3-4). Either of these CISS main menu interfaces can be used to open Self-Assessments and their corresponding CSR records in the CISS application.

This Chapter explains the mechanics of using the CISS to document and manage Self-Assessments and their respective CSR responses. Consult BPSSM Appendix A for guidance on completing the new CSR response status effectiveness levels and response comments. Users are strongly encouraged to become familiar with all the criteria and guidance contained in BPSSM Appendix A *before* attempting to use the CISS to complete Self-Assessments.

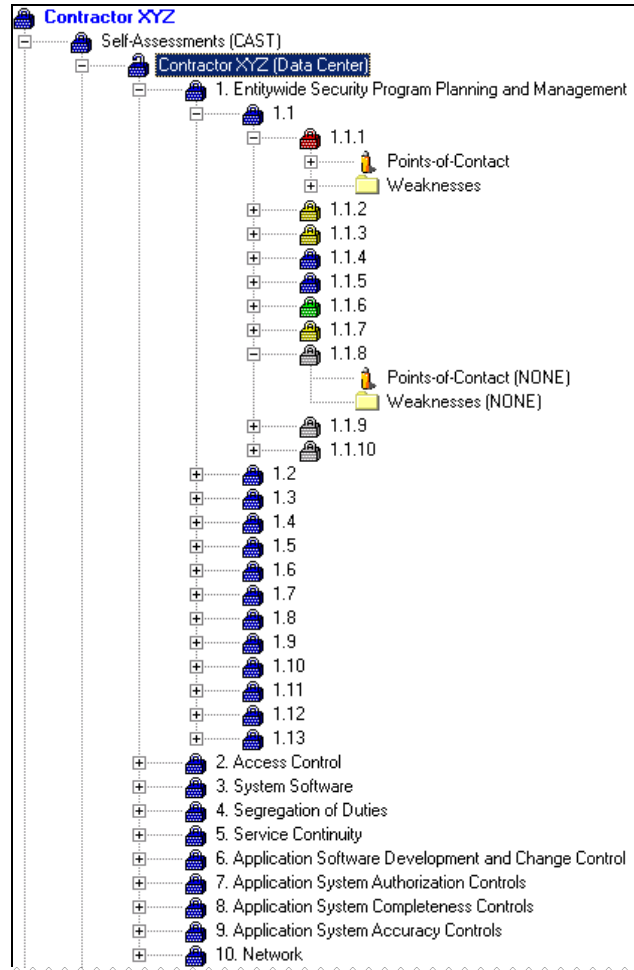
6.1 Self-Assessments and Lower-Level CSR Nodes

Each Self-Assessment title displayed in the Treeview region under the “Self-Assessments (CAST)” major-level node can be expanded by clicking its corresponding  icon [e.g., “Contractor XYZ (Data Center)” in Figure 6-1]. When the Self-Assessment name node is expanded, separate lower-level CSR-related nodes are displayed. When their respective nodes are expanded, the following CSR-related information displays in the Treeview:

- **1st Level** – The 10 Major CSR Categories (e.g., Category “1. Entitywide Security Program Planning and Management” in Figure 6-1).
- **2nd Level** – The CSR General Requirement Categories (e.g., General Requirement “1.1” in Figure 6-1).
- **3rd Level** – Individual CSR Control Techniques (e.g., CSRs “1.1.1” – “1.1.10” in Figure 6-1).
- **4th Level** – CSR links to POCs and Weaknesses, if any (e.g., CSR “1.1.1” in Figure 6-1). If there are no POCs or Weaknesses linked to a CSR, “(NONE)” displays after their nodes (e.g., “1.1.8” in Figure 6-1).

Any Self-Assessment node, at any level, can be selected (i.e., opened) by double-clicking the applicable node. In addition, right-clicking selected nodes activates a pop-up menu that allows specific functions to be performed (refer to section 3.1.5.3).

Figure 6-1. Treeview Self-Assessment and CSR nodes



The upper-level Treeview CSR nodes (i.e., Major and General Requirement Category nodes) always display with a blue node icon (🔒). However, the individual CSR node icons display in different colors to indicate the response status assigned to the CSR. The CSR node icon color legend is:

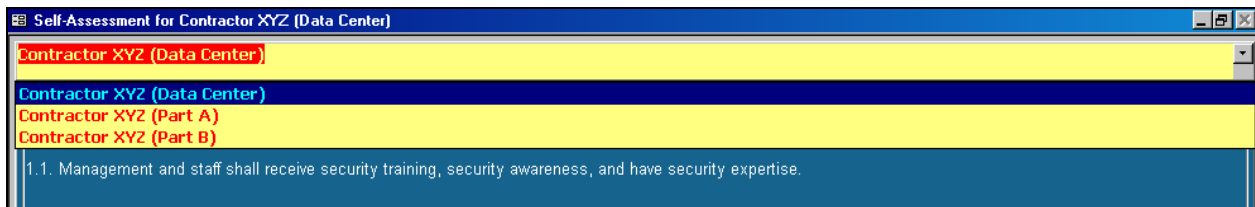
- **Green** – “Level 5” or “N/A” response status that is in agreement with the Applicability matrix (e.g., CSR “1.1.6” in Figure 6-1)
- **Blue** – “Level 3” or “Level 4” response status (e.g., CSRs “1.1.4” and “1.1.5” in Figure 6-1)
- **Yellow** – “Level 1,” “Level 2,” or “N/A” response status that is not in agreement with the Applicability matrix (e.g., CSRs “1.1.2,” “1.1.3,” and “1.1.7” in Figure 6-1)
- **Red** – “Level 0” response status (e.g., CSR “1.1.1” in Figure 6-1)
- **Grey** – Response status not yet assigned. (e.g., CSRs “1.1.8,” “1.1.9,” and “1.1.10” in Figure 6-1)

6.2 Self-Assessment Form Navigation Controls

There are multiple methods to navigate to a specific Self-Assessment, CSR, or CSR Response within the **Self-Assessment** form (Figure 6-5):

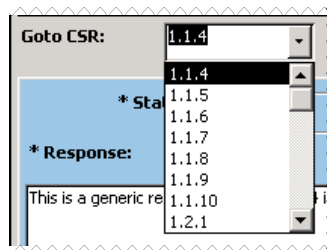
- a. The form includes a drop-down menu to select or change the selection of the currently active Self-Assessment title. If the desired Self-Assessment title is not active, as indicated by the Self-Assessment title displayed in the upper yellow area of the following figure, use the drop-down menu at the end of this title field to select the desired Self-Assessment title. Selecting **Close** closes the form and returns to the CISS main menu.

Figure 6-2. Self-Assessment form Self-Assessment Title drop-down menu



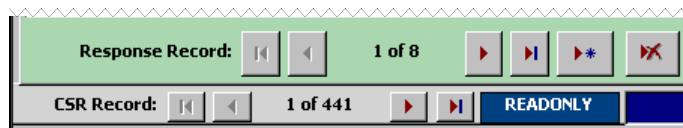
- b. The form includes a “Goto CSR” drop-down menu (Figure 6-3). To navigate to a different CSR record, type the desired CSR number into the “Goto CSR” input area or select the desired CSR number from the drop-down menu. Use the scroll bar to view and select other CSR numbers.

Figure 6-3. Goto CSR drop-down menu



- c. Section 3.2, explains how to use the form record navigation buttons to move through form records. The same record navigation controls apply to this form except that this form has two sets of navigation controls (Figure 6-4)—one for each CSR Response Record (e.g., 1 of 8) and one for each CSR Record (e.g., 1 of 441).


Figure 6-4. Response Record and CSR Record navigation buttons



To navigate to a different CSR, use the “CSR Record” navigation controls. To navigate to a different CSR Response record for the currently selected CSR (e.g., to view an older response for the currently selected CSR), if applicable, use the “Response Record” navigation controls.

6.3 Unlocking Self-Assessment Records

When existing Self-Assessment data is imported into the CISS application from a CAST back-end database, the CISS Self-Assessment records (i.e., CSR responses) are locked; they cannot be modified. The same is true when a Self-Assessment is submitted to CMS—the CISS application locks the Self-Assessment records to prevent changes (refer to Chapter 12.0).

When a Self-Assessment CSR record is locked, the **Self-Assessment** form background color for the “Date Entered” and “Response” fields is yellow instead of white, and the “Status” selections are disabled as in the following figure. In addition, the form is in READONLY mode and the  button on the form is disabled.

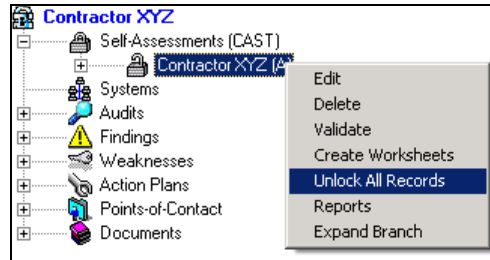
NOTE: The **Self-Assessment** form is used to display and enter CSR information. There is no separate “CSR form.”

Figure 6-5. Locked Self-Assessment form record

6.3.1 Unlocking All Self-Assessment CSR Response Records

To unlock all the Self-Assessment records, such as when preparing to complete the annual Self-Assessment process, expand the Treeview region “Self-Assessments (CAST)” major-level node and right-click the desired Self-Assessment name node [e.g., Contractor XYZ (A)] to open the following pop-up menu. Select “Unlock All Records” from the pop-up menu and the CISS will “unlock” the selected Self-Assessment CSR response records.

Figure 6-6. Treeview Self-Assessment node “Unlock All Records” pop-up menu



When the CISS “unlocks” Self-Assessment CSR response records, it creates unlocked copies of the final CSR response records submitted to CMS (or imported from CAST). The “old” CSR response records remain untouched and locked in the Self-Assessment, and the status and response information is copied into new unlocked records. The only change made from the “old” to the “new” CSR response record is the “Date Entered” field is updated to reflect the date that the records were “unlocked.”

To demonstrate this, review Figure 6-5 with the locked CSR yellow background date and response areas. Note the date and CSR “Response Record” indicates 1 of 7 records. Now review the unlocked record in Figure 6-7 with the white background date and response areas. The “Date Entered” field has changed and the CSR “Response Record” now indicates 1 of 8 records, and the **Edit** button is enabled.

Figure 6-7. Unlocked Self-Assessment form record

Contractor XYZ (A)

Entitywide Security Program Planning and Management

General Requirement

1.1. Management and staff shall receive security training, security awareness, and have security expertise.

Control Technique	Applicability	Protocols	Guidance	Reference
1.1.1 Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).				

Goto CSR: **1.1** **Validate** **There are errors on this form. Click "Validate" to see the errors!** **Reports** **Systems** **Points-of-Contact**

* Status: Level 0 Level 1 Level 2 Level 3 Level 4 Level 5 N/A **Docs**

* Response: Yes No Partial Planned * Date Entered: 5/11/2006 CMS Risk-Based Decision Made?

Formal Security Training includes: (1) awareness training; (2) periodic security reminders; (3) user education concerning virus protection; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential). Corporate Information Security issues special phonemail and e-mail bulletins relating to particular security threats (e.g., new viruses) and security policy and procedures. POC: System Security Management, Training Management

Response Record: 1 of 8 **CSR Record:** 1 of 441 **READONLY** **Undo** **Edit** **Weakness** **Worksheet** **Close**

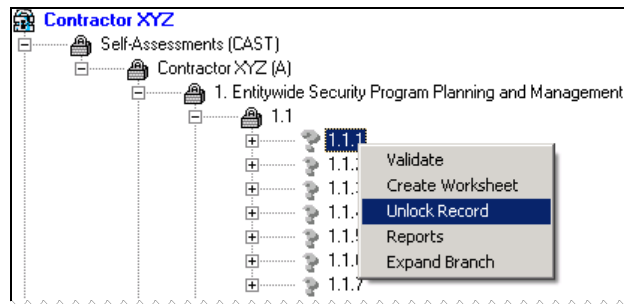
CISS Integrated Security Suite Version 5.10 / CSR Rev.5.0, December 2004

6.3.2 Unlocking Individual CSR Response Records

Individual CSR response records can be unlocked without unlocking all CSR response records included in a Self-Assessment. This might occur if the Business Partner wishes to update a specific CSR response after a Self-Assessment has been submitted to CMS but before the next Self-Assessment preparation cycle (e.g., to record updated response information).

To unlock an individual CSR response record, select the desired CSR node and right-click the CSR node to open the following pop-up menu. Select “Unlock Record” from the pop-up menu to “unlock” only that CSR response record.

Figure 6-8. Treeview CSR node “Unlock Record” pop-up menu



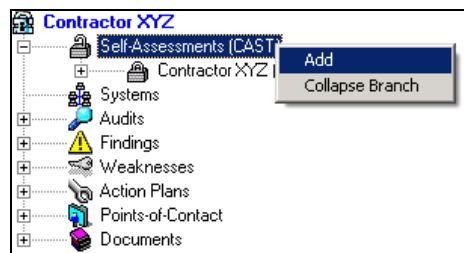
The CISS creates an unlocked copy of the selected CSR response record and the “old” CSR response record remains untouched and locked, as explained in the previous section. Later, when the entire Self-Assessment is selected to be “unlocked” (refer to the previous section), the CISS ignores all CSR response records that are already unlocked and only processes the CSR response records that remain locked.

6.4 Creating a New Self-Assessment

CMS Business Partners should use existing Self-Assessments imported from their CAST or CISS back-end databases when preparing for the next Self-Assessment submittal cycle. New Business Partner Self-Assessments should only be created when there is no existing Business Partner Self-Assessment, such as when splitting an existing combined assessment into separate Self-Assessments or when preparing the initial Self-Assessment for a new contract.

To create a new Self-Assessment, right-click the “Self-Assessments (CAST)” node in the Treeview region and select “Add” in the following pop-up menu.

Figure 6-9. Treeview Self-Assessments (CAST) node “Add” pop-up menu



This opens the following **Add Self-Assessment** form.

Figure 6-10. Add Self-Assessment form

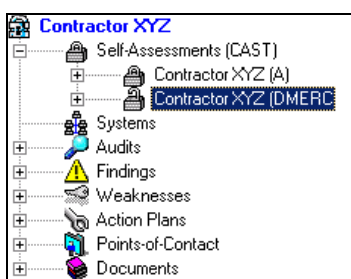
Input the CMS contract Number (e.g., 12345), Self-Assessment Title and contract Type [e.g., Contractor XYZ (Dmerc)], select the Type of Medicare contract from the drop-down menu (e.g., Dmerc) and any desired descriptive information. The “CMS Number,” “Title,” and “Type” fields are required fields and must be completed before the form can be saved. However, this dialog information can be modified later (refer to section 2.4.2).

NOTE: If preparing and submitting separate Self-Assessments for multiple contract types, ensure that each Self-Assessment title is unique by appending the contract type to the Self-Assessment title [e.g., Contractor XYZ (Part A), Contractor XYZ (Part B), etc.].

Selecting **Save and Close** saves the information, closes the dialog, and creates a new Self-Assessment. Selecting **Close w/o Saving** exits the dialog *without* saving the data or creating a new Self-Assessment. Both buttons return to the CISS main menu (Figure 3-4).

If the data entered in the above dialog are saved, the name entered in the form will be included as a lower-level node under the “Self-Assessments (CAST)” major node (Figure 6-11). If the data is not saved, no new Business Partner Self-Assessment will be created. After creating a new Self-Assessment, proceed to section 6.8.

Figure 6-11. Treeview Self-Assessments (CAST) lower-level nodes



6.5 Modifying Self-Assessment Information


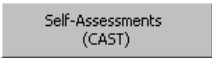
To modify the Self-Assessment contract information (Figure 6-10), refer to section 2.4.2.


6.6 Opening Self-Assessments and CSRs

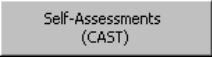
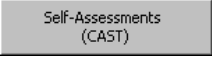
As explained in section 6.1, the Treeview “Self-Assessments (CAST)” major-level node includes several lower-level Self-Assessment and CSR-related nodes (Figure 6-1). These individual nodes can be selected to open specific Self-Assessments, CSR categories, or CSRs.

6.6.1 Opening a Self-Assessment


To open an existing Self-Assessment, use either of the following methods to open the **Self-Assessment** form (Figure 6-15):

- a. Expand the Treeview region “Self-Assessments (CAST)” major-level node (Figure 6-11). Double-click the desired Self-Assessment title [e.g., Contractor XYZ (DMERC)] node to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). If multiple Self-Assessments exist (e.g., multiple contracts), the CISS application opens either: (1) the first Self-Assessment name node listed in the Treeview region when running a new CISS session (i.e., when the CISS is initially opened) or (2) the last active Self-Assessment during the current CISS session (e.g., when a Self-Assessment was already selected).

If the desired Self-Assessment title is not active, as indicated by the Self-Assessment title displayed in the upper yellow area of the form (Figure 6-2), use the drop-down menu at the end of this title field to select the desired Self-Assessment title. Selecting  closes the form and returns to the CISS main menu.

The major difference between using the Treeview region nodes and Component region  button to open Self-Assessments is that by expanding the Self-Assessments Treeview nodes, a specific Self-Assessment, Major CSR Category, CSR General Requirement, or CSR Control Technique can be opened by double-clicking the desired node. Whereas, selecting the  button opens the first listed or last active Self-Assessment at CSR 1.1.1. Then the user must use the “Goto CSR” selection or form record navigation buttons to navigate to the desired CSR record (refer to section 6.2).

6.6.2 Opening a CSR Category or Response

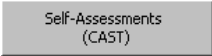
To open the **Self-Assessment** form at a specific CSR category or response, expand the Treeview region Self-Assessment title lower level nodes (refer to Figure 6-1). Double-clicking the desired CSR category or number opens the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.



For example, double-clicking General Requirements Category “1.1” (refer to Figure 6-1), opens the **Self-Assessment** form at CSR 1.1.1 while double-clicking Category “1.5,” opens the form at CSR 1.5.1. Double-clicking Major Category “3. System Software,” opens the form at CSR 3.1.1 while double-clicking CSR “1.1.9,” opens the form at CSR 1.1.9.

6.7 Editing a Self-Assessment/CSR Record

To edit an existing Self-Assessment, use either of the following methods to open the **Self-Assessment** form (Figure 6-15):

- a. Refer to the previous section, 6.6.2, to select and open a specific Self-Assessment, or CSR category or number by double-clicking the desired node. This opens the form in READONLY mode (refer to section 3.3).

- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). If multiple Self-Assessments exist (e.g., multiple contracts), the CISS application opens either the first Self-Assessment name node listed in the Treeview region if running a new CISS session (i.e., when the CISS is initially opened) or the last Self-Assessment accessed during the current CISS session (e.g., if a Self-Assessment was already selected).
- c. If the desired Self-Assessment is not opened, as indicated by the Self-Assessment Title displayed in the upper yellow area of the form (Figure 6-2), use the drop-down menu at the end of the Title field to select a different Self-Assessment.
- d. If the desired CSR is not opened, use the “Goto CSR” selection or form record navigation buttons to navigate to the desired CSR record (refer to section 6.2).

Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.

6.8 New Self-Assessments/CSR Records

When a new Self-Assessment is created (refer to section 6.4) or new CSRs are added to the CISS (i.e., CSRs that did not exist previously), there are no existing CSR response records in the Self-Assessment for the new CSRs. Instead, the **Self-Assessment** form opens with a blank response form in READONLY mode (refer to section 3.3) at record 0 of 0.

Figure 6-12. New Self-Assessment form record

Note that when creating a new Self-Assessment, the former CSR response status of “Yes,” “No,” “Partial,” and “Planned” do not appear in the CSR Status area of the **Self-Assessment** form. Since this is a new Self-Assessment, only the new response status levels appear in the CSR Status area.

6.8.1 Creating a New Response Record

To create a new CSR response record, select . This adds a new blank record (i.e., record 1 of 1) in ADD mode (refer to section 3.3).

Figure 6-13. Self-Assessment form “Entity Response” button

Note that there is a **Entity Response** button (i.e., yellow-highlight button in Figure 6-13) on the **Self-Assessment** form below the CSR “Status” area. This button is active only for new blank CSR response records when at least one other Self-Assessment exists in the back-end database. If this is a new Self-Assessment but no other Self-Assessments exist, the **Entity Response** button does not display.

6.8.2 Entity Response Button

When another Self-Assessment exists in the back-end database, the **Entity Response** button enables the Business Partner to select a baseline Self-Assessment to be used as the default response for blank CSR records. Selecting **Entity Response** opens a **Select Baseline Self-Assessment** dialog. Use the drop-down menu to select the baseline Self-Assessment from those that exist in the back-end database.

Figure 6-14. Baseline Self-Assessment selection

Selecting **Continue** closes the form and returns to the **Self-Assessment** form.

6.8.3 Baseline Self-Assessment

Once a baseline Self-Assessment has been selected, selecting **Entity Response** in a blank CSR response record automatically pastes the equivalent CSR status, response, POC assignment(s), and any Weakness(es) and supporting document links, if applicable, from the baseline Self-Assessment into the blank CSR record. If any of these fields already contain data or links, existing data and links are overwritten with baseline Self-Assessment data. The user is required to verify all fields and links, and modify them as necessary.

To change the default baseline Self-Assessment selection, use the **Shift+** **Entity Response** button combination (i.e., keep the **Shift** key depressed while selecting the **Entity Response** button) to open the **Select Baseline Self-Assessment** dialog (Figure 6-14) and select a different baseline Self-Assessment.

6.9 Completing the Self-Assessment/CSR Form

Ensure the **Self-Assessment** form is in the proper mode (refer to section 3.3). To add a new CSR record, the form must be in ADD mode; to edit an existing CSR record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified. Although Figure 6-15 displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes.

Figure 6-15. Self-Assessment form EDIT mode

The screenshot shows a software interface for a self-assessment form. At the top, a yellow bar displays 'Contractor XYZ (Part A)'. Below this, the main content area is divided into sections. The first section is '1. Entitywide Security Program Planning and Management', which includes a 'General Requirement' section with the text: '1.1. Management and staff shall receive security training, security awareness, and have security expertise.' Below this is a 'Control Technique' section with a table of columns: 'Applicability', 'Protocols', 'Guidance', and 'Reference'. The table contains detailed text for '1.1.1 Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).' Below the table, there are controls for 'Goto CSR' (set to 1.1.1), 'Validate', 'Reports', 'Systems', and 'Points-of-Contact'. The 'Status' section has radio buttons for 'Level 0', 'Level 1', 'Level 2', 'Level 3', 'Level 4', 'Level 5', and 'N/A'. The 'Response' section has radio buttons for 'Yes', 'No', 'Partial', and 'Planned'. The 'Date Entered' field is set to 6/28/2005. A large text area contains a generic response for CSR 1.1.1. The footer shows 'Response Record: 1 of 2', 'CSR Record: 1 of 441', and 'EDIT' mode. The bottom right corner displays 'CMS Integrated Security Suite Version 5.09 / CSR Rev.5.0, December 2004'.

Note in Figure 6-15 that when opening a previous Self-Assessment to complete the FY06 or later responses, the former CSR status responses of “Yes,” “No,” “Partial,” and “Planned” appear in the CSR Status area of the following **Self-Assessment** form. They only display to indicate what the previous response status was but cannot be selected when responding to FY06 or later Self-Assessments. The new response status requirements are explained in section 6.9.2 and in BPSSM Appendix A.

Figure 6-16. Self-Assessment form response status area

Since this form includes different functional areas and several buttons, the following sections explain how to complete the **Self-Assessment** form by breaking up the form into different functional areas.

6.9.1 Self-Assessment Title and CSR Screen Areas

The active Self-Assessment title and the selected CSR information are displayed in the upper region of the following **Self-Assessment** form.

Figure 6-17. Self-Assessment form upper region

This upper region of the **Self-Assessment** form displays the active Self-Assessment title and the currently selected CSR Category, General Requirement, and Control Technique (refer to BPSSM Appendix A for an explanation of these CSR elements).

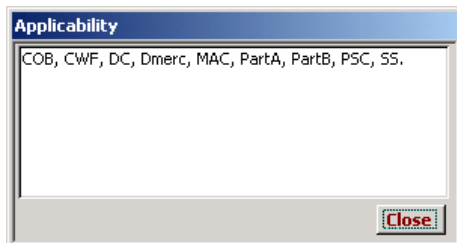
If the desired Self-Assessment title is not displayed in the yellow title area or a different one is required, refer to section 6.2a, for the procedure on changing this selection. It is important to verify that the correct Self-Assessment title is active in the **Self-Assessment** form. Otherwise, the wrong Self-Assessment information may be viewed or modified.

The CSR Category, General Requirement, and Control Technique information cannot be modified since these display CMS requirements. If the CSR General Requirement or Control Technique display is larger than the available form area, clicking the cursor anywhere in these areas opens a scroll bar that can be used scroll through the entire text.

6.9.1.1 Applicability Button

Selecting **Applicability** displays the following **Applicability** dialog for the selected CSR (refer to BPSSM Appendix A for an explanation of this information).

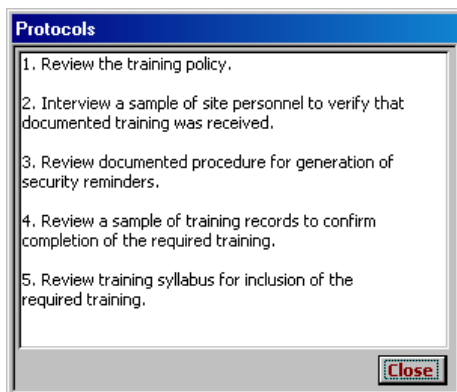
Figure 6-18. CSR Applicability dialog



6.9.1.2 Protocols Button

Selecting **Protocols** displays the following **Protocols** dialog for the selected CSR (refer to BPSSM Appendix A for an explanation of this information).

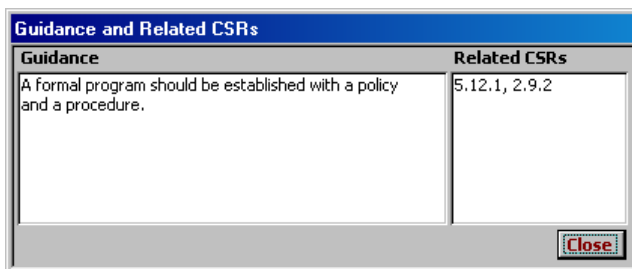
Figure 6-19. CSR Protocols dialog



6.9.1.3 Guidance Button

Selecting **Guidance** displays the following **Guidance and Related CSRs** dialog for the selected CSR (refer to BPSSM Appendix A for an explanation of this information).

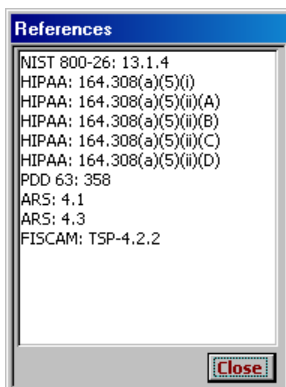
Figure 6-20. CSR Guidance and Related CSRs dialog



6.9.1.4 Reference Button

Selecting **Reference** displays the following **References** dialog for the selected CSR (refer to BPSSM Appendix A for an explanation of this information).

Figure 6-21. CSR References dialog



6.9.2 CSR Status and Response Areas

When no status or data has been entered for a CSR response (i.e., new Self-Assessment or CSR response record), the response screen area of the form looks similar to the following figure. Since the form is in EDIT mode, most of the buttons are disabled. In ADD or EDIT modes, the **Edit** button changes to **Save** and **Undo** is activated (refer to Figure 6-22 and Figure 6-23).

Figure 6-22. Self-Assessment form CSR response area in EDIT mode

Otherwise, the selected status and response description displays in the response area and most buttons are activated (Figure 6-23). When the CSR Response record already exists, selecting **Edit** opens the **Self-Assessment** form in EDIT mode (Figure 6-22). Note that although Figure 6-22 displays the form in ADD mode, the form functionality is the same for both ADD and EDIT modes.

Figure 6-23. Self-Assessment form CSR response area in READONLY mode

The background color around the CSR Status, Response, and Response Record areas corresponds to the same colors used to designate CSR nodes (refer to section 6.1). For example, the background color shown in Figure 6-23 is green to designate a fully compliant CSR Status (i.e., “Level 5” or “N/A” that is in agreement with the Applicability matrix).


6.9.2.1 CSR Status Selection

The “Status” field is a required field, so it must be completed before the form can be saved. Refer to BPSSM Appendix A for the definitions and criteria for using a response status of “Level 0-5” and “N/A.” Briefly stated, the Levels equate to:

- **Level 0** – None of the 5-Levels have been implemented
- **Level 1** – Documented Policy only
- **Level 2** – Level 1 and Documented Procedures only
- **Level 3** – Level 2 and Implemented Procedures and Controls only
- **Level 4** – Level 3 and Tested and Reviewed Procedures and Controls only
- **Level 5** – Level 4 and Fully Integrated Procedures and Controls

A *fully compliant* CSR has a Response Status of “Level 5” or “N/A” that is in agreement with the Applicability matrix. CMS considers any CSR with a “Level 3” or “Level 4” Response Status to be *compliant*, as opposed to being *fully compliant*. CMS also considers a CSR with a Response Status less than “Level 3” to be *non-compliant*.

When a *non-compliant* Response Status is selected (i.e., less than “Level 3”), the **Weakness** button is automatically activated to indicate a security Weakness (refer to section 6.9.2.10). The “CMS Risk-Based Decision Made” selection area is also automatically activated (refer to the next section, 6.9.2.2).

Selecting the response “Status” activates the selected Status indicator, such as  **Level 5**, and deselects all other Status selections. Only one Status can be active at a time, so changing the Status activates and deactivates the selections automatically. In addition, the surrounding screen background color changes based on the Status selected. This background color corresponds to the colors used to designate CSR nodes (refer to section 6.1).

NOTE: The purpose of the User Guide is to explain how to use the CISS. For guidance and criteria on selecting the correct CSR Status and what information to include in a CSR Response, refer to BPSSM Appendix A.

6.9.2.2 CMS Risk-Based Decision Selection







Refer to BPSSM Appendix A for the criteria for selecting this field. Briefly stated, selecting this field requires prior CMS concurrence and it is used in extreme cases only.

6.9.2.3 Date Entered Field



The “Date Entered” field is a required field, so it must be completed before the form can be saved. Review the “Date Entered” field—it defaults to the current Date. To change to a different Date, input the desired date in the “Date Entered” field (i.e., mm/dd/yyyy). If the Date is not entered in the specified format, it changes to this format automatically. Double-clicking in the “Date Entered” field displays a pop-up calendar from which a date can be selected.

6.9.2.4 CSR Response Field

The “Response” field is a required field, so it must be completed before the form can be saved. To input the CSR “Response” comments/explanation, enter the appropriate information in the white input area below “Response” and “Status.” Or, if copying information from a Worksheet or other source document, use the standard Windows® **Ctrl+C** (copy) and **Ctrl+V** (paste) combination keys (i.e., keeping the **Ctrl** key depressed while depressing the **C** or **V** keys) to copy from the source document and paste the information into this area.

The  button as well as the “Response Record” and “CSR Record” navigation controls are deactivated while in ADD or EDIT mode to ensure the user does not exit these modes except through the  and  buttons. Select either  to save the form information or select  to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if  is selected—all new or modified data will be lost.

6.9.2.5 Validate Button

Selecting  runs a self-check error routine that validates the selected CSR Response against established criteria. It performs the same function as the  button in the **Self-Assessment Reports** menu (Figure 6-24). Refer to the section 6.11 for more information on this button.

6.9.2.6 Reports Button



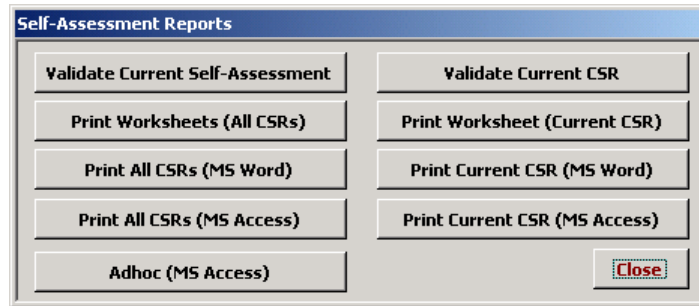

Selecting  displays the following **Self-Assessment Reports** menu. Selecting any of the activate Report buttons assembles and displays the selected Report (refer to section 6.11 for an explanation of each report type). Selecting  exits this menu and returns to the CSR **Response** dialog.

Figure 6-24. Self-Assessment Reports menu



6.9.2.7 Systems Button

The  button is not activated in this CISS release. It will be activated (and its use explained) in a future release of the CISS.

6.9.2.8 Points-of-Contact Button

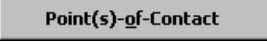
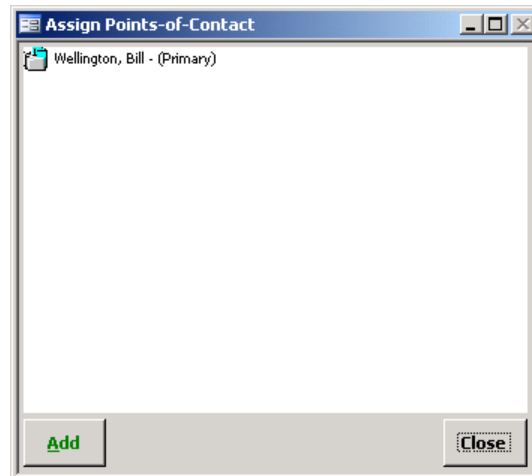
The  button is used to assign responsible existing POCs to the selected CSR. Selecting this button opens the following **Assign Points-of-Contact** dialog. This dialog displays any POCs already assigned to the CSR (if any). This dialog is used to add POC assignments to the CSR and not to add new POCs to the database. For information on adding new POCs to the database, refer to section 5.1.

Figure 6-25. Assign Points-of-Contact dialog





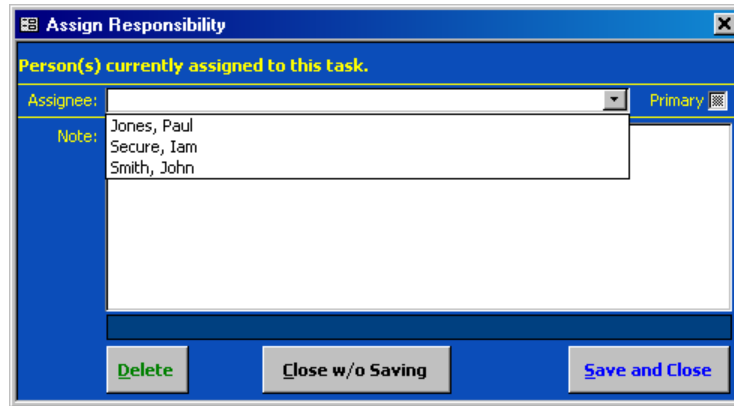
Selecting  exits this dialog and returns to the CSR **Response** dialog. Selecting  opens the **Assign Responsibility** dialog where existing POCs can be selected from the “Assignee” drop-down menu.

Figure 6-26. “Assignee” drop-down menu



After selecting a responsible POC to assign to the CSR from the “Assignee” drop-down menu (Figure 6-26), click the “Primary” checkbox to designate the POC as the Primary POC (if applicable), and select **Save and Close** to save the assignment or **Close w/o Saving** to abandon the POC selection and return to the **Assign Points-of-Contact** dialog (Figure 6-25). To assign multiple POCs to a CSR, the **Assign Responsibility** dialog must be opened again. Each assignment must be made separately; however, only one Primary POC can be designated. Selecting **Close** in the **Assign Points-of-Contact** dialog exits the dialog and returns to the CSR **Response** dialog.

6.9.2.9 Docs Button

The **Docs** button is not activated unless there is a CMS requirement to include corroborating documentation with the CSR response. If a CSR response meets one of the following criteria, the **Docs** button will become active after the CSR response is saved using the **Save** button:

- **CSR “N/A” Status Counter to Applicability Matrix** – CMS approval documentation is required for all CSR “N/A” responses that are not corroborated by the CSR Applicability matrix. That is, the CSR should be applicable for the contract type but the Business Partner does not agree.
- **Risk-Based Decision Non-Compliant CSR** – CMS concurrence documentation and updated Risk Assessment for all non-compliant CSR responses is required where a risk-based decision was made that no Weakness/Action Plan combination is required nor desired.

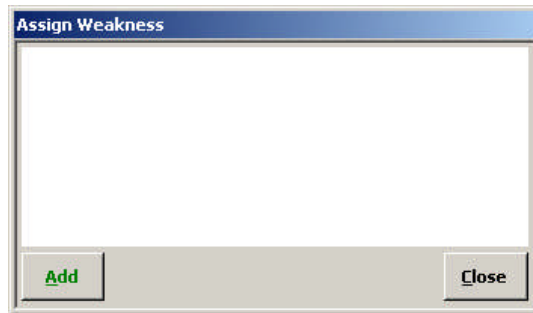
Refer to Chapter 4.0 for details on using the **Supporting Documents** form.

6.9.2.10 Weakness Button

The **Weakness** button is automatically activated whenever an non-compliant Response Status is selected and the Response is saved. A non-compliant CSR is any Response Status less than “Level 3.”

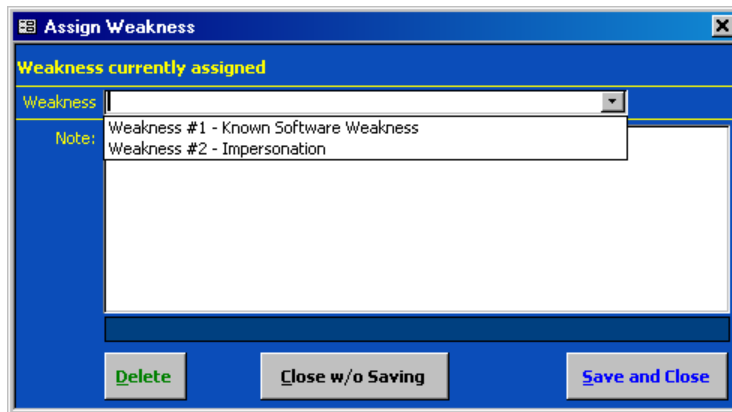
All Responses with a non-compliant Response Status must have a Weakness assigned to them (refer to BPSSM Appendix A). Selecting this button opens the following **Assign Weakness** dialog. This dialog displays any Weaknesses already assigned to the CSR (if any). This dialog is used to assign existing Weaknesses to a CSR and not to add new Weaknesses to the database. For information on adding new Weaknesses to the database, refer to section 7.1.

Figure 6-27. Assign Weakness dialog



Selecting **Close** exits this dialog and returns to the CSR **Response** dialog. Selecting **Add** opens the following **Assign Weakness** dialog where existing Weaknesses can be selected from the “Weakness” drop-down menu.

Figure 6-28. “Weakness” drop-down menu







Select a Weakness to assign to the CSR from the “Weakness” drop-down menu, and select **Save and Close** to save the assignment or **Close w/o Saving** to abandon the Weakness selection and return to the **Assign Weakness** dialog (Figure 6-27). To assign multiple Weaknesses to a CSR, the **Assign Weakness** dialog must be opened again. Each assignment must be made separately. Selecting **Close** in the **Assign Weakness** dialog exits the dialog and returns to the CSR **Response** dialog.

6.9.2.11 Worksheet Button

Selecting **Worksheet** creates a Worksheet for the active CSR only. It performs the same function as the **Print Worksheet (Current CSR)** button in the **Self-Assessment Reports** menu (Figure 6-24). Refer to the section 6.11 for more information on Worksheets.

6.9.3 Finalizing the Form

When done completing the form fields, select  to spell-check the data input fields. Then select  to save the form information or select  to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if  is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode.

Selecting  closes the **Self-Assessment** form and returns to the CISS main menu.

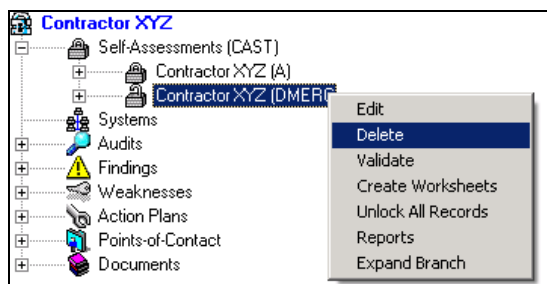
6.10 Deleting a Self-Assessment or CSR Response Record

Self-Assessments are deleted from the main menu (Figure 3-4) and CSR Responses are deleted from the **Self-Assessment** form.

6.10.1 Deleting a Self-Assessment

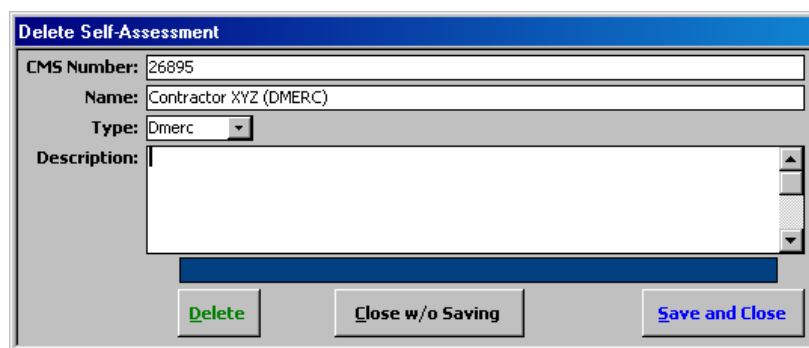
To delete a Self-Assessment and all its related CSR Response records, such as test Self-Assessment, expand the Treeview region “Self-Assessments (CAST)” major-level node and right-click the desired Self-Assessment name node [e.g., Contractor XYZ (DMERC)] to open the following pop-up menu.

Figure 6-29. Treeview “Delete” Self-Assessment node pop-up menu



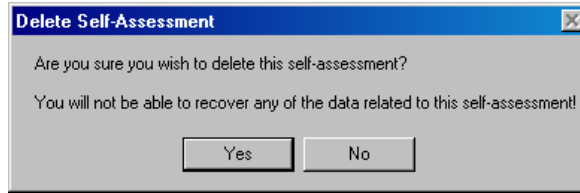
Selecting “Delete” from the pop-up menu opens the following **Delete Self-Assessment** form.

Figure 6-30. Delete Self-Assessment form



Selecting either  or  exits the form and returns to the Treeview *without* deleting the selected Self-Assessment. Selecting  displays the following warning message.

Figure 6-31. Delete Self-Assessment warning message



Selecting in this warning message exits the warning and returns to the Treeview *without* deleting the selected Self-Assessment. However, selecting *deletes* the selected Self-Assessment and all of its related CSR Response records, and their associated links *without* any further warnings or confirmations.

WARNING: All users of the CISS should be warned against using the Self-Assessment deletion process unless the objective really is to delete an existing Self-Assessment, such as a test Self-Assessment. Once a Self-Assessment is deleted, it can only be restored from a back-up copy of the back-end database. However, such a restoration will over-write all CISS data entered or modified since the last back-end database back-up.

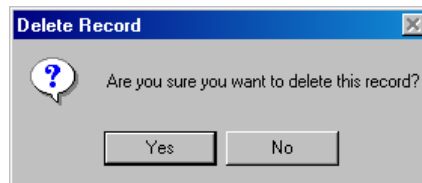
6.10.2 Deleting a CSR Response Record

Any CSR may have multiple CSR Response records either from prior year Self-Assessment Responses or prior “draft” (i.e., unlocked) Responses during the same year’s Self-Assessment. Individual prior-year Responses cannot be deleted because the records are locked (refer to section 6.3).

“Older” draft Responses do not need to be deleted when completing a Self-Assessment. The older draft Responses can be retained for historical purposes. Only the most recent Response record is reported in the Self-Assessment. However, when the Self-Assessment is submitted, all unlocked Response records become locked and can no longer be deleted.

To delete a CSR Response record, open the **Self-Assessment** form in READONLY mode. Use the form record navigation buttons to navigate to the desired CSR and CSR Response record (refer to section 6.2). Selecting closes the form and returns to the CISS main menu, and selecting displays the following **Delete Record** warning message.

Figure 6-32. Delete Record warning message



Selecting in this warning message exits from the **Delete Record** warning and returns to the CSR **Response** dialog *without* deleting the CSR Response record. However, selecting *deletes* the selected CSR Response record, as well as all POC and Weakness links to the selected CSR, *without* any further warnings or confirmations. Selecting in the resultant form exits to the main menu.

6.11 Self-Assessment/CSR Reports



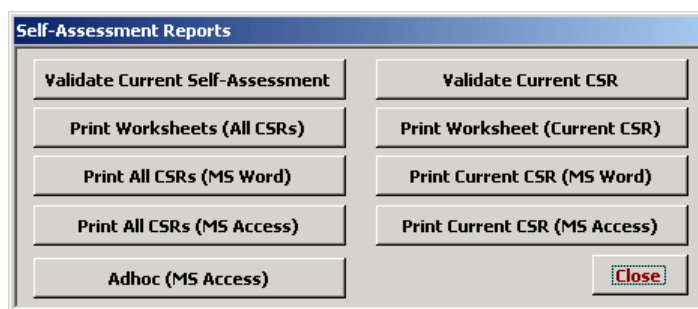
MS Excel[®] PivotTable reports (refer to section 3.11) can be accessed by selecting the  button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Self-Assessment Reports** menu can be accessed from the Treeview region using pop-up menus or from the **Self-Assessment** form using the  button (Figure 6-7).

Figure 6-33. Self-Assessment Reports menu



NOTE: The report buttons listed on the right side of the report menu (Figure 6-33) will not be active if the report selection is based on a Self-Assessment instead of a CSR. For example, if the Self-Assessment name node [e.g., Contractor XYZ (A)] “Reports” pop-up menu is selected (this selection requires a Self-Assessment report), the “Current CSR” reports on the right side will be inactive.

Any of the following methods can be used to open the **Self-Assessment Reports** menu:



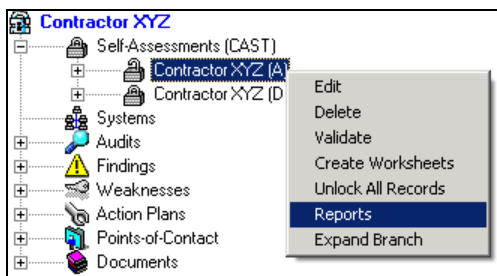
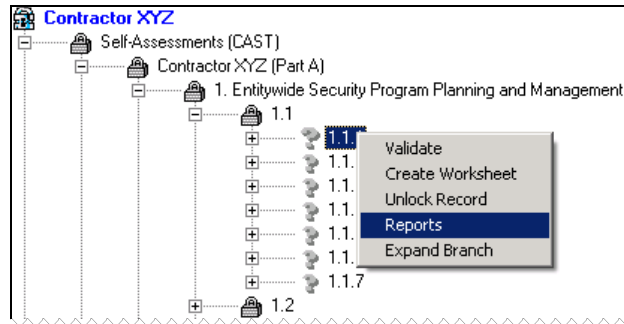
- If the **Self-Assessment** form is already open, use the form record navigation buttons to navigate to the desired CSR record (refer to section 3.2), if necessary. Then select  (Figure 6-7) to open the report menu.
- Refer to section 6.6 to open the desired Self-Assessment or CSR response record. Select  (Figure 6-7) to open the report menu.
- Expand the Treeview region “Self-Assessments (CAST)” major-level node (refer to section 3.1.5.1). Right-click the desired Self-Assessment name node [e.g., Contractor XYZ (A)] and select “Reports” in the following pop-up menu to open the report menu.

Figure 6-34. Treeview Self-Assessment name node “Reports” pop-up menu



- d. Expand the Treeview region “Self-Assessments (CAST)” major-level node (refer to section 3.1.5.1). Then expand the desired Self-Assessment name [e.g., Contractor XYZ (A)] lower-level nodes to the CSR Control Techniques lower-level nodes. Right-click the desired CSR Control Technique node (e.g., 1.1.1) and select “Reports” in the following pop-up menu to open the report menu.

Figure 6-35. Treeview CSR control technique node “Reports” pop-up menu

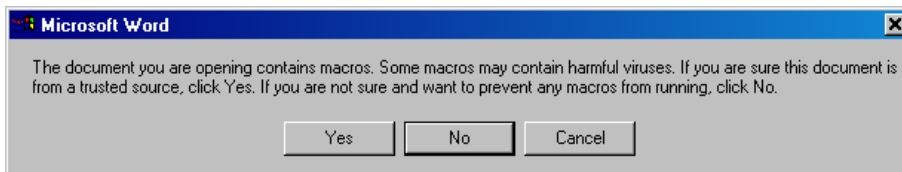


Selecting any of the report menu buttons assembles and displays the respective report (refer to the following sections for an explanation on each report). Selecting closes the **Self-Assessment Reports** menu and returns to the original starting point (i.e., CISS main menu or **Self-Assessment** form).

NOTE: After a report is generated, it may not display in the foreground (i.e., over the CISS screen). Instead, the report may appear only as a document icon in the Windows® Taskbar (e.g., “Document1 - Microsoft Word,” “Form Letters1 - Microsoft Word,” etc.). Selecting the applicable icon in the Taskbar opens the document in the foreground.

NOTE: If the MS Word® macro security setting is set to Medium, some reports may display the following warning dialog. Select either or to continue generating the report; otherwise, select to quit the generation process.

Figure 6-36. MS Word® macro warning message



WARNING: Before performing the following change, check with your System Security Administrator or SSO to ensure this change is allowed. To change the MS Word® macro Security Level setting, in Word®:

Select Tools, Macro, Security..., and High from the Security Level tab of the Security dialog. Select “OK” to make the change or “Cancel” to retain the existing setting.

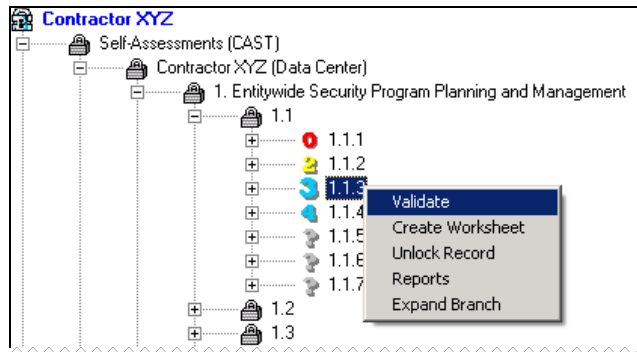
6.11.1 Validate Current CSR

To validate the current or selected CSR Response, use either of the following methods:

- a. Select from the **Self-Assessment** form (Figure 6-7).

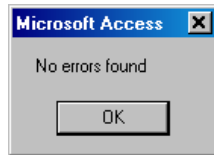
- b. Select **Validate Current CSR**, if activated, from the **Self-Assessment Reports** menu (Figure 6-33).
- c. Expand the Treeview region “Self-Assessments (CAST)” node (refer to section 3.1.5.1). Then expand the desired Self-Assessment name node [e.g., Contractor XYZ (Data Center)] and all lower-level nodes until the desired CSR number node (e.g., 1.1.3) displays. Right-click the desired CSR number node and select “Validate” in the following pop-up menu.

Figure 6-37. Treeview CSR number node “Validate” pop-up menu



Using any of the above methods runs a self-check error routine that validates the current or selected CSR Response against established criteria. If no validation errors are found, the following message displays.

Figure 6-38. CSR end of validation message



Otherwise, an error report similar to following example is prepared in MS Word® and displayed for the user to review, print, or save.

Figure 6-39. Example Word® single-CSR validation error report

CSR	Contractor XYZ (Data Center) Response
1.1.1	This CSR does not have a POC assigned.

6.11.2 Validate Current Self-Assessment

To validate all CSR Responses in the current or selected Self-Assessment, use either of the following methods:

- a. Select **Validate Current Self-Assessment** from the **Self-Assessment Reports** menu (Figure 6-33).
- b. Expand the Treeview region “Self-Assessments (CAST)” node, right-click the desired Self-Assessment title [e.g., Contractor XYZ (A)] and select “Validate” in the following pop-up menu.

Figure 6-42. Example Word® CSR Response worksheet

Category General Requirement Control Technique	CAST Worksheet for CSR 1.1.1 Contractor XYZ (Data Center) Rev 5.0, December 2004	Proprietary and Confidential
<i>I. Enterprise Security Program Planning and Management</i>		
1.1. Management and staff shall receive security training, security awareness, and have security expertise.		
1.1.1. Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).	Protocol(s): 1. Review the training policy. 2. Interview a sample of site personnel to verify that documented training was received. 3. Review documented procedure for generation of security reminders. 4. Review a sample of training records to confirm completion of the required training. 5. Review training syllabus for inclusion of the required training.	Reference(s): NIST 800-26:13.1.4 HIPAA: 144.308(a)(5)(ii) HIPAA: 144.308(a)(5)(ii)(A) HIPAA: 144.308(a)(5)(ii)(B) HIPAA: 144.308(a)(5)(ii)(C) HIPAA: 144.308(a)(5)(ii)(D) FDD 43:338 A.E.S.: 4.1 A.E.S.: 4.3 FIS: A.M.: ISF-4.2.2
Applicable Types: COB, CWF, DC, Dmcr, FariA, FariB, ISC, SS		Related CSRs(s): 5.12.1, 2.9.2
Status: Yes	Response Date: 1/18/2005	Weakness(s):
Current Answer: This is a generic response for CSR 1.1.1 in the self-assessment for Data Center. This response was created on Tuesday, April 27, 2004.		

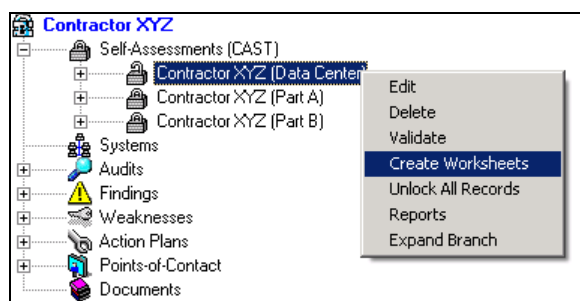
NOTE: Information obtained via Worksheets must be manually entered into the applicable CSR Responses. Electronic distribution of the Worksheets is beneficial because the input can be copied and pasted into the applicable CSR Responses.

6.11.4 Print Worksheets (All CSRs)

Worksheets facilitate communication among personnel responsible for supplying input to CSR Responses who may not have access to the CISS. When Worksheets are generated for all CSRs, only one CSR is printed per page to allow space for Response comments. To generate Worksheets for all CSRs in a Self-Assessment, use either of the following methods:

- a. Select **Print Worksheets (All CSRs)** from the **Self-Assessment Reports** menu (Figure 6-33).
- b. Expand the Treeview region “Self-Assessments (CAST)” node, right-click the desired Self-Assessment title [e.g., Contractor XYZ (Data Center)] and select “Create Worksheets” in the following pop-up menu.

Figure 6-43. Treeview Self-Assessment name node “Create Worksheets” pop-up menu



Once created, individual Worksheets similar to Figure 6-42 are available in MS Word® for each CSR (i.e., all CMS CSRs) for the user to review, print, or save.

6.11.5 Print Current CSR (MS Word)

The **Print Current CSR (MS Word)** button generates a report that includes only the CSR-related information without any Response data, so it can be selected from any active Self-Assessment. To generate the report for a single CSR, select **Print Current CSR (MS Word)**, if activated, from the **Self-Assessment Reports** menu (Figure 6-33).

Once created, a report similar to the following example is available in MS Word® for the user to review, print, or save.

Figure 6-44. Example MS Word® CSR report

Category General Requirement Control Technique	CMS Core Security Requirements	
<i>I. Entitywide Security Program Planning and Management</i>		
1.1. Management and staff shall receive security training, security awareness, and have security expertise.		
1.1.1. Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential). Guidance: A formal program should be established with a policy and a procedure. Applicable Types: COB, CWE, DC, Dman, Part6, Part8, P&C, SS	Protocol(s): <ul style="list-style-type: none"> ▪ Review the training policy. ▪ Interview a sample of site personnel to verify that documented training was received. ▪ Review documented procedure for generation of security reminders. ▪ Review a sample of training records to confirm completion of the required training. ▪ Review training syllabus for inclusion of the required training. 	Reference(s): NIST 800-24:13.1.4 HIPAA: 144.308(a)(5)(i) HIPAA: 144.308(a)(5)(ii)(A) HIPAA: 144.308(a)(5)(ii)(B) HIPAA: 144.308(a)(5)(ii)(C) HIPAA: 144.308(a)(5)(ii)(D) FPD 03:358 A.E.S.: 4.1 A.E.S.: 4.3 FISMA: ISP-4.2.2 Related CSR(s): 3121, 292

6.11.6 Print All CSRs (MS Word)

The **Print All CSRs (MS Word)** button generates a report that includes only the CSR-related information without any Response data, so it can be selected from any active Self-Assessment. When the report is generated, it prints all CSRs one after the other with no space between CSRs for writing Response comments.

To generate the report for all CSRs, select **Print All CSRs (MS Word)** from the **Self-Assessment Reports** menu (Figure 6-33). Once created, a report that includes only CSR-related information similar to Figure 6-44 (but for all the CSRs) is available in MS Word® for the user to review, print, or save.

6.11.7 Print Current CSR (MS Access)

The **Print Current CSR (MS Access)** button generates a report that includes all the CSR data—all CSR-related information along with the Response Status and Comments, and Response Weakness and POC links, if any. As such, the report is convenient for printing a complete record of a CSR and its response data. To generate the report for a single CSR, select **Print Current CSR (MS Access)**, if activated, from the **Self-Assessment Reports** menu (Figure 6-33).

Once created, a report similar to the following example is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 6-45. Example MS Access® CSR report

CSR Self-Assessment for Contractor XYZ (Data Center)

Category 1 Entitywide Security Program Planning and Management

General Req 1.1 Management and staff shall receive security training, security awareness, and have security expertise.

CSR: 1.1.1 Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).

Applicability: CCB, CWF, DC, Dmax, Part4, Part5, P8C, S8 **Status:** Yes **As of:** 01/18/05

Current Response: This is a generic response for CSR 1.1.1 in the self-assessment for Data Center. This response was created on Tuesday, April 27, 2004.

Weaknesses: None assigned.

GUIDANCE	PROCEDURES	RELATED CSRs	REFERENCES	POC
A formal program should be established with a policy and a procedure.	Entitywide training policy. Interview a sample of the personnel to verify that documented training was received. Entitywide documented procedure for generation of security reminders. Entitywide sample of training materials to confirm completion of the required training. Entitywide training syllabus for inclusion of the required training.	5121, 2.9.2	NIST 800-24:131.4 HIPAA: 144.308(a)(5)(i) HIPAA: 144.308(a)(5)(ii)(A) HIPAA: 144.308(a)(5)(ii)(B) HIPAA: 144.308(a)(5)(ii)(C) HIPAA: 144.308(a)(5)(ii)(D) EEO 3-338 AES: 4.1 AES: 4.3 NIST SP: 800-24.2.2	None Assigned.

Since this is a MS Access® report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access® report Toolbar controls. Closing the report returns to the report menu (Figure 6-33).

6.11.8 Print All CSRs (MS Access)

The **Print All CSRs (MS Access)** button generates a report that includes all the CSR data—all CSR-related information along with the Response Status and Comments, and Response Weakness and POC links, if any. As such, the report is convenient for printing a complete record of all CSRs and their response data for the active Self-Assessment (e.g., for the Security Profile). When the report is generated for all CSRs, it prints CSRs one after the other with no space between CSRs for writing Response comments.

To generate the report for all CSRs in the active Self-Assessment, select **Print All CSRs (MS Access)** from the **Self-Assessment Reports** menu (Figure 6-33). Once created, a report similar to Figure 6-45 is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Since this is a MS Access® report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access® report Toolbar controls. Closing the report returns to the report menu (Figure 6-33).

6.11.9 Adhoc (MS Access)

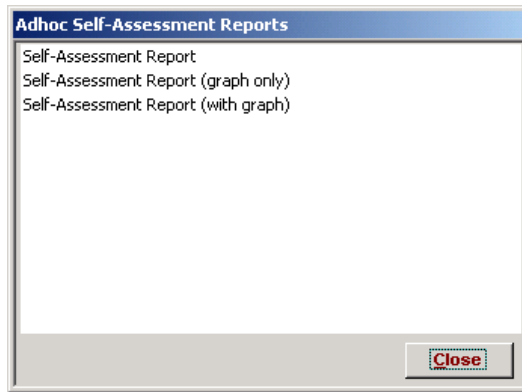
The **Adhoc (MS Access)** button allows the user to create a report that includes only the user-specified information and is based on user-selected parameters (or filters). As such, the report is useful for creating a report that includes only CSRs with a specific Reference (e.g., HIPAA) or a report that includes only CSRs with a specific Status (e.g., N/A). These examples are only a small sample of how reports can be customized to meet specific needs.

Although this function generates a report that includes only the CSRs based on user-specified filters, all CSR data is included—the CSR-related information along with the Response Status and Comments, and Response Weakness and POC links, if any. The report prints CSRs one after the other with no space between CSRs for writing Response comments.

6.11.9.1 Adhoc Reports

To generate adhoc reports, select **Adhoc (MS Access)** from the **Self-Assessment Reports** menu (Figure 6-33). This opens the following **Adhoc Self-Assessment Reports** dialog with the following Adhoc report selections.

Figure 6-46. Adhoc Self-Assessment Reports dialog



Selecting **Close** closes the dialog and returns to the **Self-Assessment Reports** menu (Figure 6-33).

6.11.9.2 Adhoc Report Selection

Refer to Figure 6-46 to select and create one of the following Self-Assessment report types:

- a. To generate adhoc reports that contain only selected Self-Assessment data but no graphs, double-click the “Self-Assessment Report” selection.
- b. To generate adhoc reports that contain only graphs that represent selected Self-Assessment data but no included data, double-click the “Self-Assessment Report (graph only)” selection.
- c. To generate adhoc reports that contain both selected Self-Assessment data and graphs, double-click the “Self-Assessment Report (with graph)” selection.

Selecting **Close** closes the **Adhoc Self-Assessment Reports** dialog (Figure 6-46) and returns to the **Self-Assessment Reports** menu (Figure 6-33).


6.11.9.3 Adhoc Report Filter Selection

The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

7.0 Weaknesses

All non-compliant CSRs (i.e., response status less than “Level 3”), and all audit or review Findings must be linked to (or associated with) a Weakness and a corresponding Action Plan and Milestones to remediate the Weakness. The progress towards completing the Action Plans associated with each Weakness is updated and submitted to CMS using the POA&M reporting process in the CISS application (refer to Chapters 8.0 and 12.0).



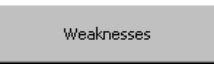

Note that all audit and review Findings must be linked to one or more Weaknesses. Since a security Weakness identified during an audit or review is the result of a non-compliant CSR, all security Weaknesses resulting from audit and review Findings must also be linked to (or associated with) a non-compliant CSR. Once the appropriate CSR(s) relating to the security Weakness(es) are found, its Response Status must be changed to something less than “Level 3” (if not already indicated as non-compliant) and the CSR must be linked to the applicable Weakness (refer to section 6.9.2.10).






As described in section 3.1, one of the major-level nodes in the Treeview region is a “Weaknesses” node (Figure 3-4). In addition, the Component region of the main menu includes a  button (Figure 3-4). Weaknesses lower-level nodes are also present under other major-level security element nodes. Any of these CISS main menu interfaces can be used to open Weakness records in the CISS application.

This Chapter explains the mechanics of using the CISS to document and manage security Weaknesses. Consult BPSSM Appendix A for guidance on security Weaknesses. Users are strongly encouraged to become familiar with all the criteria and guidance contained in BPSSM Appendix A *before* attempting to use the CISS to complete Weaknesses.

7.1 Creating a New Weakness Record

To create a new Weakness record, use either of the following methods to open the **Weakness** form (Figure 7-2):




- a. Right-click the Treeview region “Weaknesses” major-level node and select “Add” from the pop-up menu (refer to section 3.4.2). This opens a new blank form in ADD mode (refer to section 3.3). Selecting  and  closes the form *without* saving the new record and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  opens a new blank form in ADD mode.

Selecting  before selecting  closes the form *without* saving the new record and returns to the CISS main menu. After selecting  to open a new record, selecting  returns the form to READONLY mode *without* saving the new record. Selecting  closes the form and returns to the CISS main menu.

To complete the **Weakness** form, proceed to section 7.4.




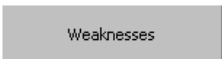


7.2 Opening a Weakness Record

To open an existing Weakness record, use either of the following methods to open the **Weakness** form (Figure 7-1):

- a. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weaknesses” node (refer to section 3.1.5.1). Double-click the desired Weakness name node to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

7.3 Editing a Weakness Record

To edit an existing Weakness record, use either of the following methods to open the **Weakness** form (Figure 7-2):

- a. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weaknesses” node (refer to section 3.4.2). Right-click the desired Weakness name node and select “Edit” from the pop-up menu. This opens the selected **Weakness** form in EDIT mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weaknesses” node (refer to section 3.1.5.1). Double-click the desired Weakness name node to open the form in READONLY mode (refer to section 3.3). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.
- c. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Weakness record (refer to section 3.2). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.

When opening an existing Weakness for editing, some **Weakness** form fields may not be editable because the fields are “locked.” Certain fields are locked automatically by the CISS whenever a new Weakness is reported to CMS in the POA&M. A new Weakness is considered any Weakness not previously reported to CMS in the POA&M.

All identified Weaknesses must be reported to CMS in the annual Self-Assessment submission (i.e., Weaknesses associated with non-compliant CSRs) or in the POA&M submissions (i.e., Weaknesses associated with audit or review findings). When a Weakness has been reported to CMS in a Self-Assessment or POA&M, certain fields contain information that is included in the annual CMS POA&M report required by the FISMA, and the FISMA dictates that certain information not be modified once submitted. To comply with the FISMA, one of the CISS steps during the Self-Assessment and POA&M submission process (refer to Chapter 12.0) is to lock all fields that can no longer be modified.

When form fields are locked, their input background color is yellow instead of white and their data cannot be modified. Only the fields with a white input background in the following figure are unlocked and only those fields can be modified while the form is in EDIT mode. The blue-highlighted area in the following figure depicts the dialog windows that can only be modified while in READONLY mode.

Figure 7-1. Weakness form locked fields

To modify the *Weakness* form data, proceed to the next section, 7.4.

7.4 Completing the Weakness Form

Ensure the *Weakness* form is in the proper mode (refer to section 3.3). To add a new Weakness record, the form must be in ADD mode; to edit an existing Weakness record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified.

Although the following figure displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes. In READONLY mode, the form fields cannot be modified. Only the unlocked form fields in the non-blue highlighted area depicted in the following figure can be edited or modified while in EDIT or ADD mode. And, the information in the blue highlighted area can only be edited or modified while in READONLY mode (refer to section 7.4.11).

Figure 7-2. Weakness form EDIT mode

7.4.1 Weakness Identifier

Refer to BPSSM Appendix A for guidance on completing the following Weakness identifier fields.

7.4.1.1 Entity Field

The “Entity” field is a required field but it is filled in by the CISS using the “Company Abbreviation” parameter value provided when the back-end database was established. If this abbreviation is not correct, refer to section 2.4.1 for information on changing the entity abbreviation.

7.4.1.2 Quarter Field

The “Quarter” field is a required field. This field represents the fiscal year quarter (i.e., A, B, C, D) in which the Weakness was first identified and entered into the POA&M.

7.4.1.3 Year Field

The “Year” field is a required field. This field represents the fiscal year in which the Weakness was identified and first reported. Although it is filled-in by the CISS to reflect the current fiscal year, this field can be modified while in ADD or EDIT mode (refer to section 3.3).

7.4.1.4 Number Field

The “Number” field is a required field. This is an incremental number representing the sequence in which the Weakness is entered into the Business Partner’s POA&M.

7.4.2 Weakness Title

The “Title” is also a required field and it is limited to 50 characters, including spaces. The “Title” *must not* include any contractor-, location-, or system-specific information, or other sensitive or identifying information.

IMPORTANT: Do NOT include any Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the “Title” field. The CISS application cannot validate this field for sensitive or identifying information, so the SSO must validate the “Title” field prior to submitting any Weakness or POA&M information to CMS.

7.4.3 Weakness Description

The “Description” field does not include any sensitive or identifying information restrictions. Include sufficient information and detail to allow CMS to evaluate the Weakness.

7.4.4 Weakness Category Selection

All Weaknesses must be assigned to a Weakness Category. The Category assignment is selectable from the following “Category” field drop-down menu selection. Consult BPSSM Appendix A for guidance on populating these fields. This selection can be made at a later time.

Figure 7-3. Weakness form “Category” selection

Category:	Physical and Environment Protection
Action Plan:	Risk Assessment Configuration Management Maintenance
Risk:	C&A and Security Assessments Planning
Likelihood	Personnel Security
Impact	Physical and Environment Protection System and Communications Protections

7.4.5 Action Plan Selection

All Weaknesses must be assigned to an Action Plan that will remediate the Weakness. The Action Plan assignment is selectable from the following “Action Plan” field drop-down menu selection. This selection can be made at a later time.

Figure 7-4. Weakness form “Action Plan” selection

Category:	Media Protection
Action Plan:	Enterprise-wide security awareness training
Risk:	Enterprise-wide security awareness training Apply FY04 CMS policies and procedures Apply latest service packs

7.4.6 Risk Selection

All Weaknesses must be assigned a Risk level. However, the Risk level is determined by the selections made in the “Likelihood” and “Impact” fields, so the Risk level is not selectable or editable. The following Likelihood and Impact assignments are selectable from their respective drop-down menu selections. Consult BPSSM Appendix A for guidance on populating these fields. These selections can be made at a later time.

Figure 7-5. Weakness form Risk “Likelihood” selection

The screenshot shows a form titled 'Risk: High'. It contains three dropdown menus: 'Likelihood', 'Impact', and 'FISMA Severity'. The 'Likelihood' dropdown is open, showing options: Negligible, Very Low, Low, Medium (selected), High, Very High, and Extreme. The 'Impact' dropdown is closed, showing 'Significant'. The 'FISMA Severity' dropdown is closed, showing 'Weakness'.

Figure 7-6. Weakness form Risk “Impact” selection

The screenshot shows the same form as Figure 7-5. The 'Impact' dropdown is open, showing options: Insignificant, Minor, Significant (selected), Damaging, Serious, and Critical. The 'Likelihood' dropdown is closed, showing 'Medium'. The 'FISMA Severity' dropdown is closed, showing 'Weakness'.

7.4.7 FISMA Severity Selection

All Weaknesses must be assigned a FISMA Severity level. However, since “Weakness” is the only FISMA Severity level that can be selected by Business Partners, the **Weakness** form defaults to this selection. Although the following drop-down menu displays other selection options, no other severity level can be selected. Consult BPSSM Appendix A for guidance on populating this field.

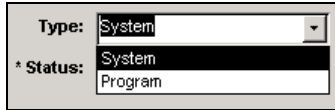
Figure 7-7. Weakness form “FISMA Severity” selection

The screenshot shows a dropdown menu titled 'FISMA Severity'. The dropdown is open, showing options: Significant Deficiency, Reportable Condition, and Weakness (selected).

7.4.8 Type Selection

All Weaknesses must be assigned as a System or Program weakness. The Type assignment is selectable from the following “Type” field drop-down menu selection. Consult BPSSM Appendix A for guidance on populating this field. This selection can be made at a later time.

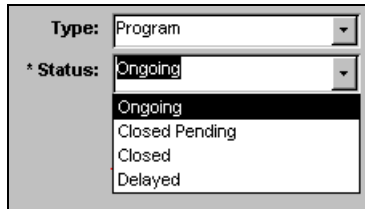
Figure 7-8. Weakness form “Type” selection







7.4.9 Status Selection

All Weaknesses must include a Status that indicates the stage or state of the Weakness condition. The Status is selectable from the following “Status” field drop-down menu selection. Consult BPSSM Appendix A for guidance on populating this field. The Status is a required field, so it must be selected before the form can be saved.

Figure 7-9. Weakness form “Status” selection



7.4.10 Finalizing the Form

When done completing the form fields, select  to spell-check the data input fields. Then select  to save the form information or select  to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if  is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode. To make changes to the selected Weakness links or associations, proceed to section 7.5.

Selecting  closes the **Weakness** form and returns to the CISS main menu.

7.4.11 Validating Weaknesses

The CISS application can run an internal self-check routine to validate the Weakness(es) against established criteria.


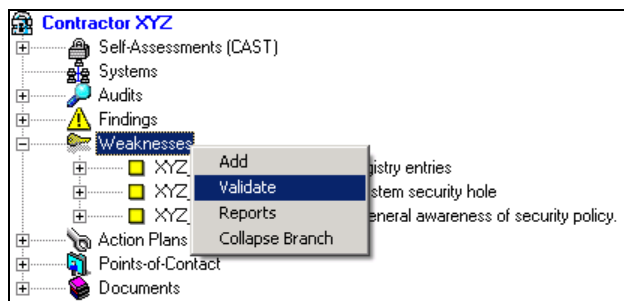
- a. To validate the current Weakness, select  from the **Weakness** form (Figure 7-15).
- b. To validate all Weaknesses in the database, right-click the Treeview “Weaknesses” major-level node and select “Validate” in the following pop-up menu.

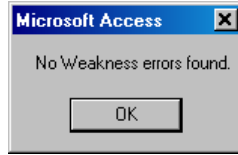
Figure 7-10. Treeview “Validate” all Weaknesses node pop-up menu



- c. To validate a specific weakness, expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weaknesses” node (refer to section 3.1.5.1), and select “Validate” from the Treeview node pop-up menu.

If no errors are found during the validation process, the following dialog displays.

Figure 7-11. Weakness Validate confirmation message



Otherwise, an error report similar to the following example is prepared in MS Word® and displayed for the user to review. This error report can be printed or saved for further review.

Figure 7-12. Example Weakness validation error report

Weakness	Error		
XYZ_C_2005_8	Weakness:#3-Test	Weakness: XYZ_C_2005_8	Weakness:#3-Test does not have an Action Plan developed

7.5 Weakness Links or Associations

The following figure displays a **Weakness** form in READONLY mode. In READONLY mode, the fields in the blue highlighted area cannot be modified. Only the non-blue highlighted dialog window areas are selectable. These dialog windows display all existing links that the selected Weakness pertaining to POC, Finding, and CSR element records, if any.

Figure 7-13. Weakness form READONLY mode

The screenshot shows a 'Weakness' form in 'READONLY' mode. At the top, it displays metadata: Entity: XYZ, Quarter: Q, Year: 2005, and Number: 1. The main form area contains a title 'Physical Access' and a description: 'Physical access to sensitive areas is excessive. This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.' Below the description are several dropdown menus: Category (Physical and Environment Protection), Action Plan (Physical Access), Risk (Medium), Type (Program), Status (Ongoing), Likelihood (Medium), Impact (Medium), and FISMA Severity (Weakness). A red error message is displayed: 'There are errors on this form. Click "Validate" to see the errors!'. To the right of the main form are four panels: 'POCs' with an 'Add' link and a list item 'Smith, James - (Primary)'; 'Findings' with an 'Add' link and a list item 'XYZ-05-E-001: Physical Access Weakness'; 'CSRs' with an 'Add' link and a list of three items: '2.2.15 - Contractor XYZ (Part A)', '2.2.18 - Contractor XYZ (Part A)', and '10.1.2 - Contractor XYZ (Part A)'; and 'Systems - (Disabled)' with an 'Add' link. At the bottom of the form, there is a 'Weakness Record: 1 of 1' indicator and a set of navigation buttons including 'Validate', 'Reports', 'Undo', 'Edit', and 'Close'.

7.5.1 Adding Weakness Links to Other Forms

Weakness links can be made to other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). Weakness links can also be made from the **Weakness** form dialog windows using the **Add** link in the dialog windows. Clicking the **Add** link in any of these dialog windows while in READONLY mode opens the selected security element form. For example, clicking the **POCs** dialog window **Add** link opens the following **Assign Responsibility** dialog.

Figure 7-14. Assign Responsibility dialog

The screenshot shows a software interface for managing weaknesses. An 'Assign Responsibility' dialog box is open, allowing users to assign tasks to specific personnel. The dialog lists 'Johnson, John' as the assignee and 'Smith, James' as a note. The background 'Weakness' form is partially visible, showing fields for entity, title, description, category, action plan, risk level, likelihood, impact, and FISMA severity. A red error message is displayed on the form, indicating that there are errors and the user should click 'Validate' to see them. The interface includes various navigation and control buttons like 'Validate', 'Reports', 'Close w/o Saving', and 'Save and Close'.

After the POC selection is made from the drop-down menu, selecting **Save and Close** saves the POC link assignment and closes the **Assign Responsibility** dialog; and selecting **Close w/o Saving** closes the form *without* making the POC link assignment. Both buttons return to the **Weakness** form.

Selecting **Close** closes the **Weakness** form and returns to the CISS main menu.

7.5.2 Removing Weakness Links to Other Forms

Weakness links can be removed from other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). Weakness links that are listed in any **Weakness** form dialog window (see following figure) can also be removed. Double-clicking the desired security element title in any dialog window while in READONLY mode selects the security element and opens its respective form.

Figure 7-15. Weakness CSRs dialog window assignment

The screenshot shows a 'Weakness' dialog window with the following details:

- Entity:** XYZ
- Quarter:** B
- Year:** 2005
- Number:** 5
- Title:** Weakness #2 - Impersonation
- Description:** Failure to protect password information.
- Category:** Access Controls
- Action Plan:** Action Plan #1
- Risk:** Medium
- Type:** Program
- Status:** Ongoing
- Likelihood:** Medium
- Impact:** Medium
- FISMA Severity:** Weakness

On the right side, there are three panels:

- POCs:** Secure, lam - (Primary)
- Findings:** XYZ-05-C-005: Finding #2 - Compromised Password, XYZ-05-R-005: Test from Weakness Form
- CSRs:** 1.1.9 - Contractor XYZ (Data Center)
- Systems - (Disabled):** (Empty)

A red error message is displayed in the center: "There are errors on this form. Click 'Validate' to see the errors!". Below the error message are buttons for 'Validate' and 'Reports'. At the bottom, there is a 'READONLY' status bar and a 'Weakness Record' section with navigation buttons (1 of 1) and a 'Close' button.

For example, double-clicking the “XYZ-05-C-005: Finding #2...” title in the **Findings** dialog window opens the respective **Finding** form in READONLY mode. Selecting **Edit** changes the following form to EDIT mode so its fields can be modified, and selecting **Close** closes the form and returns to the CISS main menu. Selecting **Close w/o Saving** or **Save and Close** both close the form *without* making any Weakness link assignment changes.

Highlight the Weakness title in the following **Findings** form “Weakness” field, “XYZ-05-C-005: Finding #2...” in this example, and press the **Delete** key to remove the highlight Weakness title from this field. Select a different Weakness title from its drop-menu, if applicable, or leave this field blank for later input.

Figure 7-16. Findings form Weakness title field

The screenshot shows a 'Findings' form window. At the top, there are input fields for * Entity (XYZ), * Year (2005), * Code (C), and * Num (005). Below these is the * Title field containing 'Finding #2 - Compromised Password'. The Description field contains the text 'User password was found written on Post-It note stuck to monitor.' To the right, a POCs (Personnel of Concern) list includes 'Secure, Iam - (Primary)' and 'Smith, John'. Below the POCs, the Risk is set to 'Medium', with Likelihood and Impact also set to 'Medium'. The FMFIA (and CPIC) Severity section has three radio buttons: 'Material Weakness' (unselected), 'Reportable Condition' (selected), and 'Neither' (unselected). The Status is 'Ongoing'. There are fields for 'Closed Pending Date' and 'Closed Date', each with a 'Docs' button. At the bottom, there are buttons for 'Validate', 'Reports', and 'Close'. A red error message at the bottom right states: 'There are errors on this form. Click "Validate" to see the errors!'. At the very bottom, there is an 'EDIT' bar and a 'Finding Record:' section showing '1 of 1' with navigation buttons and 'Undo' and 'Save' buttons.

Select **Undo** to restore the Weakness link to the Finding or select **Save** to save the deleted link association. Select **Close** to close the form and return to the **Weakness** form. Note that the “XYZ-05-C-005: Finding #2...” title in the following figure **Finding(s)** dialog window is removed.

Figure 7-17. Findings form Weakness title field

The screenshot shows a 'Weakness' form window. At the top, there are input fields for * Entity (XYZ), * Quarter (B), * Year (2005), and * Number (5). Below these is the * Title field containing 'Weakness #2 - Impersonation'. The Description field contains the text 'Failure to protect password information.' To the right, a POCs (Personnel of Concern) list includes 'Secure, Iam - (Primary)'. Below the POCs, there is a 'Findings' list with one entry: 'XYZ-05-R-005: Test from Weakness Form'. At the bottom, there are buttons for 'Add', 'Validate', 'Reports', and 'Close'.

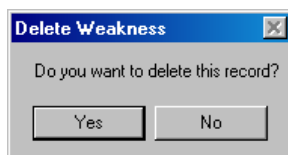
Selecting **Close** closes the **Weakness** form and returns to the CISS main menu.

7.6 Deleting a Weakness

To delete a Weakness, open the desired Weakness record using either of the following methods to open the **Weakness** form (Figure 7-1):

- a. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weaknesses” node (refer to section 3.1.5.1). Double-click the desired Weakness name node to open the form in READONLY mode (refer to section 3.3). Selecting closes the form and returns to the CISS main menu, and selecting displays the **Delete Weakness** warning message (Figure 7-18).
- b. Select the Component region button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Weakness record (refer to section 3.2). Selecting closes the form and returns to the CISS main menu, and selecting displays the following Delete Weakness warning message.

Figure 7-18. Delete Weakness warning message

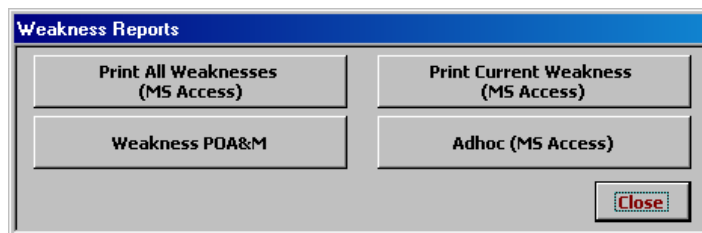


Selecting in this warning message exits from the **Delete Weakness** warning and returns to the **Weakness** form *without* deleting the Weakness. However, selecting *deletes* the selected Weakness, as well as all links to the selected Weakness, *without* any further warnings or confirmations. Selecting in the resultant form exits to the main menu.

7.7 Weakness Reports

MS Excel[®] PivotTable reports (refer to section 3.11) can be accessed by selecting the button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Weakness Reports** menu can be accessed from the Treeview region using pop-up menus or from the **Weakness** form using the button (Figure 7-1).

Figure 7-19. Weakness Reports menu



NOTE: The **Print Current Weakness (MS Access)** button (Figure 7-19) is active only if the report selection is based on a single Weakness selection. For example, double-clicking a specific Weakness or selecting the “Reports” pop-up menu from a specific Weakness results in an active button because a “current” Weakness has been identified. However, when selecting the “Reports” pop-menu from the “Weaknesses” major-level node, the button is inactive because no “current” Weakness has been identified.

Any of the following methods can be used to open the **Weakness Reports** menu (Figure 7-19):

- a. If the **Weakness** form is already open, use the form record navigation buttons to navigate to the desired Weakness record (refer to section 3.2), if necessary. Then select **Reports** (Figure 7-2) to open the report menu.
- b. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weakness” node (refer to section 3.1.5.1). Double-click the desired Weakness name node to open the Weakness record. Then select **Reports** (Figure 7-2) to open the report menu.
- c. Expand the Treeview region “Weaknesses” major-level node or any security element node with a lower-level “Weakness” node (refer to section 3.1.5.1). Right-click the “Weaknesses” node or any Weakness name node in any security element to display a pop-up menu that includes a “Reports” option (refer to section 3.4.2). Select “Reports” from the pop-up menu to open the report menu.

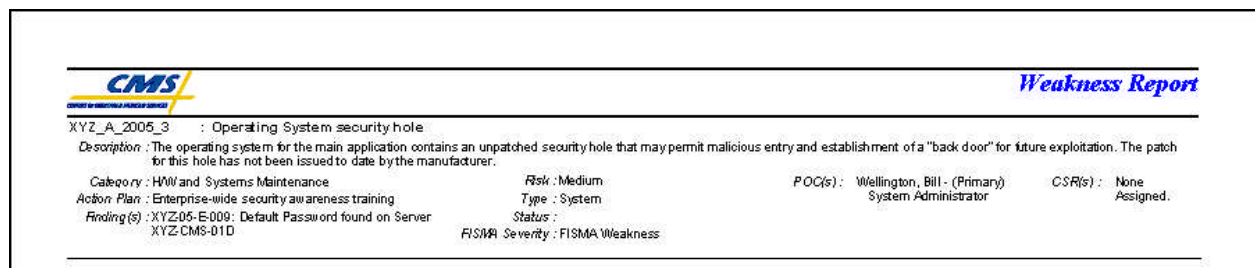
Selecting any of the report menu buttons assembles and displays the respective report (refer to the following sections for an explanation on each report). Selecting **Close** closes the **Weakness Reports** menu and returns to the original starting point (i.e., CISS main menu or **Weakness** form).

7.7.1 Print Current Weakness (MS Access)

Select **Print Current Weakness (MS Access)**, if activated, from the **Weakness Reports** menu (Figure 7-19) to generate a report that includes all information pertaining to the selected Weakness. Only the current or selected Weakness is included in the report.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 7-20. Example Current Weakness report



Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 7-19).

Selecting **Close** in the **Weakness Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Weakness** form).

7.7.2 Print All Weaknesses (MS Access)

Select **Print All Weaknesses (MS Access)** from the **Weakness Reports** menu (Figure 7-19) to generate a report that includes all Weaknesses contained in the database. The report includes all information included in all Weaknesses. The Weaknesses are printed one after the other with no page breaks between each Weakness.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 7-21. Example All Weaknesses report

CMS		Weakness Report	
XYZ_B_2006_2	: Duplicate registry entries		
<i>Description</i> : Registry anomalies have been discovered on certain systems that indicate unexplained duplication of HP_LOCAL and HP_USER key entries. Although the keys can be manually deleted with no apparent immediate ill effects, this behavior is still a concern to the system administrator.			
<i>Category</i> :	HW and Systems Maintenance	<i>Risk</i> :	Medium
<i>Action Plan</i> :	Apply latest service packs	<i>Type</i> :	System
<i>Finding(s)</i> :	None Assigned.	<i>Status</i> :	
		<i>POC(s)</i> :	None Assigned.
		<i>CSR(s)</i> :	None Assigned.
		<i>FISMA Severity</i> :	
XYZ_A_2006_1	: Test 3rd weakness		
<i>Description</i> : Test description			
<i>Category</i> :	HW and Systems Maintenance	<i>Risk</i> :	Low
<i>Action Plan</i> :	Apply FY04 CMS policies and procedures	<i>Type</i> :	System
<i>Finding(s)</i> :	None Assigned.	<i>Status</i> :	
		<i>POC(s)</i> :	Schaff, Tonya - (Primary) Line Supervisor
		<i>CSR(s)</i> :	None Assigned.
		<i>FISMA Severity</i> :	
XYZ_A_2006_3	: Operating System security hole		
<i>Description</i> : The operating system for the main application contains an unpatched security hole that may permit malicious entry and establishment of a "back door" for future exploitation. The patch for this hole has not been issued to date by the manufacturer.			
<i>Category</i> :	HW and Systems Maintenance	<i>Risk</i> :	Medium
<i>Action Plan</i> :	Enterprise-wide security awareness training	<i>Type</i> :	System
<i>Finding(s)</i> :	XYZ-05-E-009: Default Password found on Server XYZ-CMS-D1D	<i>Status</i> :	
		<i>POC(s)</i> :	Wellington, Bill - (Primary) System Administrator
		<i>CSR(s)</i> :	None Assigned.
		<i>FISMA Severity</i> :	FISMA Weakness
XYZ_A_2006_4	: Users lack general awareness of security policy.		
<i>Description</i> : Users, when interviewed, are not aware of certain basic security policy guidelines. This must be remedied.			
<i>Category</i> :	Security Awareness, Training, and Education	<i>Risk</i> :	High
<i>Action Plan</i> :	Enterprise-wide security awareness training	<i>Type</i> :	Program
<i>Finding(s)</i> :	XYZ-05-S-001: Employees unable to locate	<i>Status</i> :	
		<i>POC(s)</i> :	None Assigned.
		<i>CSR(s)</i> :	None Assigned.

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 7-19).

Selecting **Close** in the **Weakness Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Weakness** form).

7.7.3 Adhoc (MS Access)

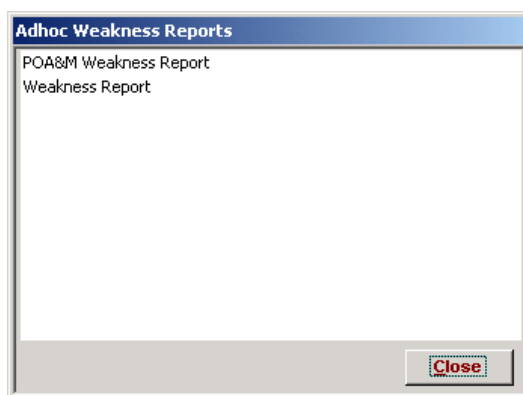
The Adhoc reports feature allows the user to generate a customized report that is based on user-selected filters (or parameters) and includes only user-specified information. For example, an Adhoc report can be created that includes only the Weaknesses assigned to a specific POC(s) or Action Plans. These examples are only a small sample of how reports can be customized to meet specific needs. Although these reports include only the Weaknesses based on user-specified

filters, all of the information pertaining to each Weakness is included in the report. The Weaknesses are printed one after the other with no page breaks between each Weakness.

7.7.3.1 Adhoc Reports

To generate adhoc reports, select **Adhoc (MS Access)** from the **Weakness Reports** menu (Figure 7-19). This opens the following **Adhoc Weakness Reports** dialog with the following Adhoc report selections.

Figure 7-22. Adhoc Weakness Reports dialog



Selecting **Close** closes the dialog and returns to **Weakness Reports** menu (Figure 7-19).

7.7.3.2 Adhoc Report Selection

Refer to Figure 7-22 to select and create one of the following Weakness report types:

- a. To generate adhoc reports that contain selected POA&M-related Weakness data, double-click the “POA&M Weakness Report” selection.
- b. To generate adhoc reports that contain selected Weakness data, double-click the “Weakness Report” selection.

Selecting **Close** closes the **Adhoc Weakness Reports** dialog Figure 7-22 and returns to the **Weakness Reports** menu (Figure 7-19).

7.7.3.3 Adhoc Report Filter Selection

The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

7.7.4 Weakness POA&M (MS Access)

Select **Weakness POA&M** from the **Weakness Reports** menu (Figure 7-19) to generate a report that includes all Weaknesses contained in the database. The report includes all information included in all Weaknesses. The Weaknesses are printed one after the other with no page breaks between each Weakness.

Once created, a report similar to the following example is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 7-23. Example Weakness POA&M report


Weakness Identifier	Weakness	IT Control Mapping	FOC	Resource Required	Scheduled Completion Date	Milestone with Completion Date	Change to Milestone	Identified in CFO audit or other audit review?	Status	Comments	Risk Level
XYZ_B_2005_2	Duplicate registration entries	HW and Systems Maintenance		Current \$200.00 Reallocated \$1,200.00 New \$200.00	3/1/2005			None			Low
XYZ_A_2005_1	Third weakness	HW and Systems Maintenance	Tony Schaff Line Supervisor		2/2/2005			None			Low
XYZ_A_2005_3	Operating System security hole	HW and Systems Maintenance	Bill Wallington System Administrator	Current \$600.00	3/2/2005	<ul style="list-style-type: none"> • Detail of failure - 3/2/2005 • Establish training dates - • Send out training announcements - • Deliver training - 		* Audit Findings: XYZ-05-E009		Medium	
XYZ_A_2005_4	Users lack general awareness of security policy.	Security Awareness, Training, and Education		Current \$600.00	3/2/2005	<ul style="list-style-type: none"> • Detail of failure - 3/2/2005 • Establish training dates - • Send out training announcements - • Deliver training - 		* Audit Findings: XYZ-05-S-001		High	

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 7-19).

Selecting in the **Weakness Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Weakness** form).

8.0 Action Plans





An Action Plan is a documented strategy for addressing known Weaknesses in a Business Partner’s IT security configuration. All non-compliant CSRs (i.e., response status less than “Level 3”), and all audit or review Findings must be linked to (or associated with) a Weakness and a corresponding Action Plan and Milestones to remediate the Weakness. The progress towards completing the Action Plans associated with each Weakness is updated and submitted to CMS using the POA&M reporting process in the CISS application (refer to Chapter 12.0).






As described in section 3.1, one of the major-level nodes in the Treeview region is an “Action Plans” node (Figure 3-4). In addition, the Component region of the main menu includes an  button (Figure 3-4). Action Plans lower-level nodes are also present under other major-level security element nodes. Any of these CISS main menu interfaces can be used to open Action Plan records in the CISS application.

This Chapter explains the mechanics of using the CISS to document and manage security Action Plans. Consult BPSSM Appendix A for guidance on Action Plans. Users are strongly encouraged to become familiar with all the criteria and guidance contained in BPSSM Appendix A *before* attempting to use the CISS to complete Action Plans.

8.1 Creating a New Action Plan Record

To create a new Action Plan record, use either of the following methods to open the **Action Plan** form (Figure 8-1):


- a. Right-click the Treeview region “Action Plans” major-level node and select “Add” from the pop-up menu (refer to section 3.4.2). This opens a new blank form in ADD mode (refer to section 3.3). Selecting  and  closes the form *without* saving the new record and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  opens a new blank form in ADD mode.



Selecting  before selecting  closes the form *without* saving the new record and returns to the CISS main menu. After selecting  to open a new record, selecting  returns the form to READONLY mode *without* saving the new record. Selecting  closes the form and returns to the CISS main menu.

To complete the **Action Plan** form, proceed to section 8.4.

8.2 Opening an Action Plan Record







To open an existing Action Plan record, use either of the following methods to open the **Action Plan** form (Figure 8-1):

- a. Expand the Treeview region “Action Plans” major-level node or any security element node with a lower-level “Action Plans” node (refer to section 3.1.5.1). Double-click the desired Action Plan name node to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

8.3 Editing an Action Plan Record

To edit an existing Action Plan record, use either of the following methods to open the **Action Plan** form (Figure 8-2):

- a. Expand the Treeview region “Action Plans” major-level node or any security element node with a lower-level “Action Plans” node (refer to section 3.4.2). Right-click the desired Action Plan name node and select “Edit” from the pop-up menu. This opens the selected **Action Plan** form in EDIT mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Expand the Treeview region “Action Plans” major-level node or any security element node with a lower-level “Action Plans” node (refer to section 3.1.5.1). Double-click the desired Action Plan name node to open the form in READONLY mode (refer to section 3.3). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.
- c. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Action Plan record (refer to section 3.2). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.

When opening an existing Action Plan for editing, some **Action Plan** form fields may not be editable because the fields are “locked.” Certain fields are locked automatically by the CISS whenever a new Action Plan is reported to CMS in the POA&M. A new Action Plan is considered any Action Plan not previously reported to CMS in the POA&M.

All identified Weaknesses must have an Action Plan to remediate the Weakness. The progress towards completing the Action Plan associated with each Weakness must be reported to CMS and updated using the CISS POA&M reporting process. When an Action Plan has been reported to CMS, certain fields contain information that is included in the annual CMS POA&M report required by the FISMA, and the FISMA dictates that certain information not be modified once submitted. To comply with the FISMA, one of the CISS steps during the POA&M submission process (refer to Chapter 12.0) is to lock all fields that can no longer be modified.

When form fields are locked, their input background color is yellow instead of white and their data cannot be modified. Only the white input background areas shown in the following figure are unlocked and only those fields can be modified while the form is in EDIT mode. The blue-shaded area depicted in following figure depicts dialog windows that can only be modified while in READONLY mode.

Although the **Milestones** Treeview dialog window area has a white input background, Milestone titles are also locked when the Action Plan is submitted and cannot be modified once submitted.

Figure 8-1. Action Plan form locked fields

To modify the *Action Plan* form data, proceed to the next section, 8.4.

8.4 Completing the Action Plan Form

Ensure the *Action Plan* form is in the proper mode (refer to section 3.3). To add a new Action Plan record, the form must be in ADD mode; to edit an existing Action Plan record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified.

Although the following figure displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes. In READONLY mode, the form fields cannot be modified. Only the unlocked form fields with white input background areas shown in the following figure can be edited or modified while in EDIT or ADD mode. And, the information in the blue highlighted area depicted in following figure can only be edited or modified while in READONLY mode (refer to the section 8.6).

Figure 8-2. Action Plan form EDIT mode

Action Plan

*** Action Plan Title**
Business Recovery Plan Compliance

Description
Revise the site's Medicare business recovery plans to be in compliance with NIST guidelines.
This is a generic comment or description to create test data for the CISS report and export/import functions.
Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.

Completion Dates
Initial Target: 4/30/2006
Current Projected: 4/30/2006
Actual:
Status: **Delayed**

*** Estimated Annual Maintenance:** \$0.00
*** Percent Security:** 100%
*** Percent Applied To CMS:** 0%

Costs
Estimated Annual Maintenance: \$0.00
Percent Security: 100%
Percent Applied To CMS: 0%

Funding Sources
Current: \$700.00
Reallocated: \$0.00
New: \$0.00

Target Implementation Costs
\$700.00

POCs
Brown, William - (Primary)
Davis, David

Weaknesses
XYZ_B_2004_4: Business Recovery Plans Not in Compliance

Milestones
Add Training Procedures to BCP Manual

Validate

There are errors on this form. Click "Validate" to see the errors!

EDIT

Action Plan Record: 1 of 1

Undo Save Reports Close

8.4.1 Action Plan Title and Description Fields

The “Action Plan Title” is a required field and it is limited to 50 characters, including spaces. The “Action Plan Title” should be descriptive of the plan and the “Description” field should include whatever description is deemed necessary to explain the Action Plan. Detailed descriptions of Action Plans are not necessary, but sufficient data is required to permit oversight and tracking.

8.4.2 Completion Dates and Target Implementation Costs Areas

The “Completion Dates” and “Target Implementation Costs” areas contain non-selectable form data that are completed automatically based on other input data. These fields update automatically as necessary.





8.4.3 Costs and Funding Sources Area Fields


The “Costs” and “Funding Sources” areas in the following figure require Business Partner remediation cost data and percentage input. All the “Costs” fields are required fields, so they must be completed before the form can be saved. Input percentage numbers as decimals (e.g., 1 = 100%, .25 = 25%, .75 = 75%). Consult BPSSM Appendix A for guidance on determining Costs and Funding Sources.

Figure 8-3. Action Plan form “Costs” and “Funding Sources” area


Costs		Funding Sources	
* Estimated Annual Maintenance:	<input type="text" value="\$0.00"/>	Current:	<input type="text" value="\$0.00"/>
* Percent Security:	<input type="text" value="100%"/>	Reallocated:	<input type="text" value="\$0.00"/>
* Percent Applied To CMS:	<input type="text" value="0%"/>	New:	<input type="text" value="\$0.00"/>

8.4.4 Finalizing the Form

When done completing the form fields, select  to spell-check the data input fields. Then select  to save the form information or select  to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if  is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode.

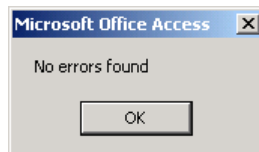
To make changes to the selected Action Plan “Milestones” area, proceed to section 8.5. To make changes to the selected Action Plan links or associations, proceed to section 8.6. Selecting  closes the **Action Plan** form and returns to the CISS main menu.

8.4.5 Validating Action Plans

The CISS application can run an internal self-check routine to validate the Action Plan against established criteria. To validate the current Action Plan, select  from the **Action Plan** form (Figure 8-2).

If no errors are found during the validation process, the following dialog displays.

Figure 8-4. Action Plan Validate confirmation message



Otherwise, an error report similar to the following example is prepared in MS Word® and displayed for the user to review. This error report can be printed or saved for further review.

Figure 8-5. Example Action Plan validation error report

Action Plan	Error
Programmer Access Restriction	Action Plan ("Programmer Access Restriction") needs an update to the Projected Date of Milestone ("Submit Documentation for Each Milestone to CMS"). Currently it is listed as 11/30/2005 with as status of Delayed

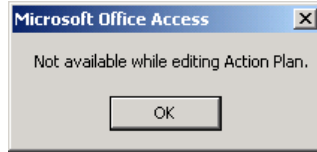
8.5 Completing Milestones

A typical Action Plan consists of activities with target dates called Milestones. The CISS Action Plans and their respective Milestones are used to produce the POA&M report, which Business Partners are required to submit to CMS as directed by BPSSM Appendix A.

NOTE: All Action Plans must include at least one milestone and all Action Plans that will take more than three months to complete must have more than one milestone.

Ensure the **Action Plan** form is in the proper mode (refer to section 3.3). Before any modifications in the **Milestones** dialog window area can be made, the **Action Plan** form must be in READONLY mode. Otherwise, a message similar to the following displays.

Figure 8-6. Milestones disabled function message

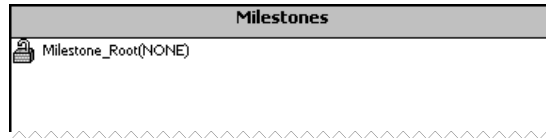


8.5.1 Adding Milestones

When a new Action Plan is created, the **Milestones** dialog window area of the **Action Plan** form is blank until the form is saved. Once the form is saved, the **Milestones** dialog window area displays a Treeview root node, “Milestone_Root(NONE)” (Figure 8-7). When Milestones are added to the Action Plan, the Milestone root node expands to include lower-level Milestones in the same manner as the Treeview nodes in the main menu.

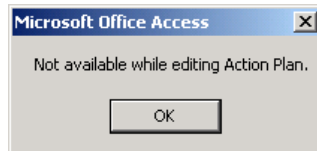
The initial (i.e., first) Milestone of an Action Plan can only be added using the procedure in the next section, 8.5.1.1. However, that same procedure can also be used to add subsequent (i.e., follow-on) Milestones. The procedure in the subsequent section, 8.5.1.2, can also be used to add subsequent Milestones, but not the initial Milestone.

Figure 8-7. Milestones root node before adding a Milestone



NOTE: While adding or editing any **Action Plan** form sub-form (i.e., **Milestone**, **Project Date**, or **Status Update**), all **Action Plan** form buttons and fields are disabled so its data cannot be modified. Any attempt to modify these fields displays the following message.

Figure 8-8. Action Plan disabled function message



8.5.1.1 Creating the Initial Milestone

Adding the initial Milestone can only be done by right-clicking the Treeview “Milestones” root node in the **Milestones** dialog window and selecting “Add Milestone” in the following pop-up menu.

Figure 8-9. Milestones node “Add Milestone” pop-up menu



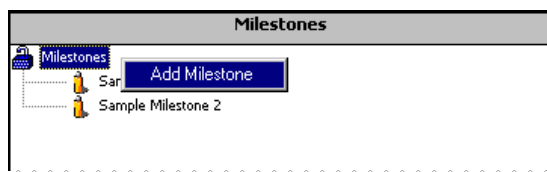
This opens the **Milestone** sub-form in the **Action Plan** form in ADD mode (Figure 8-12). To complete the **Milestone** form, proceed to section 8.5.1.3.

8.5.1.2 Adding Subsequent Milestones

After the initial Milestone has been created, additional Milestones can be created by using either of the following methods:

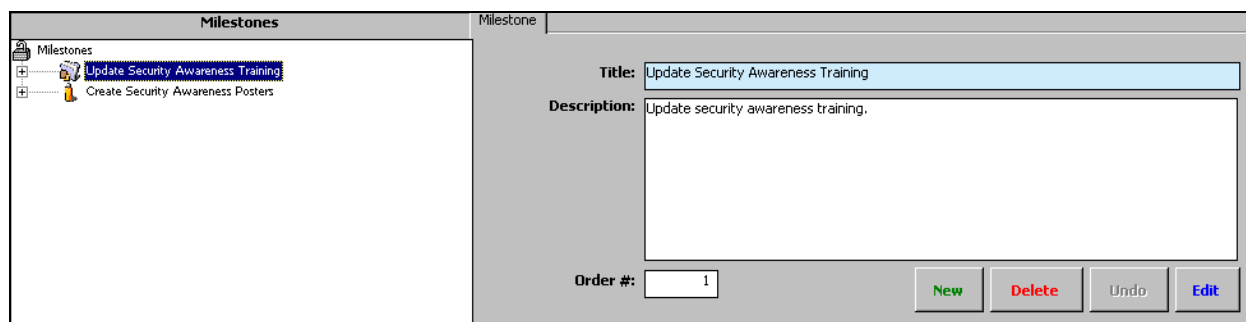
- a. Right-click the Treeview “Milestones” root node in the **Milestones** dialog window and select the following “Add Milestone” pop-up menu.

Figure 8-10. Milestone node “Add Milestone” pop-up menu



- b. Select any Milestone name node in the Treeview to display its **Milestone** sub-form to the right of the Treeview window.

Figure 8-11. Milestone sub-form method of adding Milestones



- c. Selecting **New** in its **Milestone** sub-form opens a new **Milestone** sub-form in the **Action Plan** form. It is not important which Milestone is selected when adding a new Milestone.

Either method opens the **Milestone** sub-form in the **Action Plan** form in ADD mode (Figure 8-12). To complete the **Milestone** form, proceed to the next section, 8.5.1.3.

8.5.1.3 Completing the Milestone Form

Figure 8-12 displays the **Milestone** sub-form inside the **Action Plan** form in ADD mode but the only area that can be modified is the **Milestone** sub-form. The blue highlighted areas depicted in the Figure 8-12 cannot be edited or modified while the **Milestone** sub-form is in ADD mode.

8.5.1.3.1 Title Field

The “Title” field is limited to 50 characters, including spaces. The “Title” *must not* include any contractor-, location-, or system-specific information, or other sensitive or identifying information. It is used only to provide a descriptive name to the Milestone so it can be distinguished from other Milestones.

8.5.1.3.2 Description Field

The “Description” field does not include any sensitive or identifying information restrictions. Include sufficient data to permit oversight and tracking.

8.5.1.3.3 Order # Field

The “Order #” field is used to arrange or re-arrange multiple Milestones into their order of completion.

Figure 8-12. Action Plan form Milestone sub-form

IMPORTANT: Do NOT include any Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the “Title” field. The CISS application cannot validate this field for sensitive or identifying information, so the SSO must validate the “Title” field prior to submitting any Action Plan or POA&M information to CMS.

NOTE: The Milestone title becomes locked when an Action Plan is submitted to CMS and can no longer be modified.

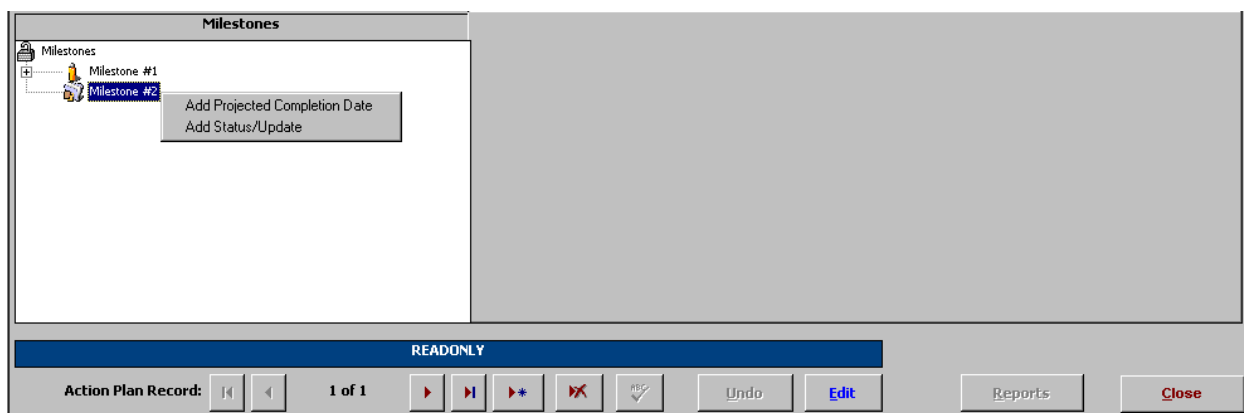
8.5.1.4 Finalizing the Milestone Form

Select **Save** to save the Milestone data or select **Undo** to close the form *without* saving the Milestone. There is no confirmation or warning message if **Undo** is selected—all new or modified data will be lost. Both buttons return the user to the **Action Plan** form in READONLY mode (Figure 8-1). Selecting **Close** closes the **Action Plan** form and returns to the CISS main menu.

After a Milestone has been added to an Action Plan, the **Milestones** dialog window Treeview root node [i.e., Milestone_Root(NONE)] is renamed to “Milestones,” and it displays a lower-level node for each existing Milestone (Figure 8-11). Expanding the Milestone node displays the updated information. After a new Milestone has been created, there are two other Milestone-related sub-forms, **Projected Date** and **Status Update**, that must also be populated.

Right-clicking the desired Treeview Milestone node displays the following pop-up menu for the two sub-forms. The following sections explain how to complete the two sub-forms.

Figure 8-13. Milestone node pop-up menu



8.5.2 Adding Projected Completion Dates

The initial (i.e., first) Projected Completion Date of a new Milestone can only be added using the procedure in the next section, 8.5.2.1. However, that same procedure can also be used to add subsequent (i.e., follow-on) Projected Completion Dates to a Milestone. The procedure in the section 8.5.2.2 can also be used to add subsequent Projected Completion Date, but not the initial Projected Completion Date to a new Milestone.

NOTE: While adding or editing any **Action Plan** sub-form (i.e., **Milestone**, **Project Date**, or **Status Update** forms), all **Action Plan** buttons and fields are disabled so its data cannot be changed.

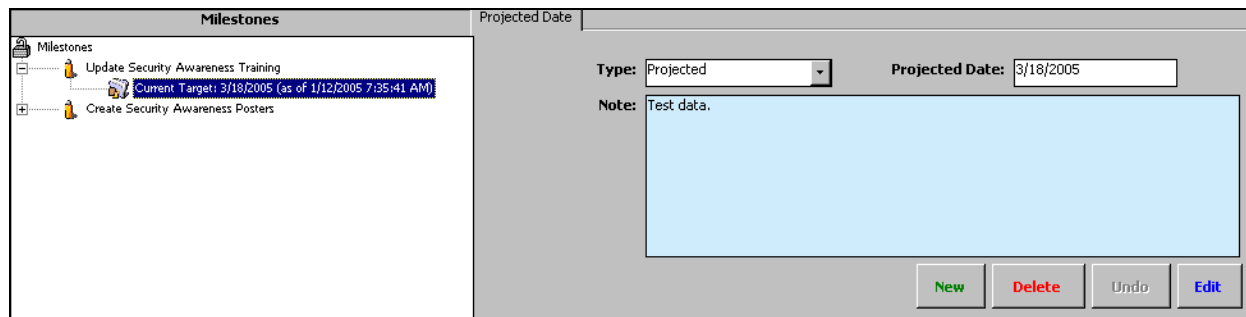
8.5.2.1 Creating the Initial Projected Completion Date

Right-click the desired Treeview Milestone node (refer to section 3.4.2) and select the “Add Projected Completion Date” pop-up menu (Figure 8-13). This opens a new **Projected Date** sub-form inside the **Action Plan** form (Figure 8-15). To complete the **Projected Date** form, proceed to section 8.5.2.3.

8.5.2.2 Adding Subsequent Projected Completion Dates

In addition to the method stated in the previous section, 8.5.2.1, a subsequent (i.e., follow-on) Projected Completion Date can be entered by selecting any Treeview Projected Completion Date node. The selected nodes **Projected Date** sub-form displays to the right of the Treeview dialog window.

Figure 8-14. Adding a subsequent Projected Completion Date



Selecting **New** in its **Projected Date** sub-form opens a new **Projected Date** sub-form in the **Action Plan** form (Figure 8-15). It is not important which target date node is highlighted when adding new projected dates as long as the target date node is a sub-node of the desired Milestone.

Either method opens the following **Projected Date** sub-form in the **Action Plan** form in ADD mode. To complete the **Projected Date** form, proceed to the next section, 8.5.2.3.

8.5.2.3 Completing the Projected Date Form

The following figure displays the **Projected Date** sub-form inside the **Action Plan** form in ADD mode but the only area that can be modified is the **Projected Date** sub-form. The blue highlighted areas depicted in the following figure cannot be edited or modified while the **Projected Date** sub-form is in ADD mode.

Figure 8-15. Action Plan form Projected Date sub-form

8.5.2.3.1 Type Field

The “Type” field has two selections, “Projected” and “Actual.” Normally, a date is “Projected” when specifying a future Milestone date and “Actual” when specifying a known date, such as when closing a Milestone.

8.5.2.3.2 Projected Date Field

Double-clicking in the “Projected Date” field displays a pop-up calendar where the date can be selected from the displayed calendar.

8.5.2.3.3 Note Field

The “Note” field *must not* include any contractor-, location-, or system-specific information, or other sensitive or identifying information.

IMPORTANT: Do NOT include any Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the “Note” field. The CISS application cannot validate this field for sensitive or identifying information, so the SSO must validate the “Note” field prior to submitting any Action Plan or POA&M information to CMS.

8.5.2.3.4 Finalizing the Form

Select **Save** to save the Milestone data or select **Undo** to close the form *without* saving the data. There is no confirmation or warning message if **Undo** is selected—all new or modified

data will be lost. Both buttons return the user to the **Action Plan** form in READONLY mode (Figure 8-1). Expanding the Milestone node displays the updated information. Note that the **Action Plan** form “Completion Dates” area may be updated (if applicable) to reflect the “Initial Target” and “Current Projected” date information (refer to section 8.5.4).

Selecting **Close** closes the **Action Plan** form and returns to the CISS main menu.

8.5.3 Adding Status Updates

The initial (i.e., first) Status Update of a Milestone can only be added using the procedure in the next section, 8.5.3.1. However, that same procedure can also be used to add subsequent (i.e., follow-on) Status Updates to a Milestone. The procedure in the subsequent section, 8.5.3.2, can also be used to add subsequent Status Updates, but not the initial Status Update to a Milestone.

NOTE: While adding or editing any **Action Plan** sub-form (i.e., **Milestone**, **Project Date**, or **Status Update** forms), all **Action Plan** buttons and fields are disabled so its data cannot be changed.

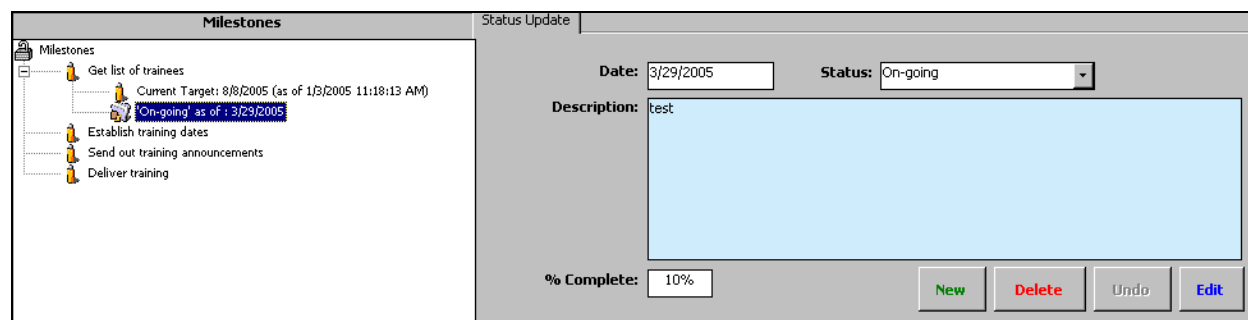
8.5.3.1 Creating the Initial Status Update

Right-click the desired Treeview Milestone node and select the “Add Status/Update” pop-up menu (Figure 8-13). This opens a new **Status Update** sub-form inside the **Action Plan** form (Figure 8-17). To complete the **Status Update** form, proceed to section 8.5.3.3.

8.5.3.2 Adding Subsequent Status Updates

In addition to the procedures stated in the previous section, 8.5.3.1, a subsequent (i.e., follow-on) Status Update can be entered by selecting any Treeview Status Update node. The following selected node’s **Status Update** sub-form displays to the right of the Treeview dialog window.

Figure 8-16. Preparing to add a subsequent Status Update



Selecting **New** at the bottom of the **Status Update** form opens a blank **Status Update** form so a new Status Update can be added (Figure 8-17). It is not important which on-going or status node is highlighted when adding new Status Updates as long as the node is below the desired Milestone. The “Date” field in the form is used to update the “Completion Dates” fields (if applicable) and to set the current on-going status order below each Milestone.

Either method opens the **Status Update** sub-form in the **Action Plan** form in ADD mode (Figure 8-17). To complete the **Status Update** form, proceed to the next section, 8.5.3.3.

8.5.3.3 Completing the Status Update Form

The following figure displays the **Status Update** sub-form inside the **Action Plan** form in ADD mode but the only area that can be modified is the **Status Update** sub-form. The blue highlighted

areas depicted in the following figure cannot be edited or modified while the **Status Update** sub-form is in ADD mode.

Figure 8-17. Action Plan form Status Update sub-form

8.5.3.3.1 Date Field

Double-clicking in the “Date” field displays a pop-up calendar where the date can be selected from the displayed calendar.

8.5.3.3.2 Status Field

The “Status” field displays a drop-down menu where the desired status type can be selected.

8.5.3.3.3 Description Field

The “Description” field *must not* include any contractor-, location-, or system-specific information, or other sensitive or identifying information. However, it should include sufficient data to permit oversight and tracking.

IMPORTANT: Do NOT include any Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the “Description” field. The CISS application cannot validate this field for sensitive or identifying information, so the SSO must validate the “Description” field prior to submitting any Action Plan or POA&M information to CMS.

8.5.3.3.4 Percent Completed Field

In the “% Complete” field, input a percentage (e.g., .15 = 15%) that represents an estimation of the Milestone completion.

8.5.3.3.5 Finalizing the Form

Select **Save** to retain the update data and **Undo** to close the form *without* saving the data. There is no confirmation or warning message if **Undo** is selected—all new or modified data will be lost. Both buttons return the user to the **Action Plan** form (Figure 8-1). Expanding the Milestone node displays the updated information. Note that the **Action Plan** form “Completion Dates” area may be updated (if applicable) to reflect the “Initial Target” and “Current Projected” or “Actual” date information (refer to the next section, 8.5.4).

Selecting **Close** closes the **Action Plan** form and returns to the CISS main menu.

8.5.4 Action Plan Completion Dates

When Projected Completion Dates or Status Updates are added to Milestones, the “Completion Dates” area of the following **Action Plan** form may update to reflect any updates or changes made. The “Initial Target” date will continue to update/change based on the latest projected Milestone date information until the Action Plan has been submitted in a POA&M report to CMS (refer to Chapter 12.0). When the POA&M is submitted, the “Initial Target” date field is locked and can never be changed—it will always remain the “Initial Target Date.” However, the “Current Projected” date field will continue to update/change based on the latest projected Milestone update status date information.

Figure 8-18. Action Plan Completion Dates area

The screenshot displays a web form interface. At the top, a yellow box titled "Completion Dates" contains the following fields: "Initial Target: 8/8/2005", "Current Projected: 8/8/2005", "Actual:", and "Status:". To the right of this box are three labels: "* Estimated Annual Maintenance:", "* Percent Security:", and "* Percent Applied To CMS:". Below the yellow box is a section titled "Milestones" which contains a tree view. The tree view has a root node "Milestones" with a sub-node "Current Target: 8/8/2005 (as of 1/3/2005 11:18:13 AM)". Underneath this sub-node are four tasks, each with a small icon: "Get list of trainees", "Establish training dates", "Send out training announcements", and "Deliver training".

The “Actual Date” field will not be filled-in until the “Status” field in the following **Status Update** form reflects a “Closed” or “Closed Pending” status.

Figure 8-19. Status Update form Status field

The screenshot shows a 'Status Update' dialog box. It contains a 'Date' text field, a 'Status' dropdown menu, a large 'Description' text area (highlighted in light blue), and a '% Complete' text field. The 'Status' dropdown menu is open, showing four options: 'Ongoing', 'Closed Pending', 'Closed', and 'Delayed'. At the bottom right, there are four buttons: 'New', 'Delete', 'Undo', and 'Save'.

Selecting **Close** closes the *Action Plan* form and returns to the CISS main menu.

8.6 Action Plan Links or Associations

The following figure displays an *Action Plan* form in READONLY mode. In READONLY mode, the fields depicted in the blue highlighted area of this figure cannot be modified. Only the non-blue highlighted dialog window areas are selectable. Although the *Milestones* Treeview dialog window is selectable, this section explains how to add or remove Action Plan links or associations. The other dialog windows in the *Action Plan* form display all existing links that the selected Action Plan pertaining to POC and Weakness element records, if any.

Figure 8-20. Action Plan form READONLY mode

Action Plan

* Action Plan Title
Action Plan #1

Description
Action Plan for Weakness #1 - Known Software Weakness
Improper configuration of system software settings.

POC(s) [Add](#)
Secure, Iam - (Primary)

Weakness(es)
MED_A_2005_1: Weakness #1 - Known Software Weakness

Completion Dates	* Estimated Annual Maintenance:	Costs	Funding Sources	Target Implementation Costs
Initial Target: 2/28/2005	* Percent Security: 100%	\$20,000.00	Current: \$20,000.00	\$20,000.00
Current Projected: 2/28/2005	* Percent Applied To CMS: 0%		Reallocated: \$0.00	
Actual:			New: \$0.00	

Milestones

- Update System Configuration Documentation
- Run Password Cracking Tool

READONLY

Action Plan Record: 1 of 1

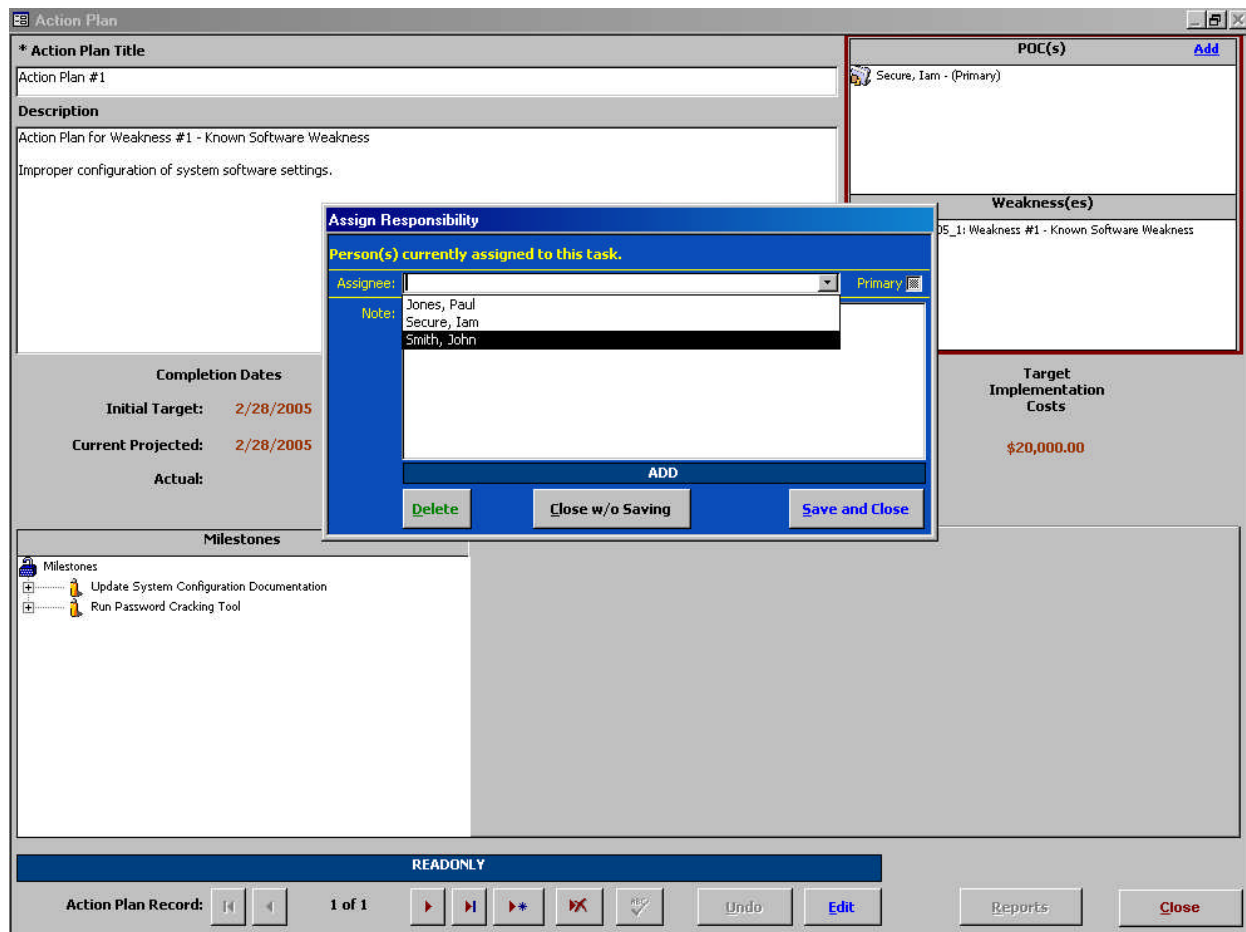
Buttons: Undo, Edit, Reports, Close

Action Plan links or associations to Weaknesses cannot be made from the **Action Plan** form. Links to Weaknesses are made in the **Weakness** form by selecting the desired Action Plan from a drop-down menu. The procedure for linking a Weakness to an Action Plan is discussed in section 7.4.5. Using the same procedure discussed in section 7.4.5 to remove an Action Plan selection removes the Weakness link to an Action Plan.

8.6.1 Adding Action Plan Links to POCs

Action Plan links can be made to other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). Action Plan links to POCs (and only POCs) can also be made from the **Action Plan** form dialog window using the [Add](#) link in the **POCs** dialog window. Clicking the [Add](#) link while in READONLY mode opens the following **Assign Responsibility** dialog.

Figure 8-21. Assign Responsibility dialog



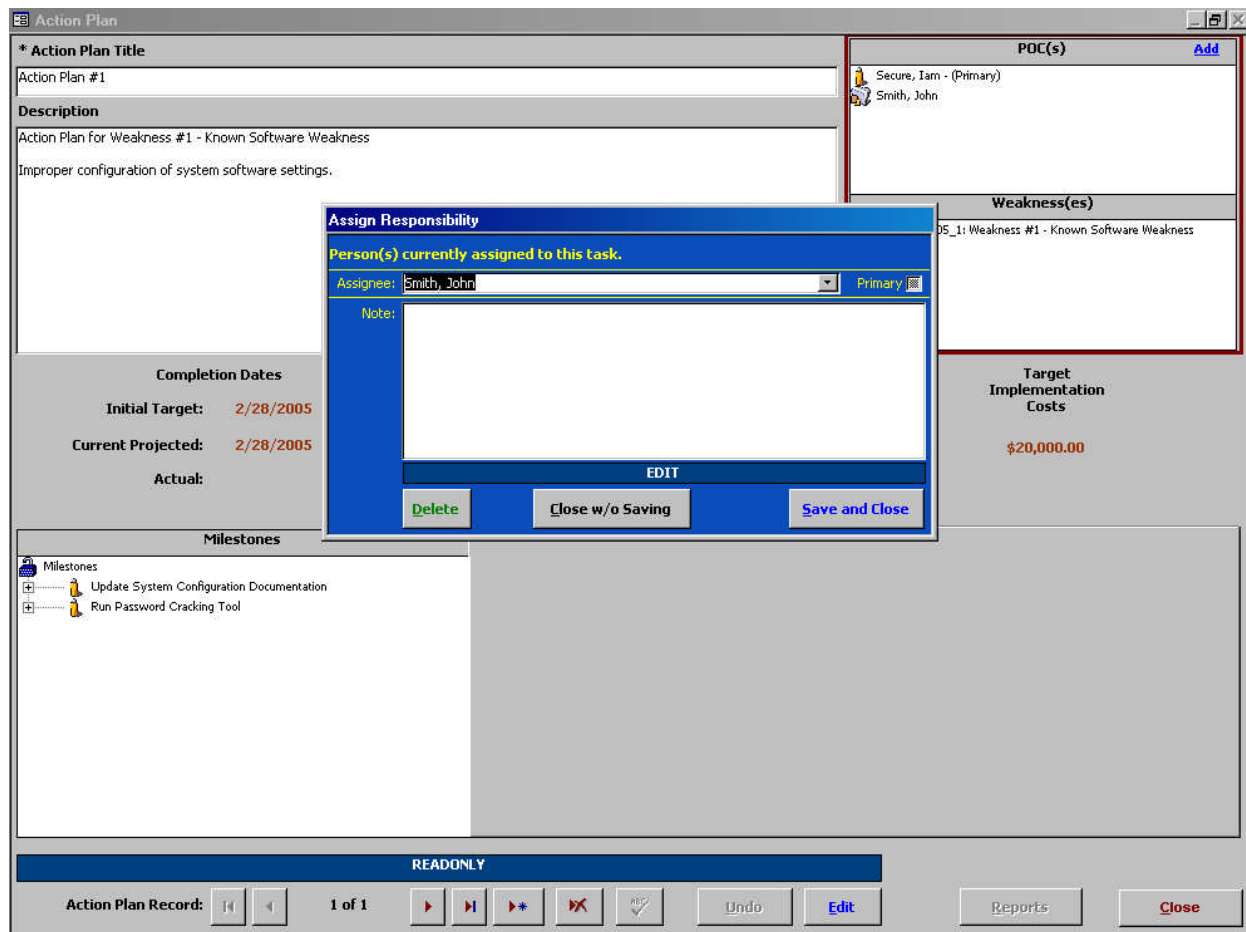
After the POC selection is made from the drop-down menu, selecting **Save and Close** saves the POC link assignment and closes the **Assign Responsibility** dialog; and selecting **Close w/o Saving** closes the form *without* making the POC link assignment. Both buttons return to the **Weakness** form with the new POC assignment displayed in its dialog window (Figure 8-22), if applicable.

Selecting **Close** closes the **Weakness** form and returns to the CISS main menu.

8.6.2 Removing Action Plan Links to POCs

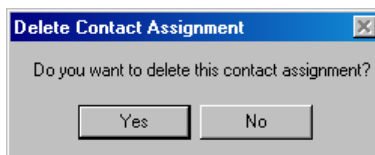
Action Plan links can be removed from other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). Action Plan links that are listed in the following **Action Plan** form **POCs** dialog window can also be removed. Double-clicking the desired POC name in the dialog window while in **READONLY** mode opens the following **Assign Responsibility** dialog.

Figure 8-22. Assign Responsibility dialog



For example, double-clicking the “Smith, John” name in the **POCs** dialog window opens the respective POC record **Assign Responsibility** dialog. Selecting **Delete** opens the following warning dialog.

Figure 8-23. Delete Contact Assignment warning message



Selecting **No** exits the warning dialog and returns to the selected Action Plan *without* removing the POC link. Selecting **Yes** *removes* the POC link *without* any further warnings or confirmations, and exits to the selected Action Plan. Selecting **Close** in the **Action Plan** form exits to the main menu.

8.7 Deleting an Action Plan Record

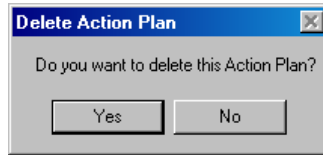
To delete an Action Plan, open the desired Action Plan record using either of the following methods to open the **Action Plan** form (Figure 8-1):

- a. Expand the Treeview region “Action Plan” major-level node or any security element node with a lower-level “Action Plan” node (refer to section 3.1.5.1). Double-click the

desired Action Plan name node to open the form in READONLY mode (refer to section 3.3). Selecting **Close** closes the form and returns to the CISS main menu, and selecting **X** displays the **Delete Action Plan** warning message (Figure 8-24).

- b. Select the Component region **Weaknesses** button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Action Plan record (refer to section 3.2). Selecting **Close** closes the form and returns to the CISS main menu, and selecting **X** displays the following Delete Action Plan warning message.

Figure 8-24. Delete Action Plan warning message

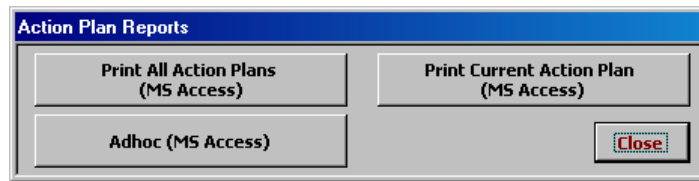


Selecting **No** in this warning message exits from the **Delete Action Plan** warning and returns to the **Action Plan** form *without* deleting the Action Plan. However, selecting **Yes** *deletes* the selected Action Plan, as well as all links to the selected Action Plan, *without* any further warnings or confirmations. Selecting **Close** closes the form and returns to the CISS main menu.

8.8 Action Plan Reports

MS Excel[®] PivotTable reports (refer to section 3.11) can be accessed by selecting the **Pivot Reports** button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Action Plan Reports** menu can be accessed from the Treeview region using pop-up menus or from the **Action Plan** form using the **Reports** button (Figure 8-1).


Figure 8-25. Action Plan Reports menu




NOTE: The **Print Current Action Plan (MS Access)** button (Figure 8-25) is active only if the report selection is based on a single Action Plan selection. For example, double-clicking a specific Action Plan or selecting the “Reports” pop-up menu from a specific Action Plan results in an active button because a “current” Action Plan has been identified. However, when selecting the “Reports” pop-menu from the “Action Plans” major-level node, the button is inactive because no “current” Action Plan has been identified.

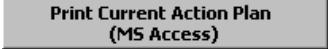
Any of the following methods can be used to open the **Action Plan Reports** menu (Figure 8-25):

- a. If the **Action Plan** form is already open, use the form record navigation buttons to navigate to the desired Weakness record (refer to section 3.2), if necessary. Then select **Reports** (Figure 8-1) to open the report menu.

- b. Expand the Treeview region “Action Plans” major-level node or any security element node with a lower-level “Action Plan” node (refer to section 3.1.5.1). Double-click the desired Action Plan name node to open the Action Plan record. Then select  (Figure 8-1) to open the report menu.
- c. Expand the Treeview region “Action Plans” major-level node or any security element node with a lower-level “Action Plan” node (refer to section 3.4.2). Right-click the “Action Plans” node or any Action Plan name node (e.g., Apply latest service packs) in any security element to display a pop-up menu that includes a “Reports” option. (Refer to Figure 3-11 for an expansion of all Treeview nodes and their available pop-up menu options.) Select “Reports” from the pop-up menu to open the report menu.

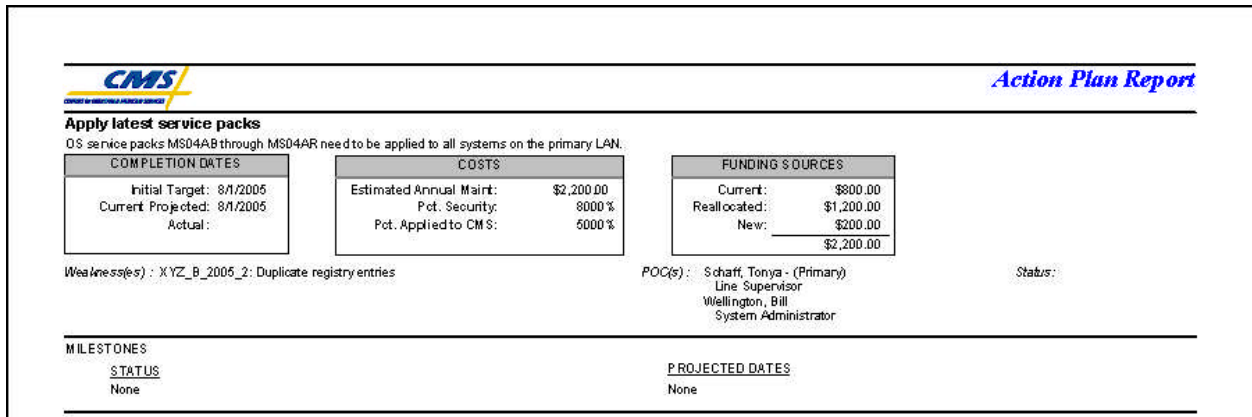
Selecting any of the report menu buttons assembles and displays the respective report (refer to the following sections for an explanation on each report). Selecting  closes the **Action Plan Reports** menu and returns to the original starting point (i.e., CISS main menu or **Action Plan** form).

8.8.1 Print Current Action Plan (MS Access)

Select , if activated, from the **Action Plan Reports** menu (Figure 8-25) to generate a report that includes all information pertaining to the selected Action Plan. Only the current or selected Action Plan is included in the report.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 8-26. Example Current Action Plan report



CMS *Action Plan Report*

Apply latest service packs
 OS service packs MS04AB through MS04AR need to be applied to all systems on the primary LAN.

COMPLETION DATES	COSTS	FUNDING SOURCES
Initial Target: 8/1/2005 Current Projected: 8/1/2005 Actual:	Estimated Annual Maint: \$2,200.00 Pot. Security: 8000 % Pot. Applied to CM S: 5000 %	Current: \$800.00 Reallocated: \$1,200.00 New: \$200.00 \$2,200.00


Weakness(es) : XYZ_B_2005_2: Duplicate registry entries

POC(s) : Schaff, Tonya - (Primary)
Line Supervisor
Wellington, Bill
System Administrator

Status:

MILESTONES	PROJECTED DATES
STATUS None	None

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 8-25).

Selecting  in the **Action Plan Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Action Plan** form).

8.8.2 Print All Action Plans (MS Access)

Select **Print All Action Plans (MS Access)** from the **Action Plan Reports** menu (Figure 8-25) to generate a report that includes all Action Plans contained in the database. The report includes all information included in all Action Plans. This Action Plan report is formatted so each Action Plan starts printing on a new page.

Once created, a report similar to the following example is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 8-27. Example All Action Planes report

CMS **Action Plan Report**

Apply FY04 CMS policies and procedures
Policies and procedures issued in FY04 have not been completely integrated into existing processes. Managers must review directives relevant to their work areas and meet with their employees to ensure process improvements effective immediately.

COMPLETION DATES	COSTS	FUNDING SOURCES
Initial Target: 2/8/2005 Current Projected: 2/1/2005 Actual:	Estimated Annual Maint: \$350.00 Pct. Security: 50 % Pct. Applied to CMS: 20 %	Current: \$0.00 Reallocated: \$0.00 New: \$0.00 \$0.00

Weakness(es): XYZ_A_2005_4: Users lack general awareness of security policy.
XYZ_A_2005_3: Operating System security hole. POC(s): Schaff, Tonya - (Primary)
Line Supervisor. Status:

MILESTONES
STATUS: None PROJECTED DATES: None

Apply latest service packs
OS service packs MS04A8 through MS04AR need to be applied to all systems on the primary LAN.

COMPLETION DATES	COSTS	FUNDING SOURCES
Initial Target: 8/1/2005 Current Projected: 8/1/2005 Actual:	Estimated Annual Maint: \$2,200.00 Pct. Security: 8000 % Pct. Applied to CMS: 5000 %	Current: \$800.00 Reallocated: \$1,200.00 New: \$200.00 \$2,200.00

Weakness(es): XYZ_A_2005_1: Test 3rd weakness. POC(s): None Assigned. Status:

MILESTONES
STATUS: None PROJECTED DATES: None

Since this is a MS Access® report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access® report Toolbar controls. Closing the report returns to the report menu (Figure 8-25).

Selecting **Close** in the **Action Plan Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Action Plan** form).

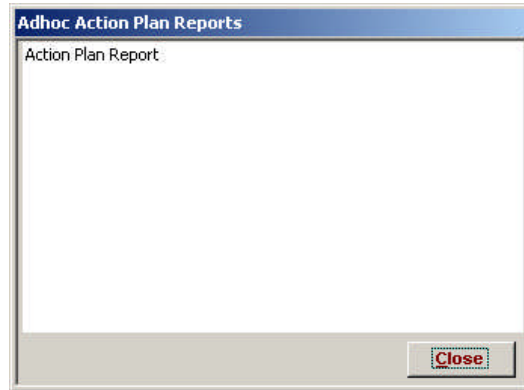
8.8.3 Adhoc (MS Access)

The Adhoc reports feature allows the user to generate a customized report that is based on user-selected filters (or parameters) and includes only user-specified information. For example, an Adhoc report can be created that includes only the Action Plans assigned to a specific POC(s) or Weakness(es). These examples are only a small sample of how reports can be customized to meet specific needs. Although these reports include only the Action Plans based on user-specified filters, all of the information pertaining to each Action Plan is included in the report. The Action Plans are printed one after the other with no page breaks between each Action Plan.

8.8.3.1 Adhoc Report Selection

Select **Adhoc (MS Access)** from the *Action Plan Reports* menu (Figure 8-25). This opens the following *Adhoc Action Plan Reports* dialog with the following Adhoc report selection.

Figure 8-28. Adhoc Action Plan Reports dialog



Selecting **Close** closes the dialog and returns to the *Action Plan Reports* menu (Figure 8-25).

8.8.3.2 Adhoc Report Filter Selection

The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

9.0 Systems

This Chapter will be expanded in a future revision of the User Guide.

9.1 Risk Assessment and Contingency Planning Schedules

This section will be expanded in a future revision of the User Guide and CISS. When the Systems functional area of the CISS is developed, the CISS will allow users to maintain Risk Assessment and Contingency Plan dates and review schedules.



10.0 Audits

The Audits feature is new with the CISS application. It enables security Audit (or Review) Findings to be associated with Weaknesses, and tracked and reported in the POA&M. Security Audits can be performed by internal (e.g., Annual Compliance Audit) or external (e.g., SAS 70 or CFO/EDP Audits) sources. In general, all security-related Findings resulting from Audits should be entered into the CISS and associated with at least one Weakness. If no Weakness corresponding to a particular Finding exists, then one must be created (refer to Chapter 7.0).


As described in section 3.1, one of the major-level nodes in the Treeview region is an “Audits” node (Figure 3-4). However, the Component region of the main menu does not include an Audits button, so only the Treeview region interface can be used to open Audit records in the CISS application.

This Chapter explains the mechanics of using the CISS to document and manage security Audits. Consult BPSSM Appendix A for a review of the relationship among Audits, Findings, and Weaknesses in the CISS application, and guidance on completing Audits. Users are strongly encouraged to become familiar with all the criteria and guidance contained in BPSSM Appendix A *before* attempting to use the CISS to complete Audits.

10.1 Creating a New Audit Record

To create a new Audit record, right-click the Treeview region “Audits” major-level node and select “Add” from the pop-up menu (refer to section 3.4.2). This opens a blank **Audits and Review** form (Figure 10-1) in ADD mode (refer to section 3.3). Selecting  and  closes the form *without* saving the new record and returns to the CISS main menu. To complete the **Audits and Reviews** form, proceed to section 10.4.




10.2 Opening an Audit Record


Expand the Treeview region “Audits” or “Findings” major level nodes to the desired Audit name (refer to section 3.1.5.1). Double-click the Audit name node to open the form (Figure 10-1) in READONLY mode (refer to section 3.3). There are no lower-level Audit nodes under other security element nodes. Selecting  closes the form and returns to the CISS main menu.

To complete the **Audits and Reviews** form, proceed to section 10.4.

10.3 Editing an Audit Record

To edit an existing Audit record, use either of the following methods to open the **Audits and Reviews** form (Figure 10-1):

- a. Expand the Treeview region “Audits” or “Findings” major level nodes to the desired Audit name. Right-click the Audit name node and select “Edit” from the pop-up menu (refer to section 3.4.2). This opens the selected **Audit** form in EDIT mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Expand the Treeview region “Audits” or “Findings” major level nodes to the desired Audit name (refer to section 3.1.5.1). Double-click the Audit name node to open the form in READONLY mode (refer to section 3.3). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.

When opening an existing Audit for editing, the  button may be disabled because it has been reported in a POA&M. This button is disabled automatically by the CISS whenever Findings related to the Audit are reported to CMS in the POA&M (refer to Chapter 12.0).

All the fields with a white input background in Figure 10-1 are unlocked and they can be modified while the form is in EDIT mode. The blue-highlighted area in Figure 10-1 depicts the **Findings** dialog window which is not locked by the POA&M submission process but cannot be modified or edited from the **Audits and Reviews** form.

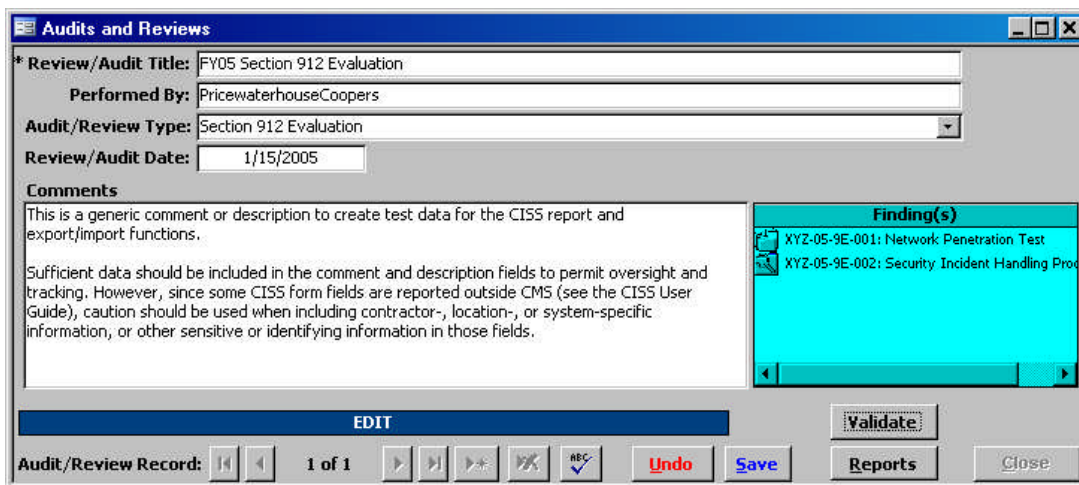
To complete the **Audits and Reviews** form, proceed to the next section, 10.4.

10.4 Completing the Audits Form

Ensure the **Audits and Reviews** form is in the proper mode (refer to section 3.3). To add a new Audit record, the form must be in ADD mode; to edit an existing Audit record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified.

Although the following figure displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes. In READONLY mode, the form fields cannot be modified. Only the unlocked form fields in the non-blue highlighted area depicted in the following figure can be edited or modified while in EDIT or ADD mode.

Figure 10-1. Audits and Reviews form EDIT mode



The screenshot shows a window titled "Audits and Reviews" with the following fields and content:

- * Review/Audit Title:** FY05 Section 912 Evaluation
- Performed By:** PricewaterhouseCoopers
- Audit/Review Type:** Section 912 Evaluation
- Review/Audit Date:** 1/15/2005
- Comments:** This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.
- Finding(s) window:**
 - XYZ-05-9E-001: Network Penetration Test
 - XYZ-05-9E-002: Security Incident Handling Proc
- Form Mode:** EDIT
- Buttons:** Validate, Undo, Save, Reports, Close
- Navigation:** Audit/Review Record: 1 of 1

10.4.1 Review/Audit Title Field

Input a descriptive “Review/Audit Title,” such as the fiscal year and abbreviated type of the audit/review. The “Review/Audit Title” is a required field and it is limited to 50 characters, including spaces.

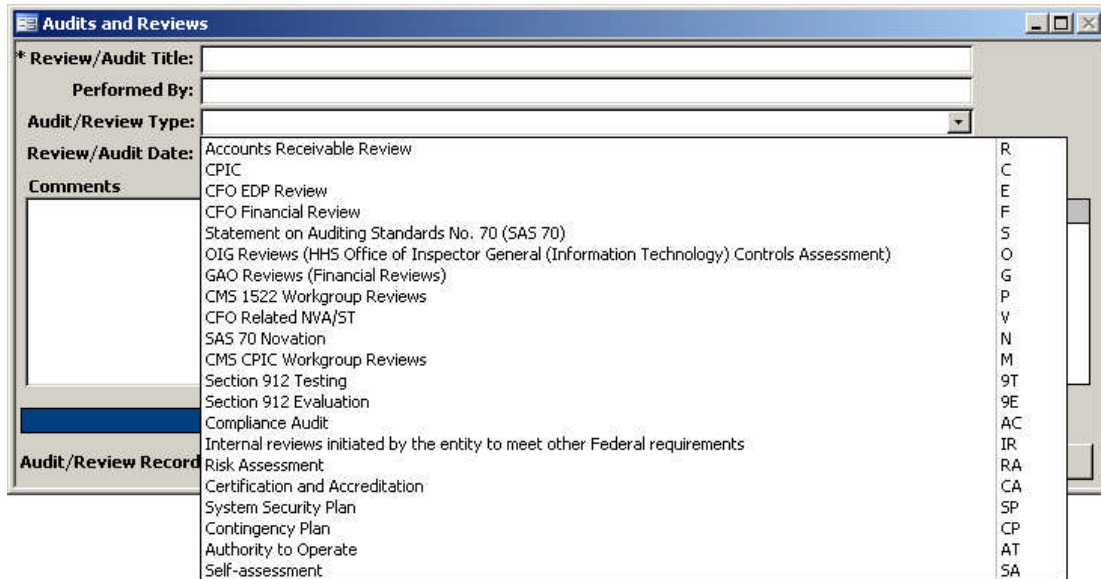
10.4.2 Performed By Field

The “Performed By” field should be completed with the name of the firm/agency that performed the review/audit.

10.4.3 Audit/Review Type Field

The “Audit/Review Type” field can only be completed by selecting the Type from the following drop-down selection menu.

Figure 10-2. Audit/Review Type drop-down selection menu







10.4.4 Review/Audit Date Field

Double-clicking in the “Review/Audit Date” field displays a pop-up calendar where the date can be selected from the displayed calendar.

10.4.5 Comments Field


The “Comments” field does not include any sensitive or identifying information restrictions. Include for any information deemed necessary by the Business Partner.

10.4.6 Finalizing the Form

When done completing the form fields, select  to spell-check the data input fields. Then select  to save the form information or select  to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if  is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode.

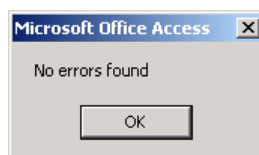
Selecting  closes the **Audits and Reviews** form and returns to the CISS main menu.

10.4.7 Validating Audits

The CISS application can run an internal self-check routine to validate the Audit against established criteria. To validate the current Audit, select  from the **Audits and Reviews** form (Figure 10-1).

If no errors are found during the validation process, the following dialog displays.

Figure 10-3. Audit Validate confirmation message



Otherwise, an error report similar to the following example is prepared in MS Word® and displayed for the user to review. This error report can be printed or saved for further review.

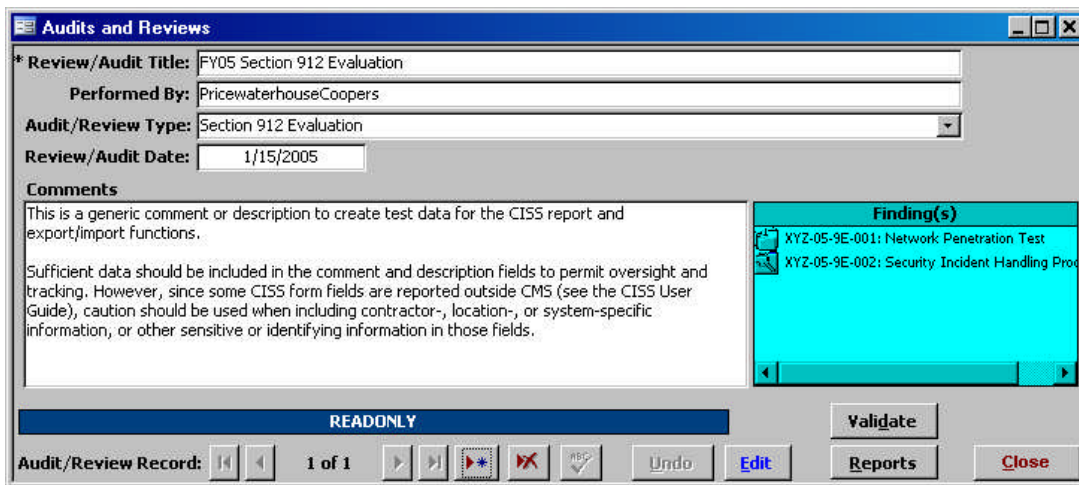
Figure 10-4. Example Audit validation error report



10.5 Audit Links or Associations

The following figure illustrates an **Audits and Reviews** form with the **Finding(s)** dialog window highlighted in blue. Although the highlighted **Finding(s)** dialog window displays existing links or associations to Findings, if any, this dialog area is not active or selectable in the **Audits and Reviews** form. All links must be made from the **Findings** form (refer to section 11.4.12).

Figure 10-5. Audits and Reviews form Finding(s) dialog window

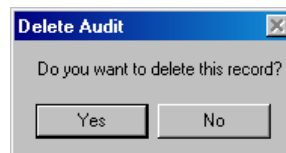


10.6 Deleting an Audit Record

Expand the Treeview region “Audits” or “Findings” major-level nodes to the desired Audit name (refer to section 3.1.5.1). Double-click the Audit name node to open the form in READONLY mode (refer to section 3.3).

Selecting closes the form and returns to the CISS main menu, and selecting displays the following **Delete Audit** warning message.

Figure 10-6. Delete Audit warning message



Selecting in this warning message exits from the **Delete Audit** warning and returns to the **Audits and Reviews** form *without* deleting the Audit. However, selecting *deletes* the selected Audit, as well as all links to the selected Audit, *without* any further warnings or confirmations. Selecting in the resultant form exits to the main menu.

10.7 Audit Reports



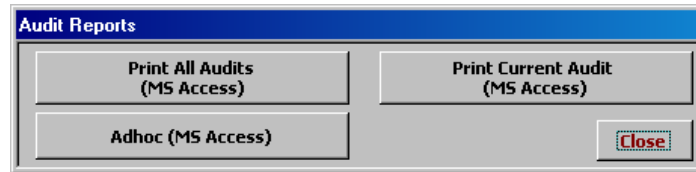



MS Excel[®] PivotTable reports (refer to section 3.11) can be accessed by selecting the  button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Audit Reports** menu can be accessed from the Treeview region using pop-up menus or from the **Audits and Reviews** form using the  button (Figure 10-5).


Figure 10-7. Audit Reports menu




NOTE: The  button (Figure 10-7) is active only if the report selection is based on a single Audit selection. For example, double-clicking a specific Audit or selecting the “Reports” pop-up menu from a specific Audit results in an active button because a “current” Audit has been identified. However, when selecting the “Reports” pop-menu from the “Audits” major-level node, the button is inactive because no “current” Audit has been identified.

Any of the following methods can be used to open the **Audit Reports** menu (Figure 10-7):

- If the **Audits and Reviews** form is already open, use the form record navigation buttons to navigate to the desired Audit record (refer to section 3.2), if necessary. Then select  (Figure 10-5) to open the report menu.
- Expand the Treeview region “Audits” or “Findings” major-level nodes to the desired Audit name (refer to section 3.1.5.1). There are no lower-level Audit nodes under other security element nodes. Double-click the Audit name node to open the Audit record. Then select  (Figure 10-5) to open the report menu.
- Expand the Treeview region “Audits” or “Findings” major-level nodes to the desired Audit name. Right-click the “Audits” major-level node or any Audit name node to display a pop-up menu that includes a “Reports” option (refer to section 3.4.2). Select “Reports” from the Treeview node pop-up menu to open the report menu.

Selecting any of the report menu buttons assembles and displays the respective report (refer to the following sections for an explanation on each report). Selecting  closes the **Audit Reports** menu and returns to the original starting point (i.e., CISS main menu or **Audits and Reviews** form).

10.7.1 Print Current Audit (MS Access)

Select , if activated, from the **Audit Reports** menu (Figure 10-7) to generate a report that includes all information pertaining to the selected Audit. Only the current or selected Audit is included in the report.

Once created, a report similar to following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 10-8. Example Current Audit report

The screenshot shows an 'Audit Report' form with the following details:

- Audit Name #1**
- Type:** Statement on Auditing Standards No. 70 (SAS 70)
- Notes:**
- Table:**

Finding	Risk	Severity Type	Status
MED-05-S-003 : Finding #1 - Default Passwords	High	Reportable Condition	On-going
- Author:** PWC
- Date:** 12/1/2004

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 10-7).

Selecting **Close** in the **Audit Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Audits and Reviews** form).

10.7.2 Print All Audits (MS Access)

Select **Print All Audits (MS Access)** from the **Audit Reports** menu (Figure 10-7) to generate a report that includes all Audits contained in the database. The report includes all information included in all Audits. The Audits are printed one after the other with no page breaks between each Audit.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 10-9. Example All Audits report

The screenshot shows an 'All Audits' report with two distinct audit sections:

- Audit Name #1**
 - Type:** Statement on Auditing Standards No. 70 (SAS 70)
 - Notes:**
 - Table:**

Finding	Risk	Severity Type	Status
MED-05-S-003 : Finding #1 - Default Passwords	High	Reportable Condition	On-going
 - Author:** PWC
 - Date:** 12/1/2004
- Audit Name #2**
 - Type:** OIG Reviews (HHS Office of Inspector General (Information Technology) Controls Assessment)
 - Notes:**
 - Table:**

Finding	Risk	Severity Type	Status
MED-05-C-005 : Finding #2 - Compromised Password	Medium	Reportable Condition	On-going
 - Author:** BAH
 - Date:** 1/5/2005

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 10-7).

Selecting **Close** in the **Audit Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Audits and Reviews** form).

10.7.3 Adhoc (MS Access)

The Adhoc reports feature allows the user to generate a customized report that is based on user-selected filters (or parameters) and includes only user-specified information. Although these reports include only the Audits based on user-specified filters, all of the information pertaining to each Audit is included in the report. The Audits are printed one after the other with no page breaks between each Audit.

10.7.3.1 Adhoc Report Selection

Select **Adhoc (MS Access)** from the **Audit Reports** menu (Figure 10-7). This opens the following **Adhoc Audit Reports** dialog with the following Adhoc report selection.

Figure 10-10. Adhoc Audit Reports dialog




Selecting **Close** closes the dialog and returns to the **Audit Reports** menu (Figure 10-7).

10.7.3.2 Adhoc Report Filter Selection

The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

11.0 Findings





The Findings feature is new with the CISS application. It enables security Audit (or Review) Findings to be associated with Weaknesses, and tracked and reported in the POA&M. In general, all security-related Findings reported from Audits or Reviews should be entered into the CISS and associated with at least one Weakness and an Action Plan to remediate the Weakness. If no Weakness corresponding to a particular Finding exists, then one must be created (refer to Chapter 7.0).






As described in section 3.1, one of the major-level nodes in the Treeview region is a “Findings” node (Figure 3-4). In addition, the Component region of the main menu includes a  button (Figure 3-4). Findings lower-level nodes are also present under other major-level security element nodes. Any of these CISS main menu interfaces can be used to open Finding records in the CISS application.

This Chapter explains the mechanics of using the CISS to document and manage security Findings. Consult BPSSM Appendix A for a review of the relationship among Audits, Findings, and Weaknesses in the CISS application, and guidance on completing Findings. Users are strongly encouraged to become familiar with all the criteria and guidance contained in BPSSM Appendix A *before* attempting to use the CISS to complete Findings.

11.1 Creating a New Finding Record

To create a new Finding record, use either of the following methods to open the *Findings* form (Figure 11-1):


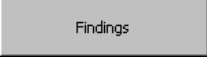

- a. Right-click the Treeview region “Findings” major-level node and select “Add” from the pop-up menu (refer to section 3.4.2). This opens a new blank form in ADD mode (refer to section 3.3). Selecting  and  closes the form *without* saving the new record and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Select  to open a new blank form in ADD mode.

Selecting  before selecting  closes the form *without* saving the new record and returns to the CISS main menu. After selecting  to open a new record, selecting  returns the form to READONLY mode *without* saving the new record. Selecting  closes the form and returns to the CISS main menu.

To complete the *Findings* form, proceed to section 11.4.







11.2 Opening a Finding Record

To open an existing Finding record, use either of the following methods to open the *Findings* form (Figure 11-1):

- a. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node (refer to section 3.1.5.1). Double-click the desired Finding name node to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.

11.3 Editing a Finding Record

To edit an existing Finding record, use either of the following methods to open the *Findings* form (Figure 11-2):

- a. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node (refer to section 3.4.2). Right-click the desired Finding name node and select “Edit” from the pop-up menu. This opens the selected *Findings* form in EDIT mode (refer to section 3.3). Selecting  closes the form and returns to the CISS main menu.
- b. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node (refer to section 3.1.5.1). Double-click the desired Finding name node to open the form in READONLY mode (refer to section 3.3). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.
- c. Select the Component region  button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Finding record (refer to section 3.2). Selecting  changes the form to EDIT mode, and selecting  closes the form and returns to the CISS main menu.

When opening an existing Finding for editing, some *Findings* form fields may not be editable because the fields are “locked.” Certain fields are locked automatically by the CISS whenever a new Finding is reported to CMS in the POA&M. A new Finding is considered any Finding not previously reported to CMS in the POA&M.

All identified Findings must be reported to CMS in the POA&M submissions (i.e., Findings associated with audit or review findings). When a Finding has been reported to CMS in the POA&M, certain fields contain information that is included in the annual CMS POA&M report required by the FISMA, and the FISMA dictates that certain information not be modified once submitted. To comply with the FISMA, one of the CISS steps during the POA&M submission process (refer to Chapter 12.0) is to lock all fields that can no longer be modified.

Figure 11-1. Findings form locked fields

To modify the *Findings* form data, proceed to the next section, 11.4.

11.4 Completing the Findings Form

Ensure the *Findings* form is in the proper mode (refer to section 3.3). To add a new Finding record, the form must be in ADD mode; to edit an existing Finding record, the form must be in EDIT mode; and in READONLY mode, none of the form fields can be modified.

Although the following figure displays the form in EDIT mode, the form functionality is the same for both EDIT and ADD modes. In READONLY mode, the form fields cannot be modified. Only the unlocked form fields in the non-blue highlighted area depicted in the following figure can be edited or modified while in EDIT or ADD mode. And, the information in the blue highlighted area can only be edited or modified while in READONLY mode (refer to the section 11.4.12).

Figure 11-2. Findings form EDIT mode

The screenshot shows the 'Findings' form in EDIT mode. At the top, there are four input fields: '* Entity' (XYZ), '* Year' (2005), '* Code' (E), and '* Num' (004). Below these is the '* Title' field containing 'Entitywide Security Plan Has Not Been Developed'. The 'Description' section contains a text area with the following content: 'XYZ-xxxx-E-004 Description: This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.' To the right of the description is a 'POCs' list with one entry: 'Smith, James - (Primary)'. Below the description are several dropdown menus: 'Weakness' (XYZ_C_2004_1: Entitywide Security Plan), 'Audit' (CFO EDP Review: FY05 CFO EDP), and 'Category' (Planning). To the right of these are 'Risk: High', '* Likelihood: Medium', and '* Impact: Significant'. Below these are radio buttons for 'FMFIA (and CPIC) Severity': 'Material Weakness', 'Reportable Condition' (selected), and 'Neither'. There is also a 'Status: Delayed' dropdown. At the bottom right, there are 'Closed Pending Date' and 'Closed Date' fields, each with a 'Docs' button. A red error message at the bottom right reads: 'There are errors on this form. Click "Validate" to see the errors!'. At the bottom of the form, there is a 'VALIDATE' button, a 'Reports' button, and a 'Close' button. The bottom of the window shows a 'Finding Record: 1 of 1' and navigation buttons, including 'Edit'.

11.4.1 Finding Identifier

Refer to BPSSM Appendix A for guidance on completing the following Finding identifier fields.

11.4.1.1 Entity Field

The “Entity” field is a required field but it is filled in by the CISS using the “Company Abbreviation” parameter value provided when the back-end database was established. If this abbreviation is not correct, refer to section 2.4.1 for information on changing the entity abbreviation.

11.4.1.2 Year Field

The “Year” field is a required field. This field represents the fiscal year in which the Finding was first identified and reported. Although it is filled-in by the CISS to reflect the current fiscal year, this field can be modified while in ADD or EDIT mode (refer to section 3.3).

11.4.1.3 Code Field

The “Code” field is a required field. Select the appropriate one or two character code from the drop-down selection that identifies the type of Review or Audit that identified the Finding.

11.4.1.4 Num Field

The “Num” field is a required field. This is the three-digit incremental Finding number assigned to each individual Finding beginning with 001, 002, 003, etc. This number is normally the same as the number assigned in the Audit or Review report.

11.4.1.5 Title Field

The “Title” field is also a required field and it is limited to 50 characters, including spaces. The “Title” should be the same finding title reported in the Audit or Review report. Refer to BPSSM Appendix A for guidance on completing this field.

11.4.2 Description Field

The “Description” field should be the same description reported in the Audit or Review report and it should provide sufficient information and detail to allow CMS to evaluate the Finding. If the Finding is the result of an internal Audit or Review, the Description should include the finding information required by the GAO, “Government Auditing Standards,” GAO-03-673G. Refer to BPSSM Appendix A for guidance on completing this field.

11.4.3 Weakness Link Selection

All Findings must be associated with a Weakness. The Weakness assignment is selectable from the following “Weakness” field drop-down menu selection. This selection can be made at a later time if the Weakness does not already exist.

Figure 11-3. Findings form “Weakness” selection

The screenshot shows a form with two dropdown menus. The first dropdown is labeled "Weakness:" and contains the text "MED_A_2005_1: Weakness #1 - Known Software Weakness". The second dropdown is labeled "Audit:" and contains the text "MED_B_2005_5: Weakness #2 - Impersonation". Below the "Audit:" dropdown, there is a list of options, with "MED_A_2005_1: Weakness #1 - Known Software Weakness" selected.

11.4.4 Audit Link Selection

All Findings must be associated with the Audit or Review that reported them. The Audit assignment is selectable from the following “Audit” field drop-down menu selection. This selection can be made at a later time if the Audit does not already exist.

Figure 11-4. Findings form “Audit” selection

The screenshot shows a form with three dropdown menus. The first dropdown is labeled "Weakness:" and contains the text "MED_A_2005_1: Weakness #1 - Known Software Weakness". The second dropdown is labeled "Audit:" and contains the text "Statement on Auditing Standards No. 70 (SAS 70): Audit Name #1". The third dropdown is labeled "Category:" and contains the text "OIG Reviews (HHS Office of Inspector General (Information Technology) Co". Below the "Category:" dropdown, there is a list of options, with "Statement on Auditing Standards No. 70 (SAS 70): Audit Name #1" selected.

11.4.5 Category Selection

All Findings must be assigned to a Weakness Category. The Category assignment is selectable from the following “Category” field drop-down menu selection. Consult BPSSM Appendix A for guidance on populating this field. This selection can be made at a later time.

Figure 11-5. Findings form “Category” selection

Weakness: []

Audit: []

Category: **Planning**

11.4.6 Risk Selection

All Findings must be assigned a Risk level. However, the Risk level is determined by the selections made in the “Likelihood” and “Impact” fields, so the Risk level is not selectable or editable. The following Likelihood and Impact assignments are selectable from their respective drop-down menu selections. Consult BPSSM Appendix A for guidance on populating these fields. These fields are required fields, so they must be completed before the form can be saved.

Figure 11-6. Findings form Risk “Likelihood” selection

Risk: **High**

* Likelihood: **Medium**

* Impact: Negligible, Very Low, Low, **Medium**, High, Very High, Extreme

FMFIA (and CPIC) Se: []

Material Weakness

Figure 11-7. Findings form Risk “Impact” selection

Risk: **High**

* Likelihood: **Medium**

* Impact: Insignificant, Minor, **Significant**, Damaging, Serious, Critical

FMFIA (and CPIC) Se: []

Material Weakness

Reportable Condition

11.4.7 FMFIA (and CPIC) Severity Selection

All Weaknesses must be assigned a FMFIA or CPIC Severity level. The Severity level is made by selecting either the following “Material Weakness,” “Reportable Condition,” or “Neither” options. Consult BPSSM Appendix A for guidance on populating this field. This selection can be made at a later time.

Figure 11-8. Findings form “FMFIA (and CPIC) Severity” selection

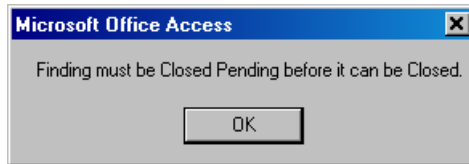
11.4.8 Status Selection

The Finding Status indicates the stage or state of the Finding condition. The Status is selectable from the following “Status” field drop-down menu selection. Consult BPSSM Appendix A for guidance on populating this field.

Figure 11-9. Findings form “Status” selection

Before a Finding Status can be “Closed,” its Status must first be reported as “Closed Pending.” If “Closed” is selected before it has been reported as “Closed Pending,” the following message displays.

Figure 11-10. Findings form “Status” error message



11.4.9 Closed Pending and Closed Date Fields

Double-clicking in the “Closed Pending Date” and “Closed Date” fields displays a pop-up calendar where the dates can be selected from the displayed calendar.

CMS requires a “Closed Pending” status to be validated before it is considered “Closed.” The “Closed Pending Date” field reflects the date the Business Partner closed the finding that is still pending CMS validation. The “Closed Date” field reflects the date that CMS validated the Finding closure and its “Closed” status.

11.4.10 Docs Buttons



Appropriate documentation is required to substantiate a “Closed Pending” or “Closed” Finding Status, including the letter from CMS confirming the closure status. This requirement applies only to those Findings that have a Finding “Year” field date of 2005 or later. To support this requirement, the  button to the right of the following “Closed Pending Date” and “Closed Date” fields will be active for any Findings with a “Year” field date of 2005 or later. If the Finding “Year” field date is prior to 2005, the  button will not be active.

Figure 11-11. Findings form “Docs” selections

The screenshot shows a form with a 'Status' dropdown menu set to 'Ongoing'. Below it are two rows of input fields. The first row is labeled 'Closed Pending Date:' and has a text input field followed by a 'Docs' button. The second row is labeled 'Closed Date:' and also has a text input field followed by a 'Docs' button.

Refer to Chapter 4.0 for details on using the **Supporting Documents** form.

When a Status of “Closed Pending” or “Closed” is selected, a pop-up calendar displays so the appropriate date can be select from the calendar. After selecting a date and the **Save** button to save the form information, the **Docs** button will be active so the required supporting documents can be attached to the Finding.

Although documentation is only required to substantiate a “Closed Pending” or “Closed” Finding Status, the **Docs** button will be active for all Findings that have a Finding “Year” field date of 2005 or later. This allows the user to include supporting documents at any time, such as when the Finding is created or updated, instead of only when closing the Finding.

All documents included as supporting documents for a Finding are included in the POA&M submission, even if the Finding Status is “Ongoing.” However, if supporting documents are not required (i.e., status other than “Closed Pending” or “Closed”), the Finding will *not* fail a Validation test if supporting documents are not included. Inversely, a Validation test will fail if supporting documents are required and none are included.

11.4.11 Finalizing the Form

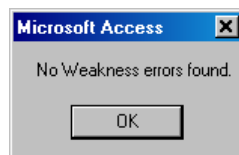
When done completing the form fields, select **ABC** to spell-check the data input fields. Then select **Save** to save the form information or select **Undo** to close the form *without* saving any of the new or modified information. There is no confirmation or warning message if **Undo** is selected—all new or modified data will be lost. Both buttons return the form to READONLY mode. To make changes to the selected Finding links or associations, proceed to section 11.5.

Selecting **Close** closes the **Findings** form and returns to the CISS main menu.

11.4.12 Validating Findings

The CISS application can run an internal self-check routine to validate the Finding against established criteria. To validate the current Finding, select **Validate** from the **Findings** form (Figure 11-16). If no errors are found during the validation process, the following dialog displays.

Figure 11-12. Finding Validate confirmation message



Otherwise, an error report similar to the following example is prepared in MS Word® and displayed for the user to review. This error report can be printed or saved for further review.

Figure 11-13. Example Finding validation error report

Finding	Error
XYZ-05-E-009	An Action Plan ("Enterprise-wide security awareness training") has a Milestone ("Send out training announcements") without a projected completion date.
	An Action Plan ("Enterprise-wide security awareness training") has a Milestone ("Establish training dates") without a projected completion date.
	An Action Plan ("Enterprise-wide security awareness training") for Weakness XYZ_A_2005_3 has a Milestone ("Deliver training") without a description.
	An Action Plan ("Enterprise-wide security awareness training") has a Milestone ("Deliver training") without a projected completion date.
	Audit/review type in Finding (XYZ-05-E-009) does not match the assigned Audit's type.

11.5 Finding Links or Associations

The following figure depicts a *Findings* form in READONLY mode. In READONLY mode, the fields depicted in the blue highlighted area cannot be modified. Only the depicted non-blue highlighted *POCs* dialog window area and the **Docs** buttons are selectable. The *POCs* dialog window displays any existing links between the selected Finding and POC element records, if any.

Figure 11-14. Findings form READONLY mode

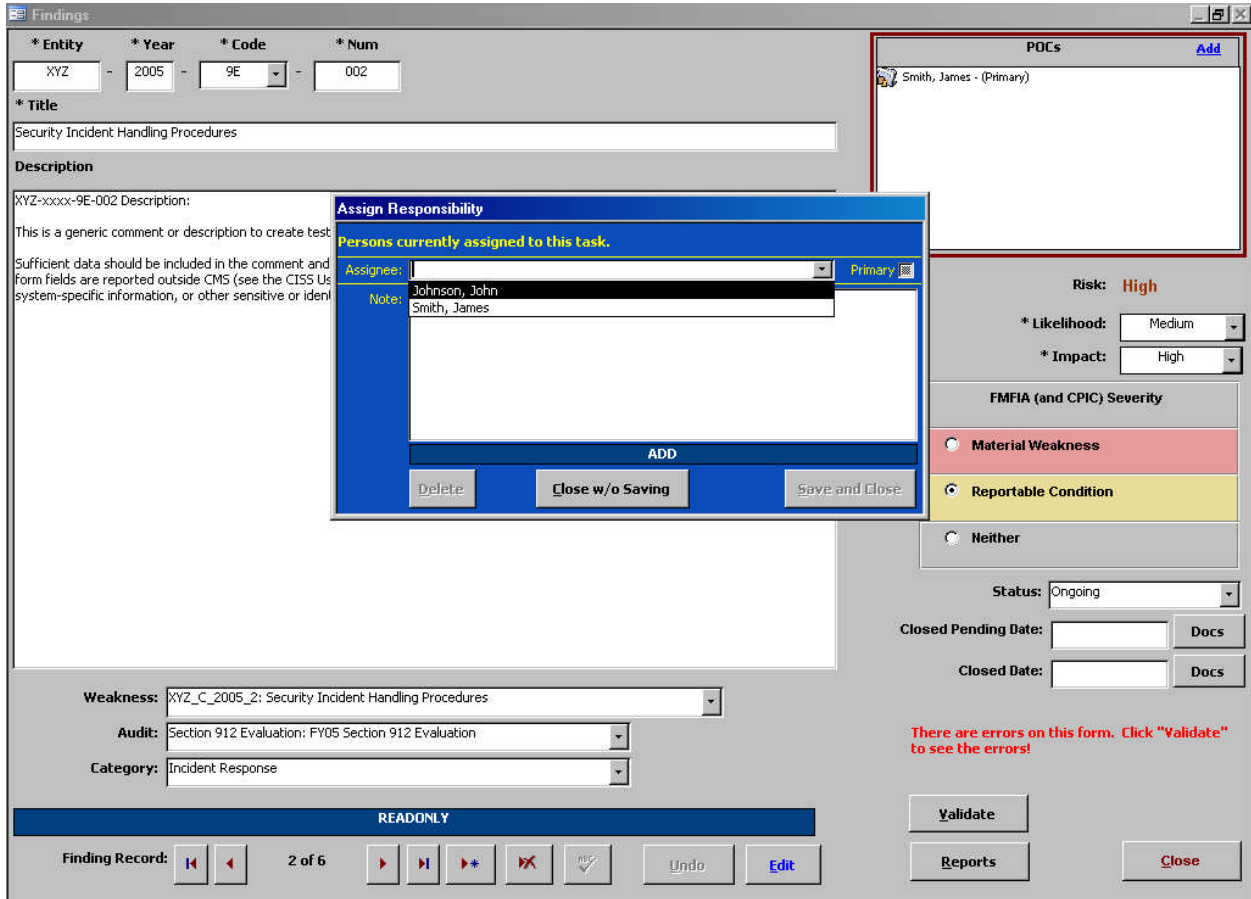
The screenshot shows the 'Findings' form in a 'READONLY' mode. The form is divided into several sections:

- Header:** Fields for * Entity (XYZ), * Year (2005), * Code (E), and * Num (004).
- Title:** Entitywide Security Plan Has Not Been Developed
- Description:** XYZ-xxxx-E-004 Description: This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS Form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.
- Weakness:** XYZ_C_2004_1: Entitywide Security Plan
- Audit:** CFO EDP Review: FY05 CFO EDP
- Category:** Planning
- POCs Dialog:** Shows a list of POCs (Smith, James - (Primary)).
- Risk:** High
- Likelihood:** Medium
- Impact:** Significant
- FMFIA (and CPIC) Severity:** Reportable Condition (selected)
- Status:** Delayed
- Closed Pending Date:** [Field] Docs
- Closed Date:** [Field] Docs
- Buttons:** Validate, Reports, Close
- Status Bar:** FINDING RECORD: 1 of 1

11.5.1 Adding Finding Links to Other Forms

Finding links can be made to other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). POC links can also be made from the **Findings** form dialog window using the **Add** link in the **POCs** dialog window. Clicking the **Add** link while in READONLY mode opens the following **Assign Responsibility** dialog.

Figure 11-15. Assign Responsibility dialog



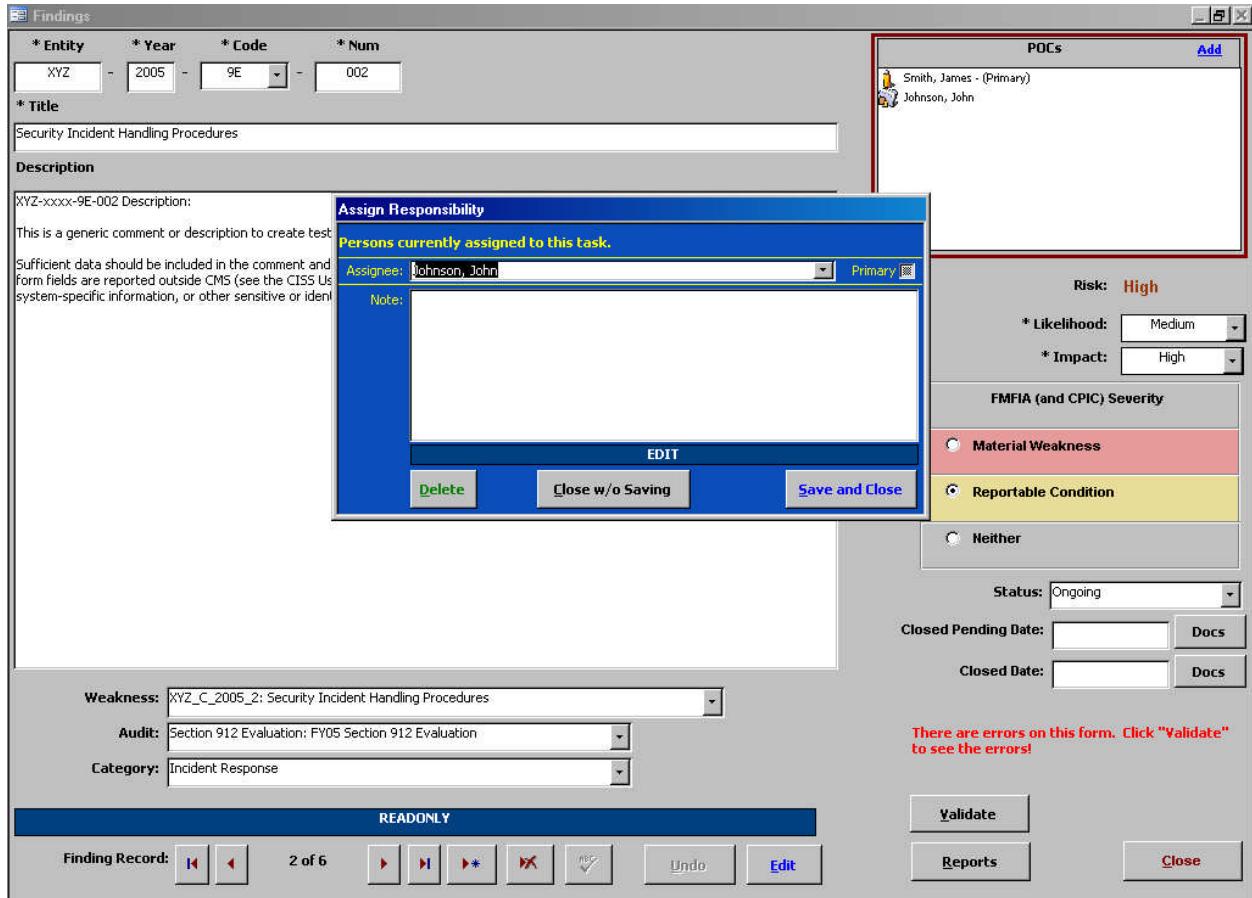
After the POC selection is made from the drop-down menu, selecting **Save and Close** saves the POC link assignment and closes the **Assign Responsibility** dialog; and selecting **Close w/o Saving** closes the form *without* making the POC link assignment. Both buttons return to the **Findings** form with the new POC assignment displayed in its dialog window (Figure 11-16), if applicable.

Selecting **Close** closes the **Findings** form and returns to the CISS main menu.

11.5.2 Removing Finding Links to Other Forms

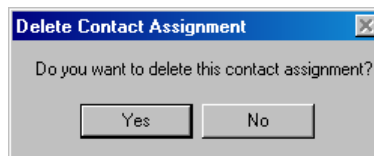
Finding links can be removed from other security elements while editing the respective security element forms (refer to the applicable User Guide security element chapters). POC links that are listed in the **Findings** form **POCs** dialog window (refer to the following figure) can also be removed. Double-clicking the desired POC name in the dialog window while in READONLY mode opens the selected POC **Assign Responsibility** dialog.

Figure 11-16. Assign Responsibility dialog



For example, double-clicking the “Johnson, John” name in the **POCs** dialog window opens the respective POC record **Assign Responsibility** dialog. Selecting **Delete** opens the following warning dialog.

Figure 11-17. Delete Contact Assignment warning message



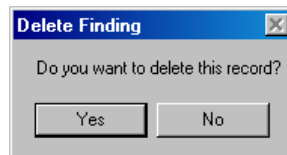
Selecting **No** exits the warning dialog and returns to the selected Finding *without* removing the POC link. Selecting **Yes** *removes* the POC link *without* any further warnings or confirmations, and exits to the selected Finding. Selecting **Close** in the **Findings** form exits to the main menu.

11.6 Deleting a Finding Record

To delete a Finding, open the desired Finding record using either of the following methods to open the **Findings** form (Figure 11-1):

- a. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node (refer to section 3.1.5.1). Double-click the desired Finding name node to open the form in READONLY mode (refer to section 3.3). Selecting closes the form and returns to the CISS main menu, and selecting displays the **Delete Finding** warning message (Figure 11-18).
- b. Select the Component region button (refer to section 3.4.1) to open the form in READONLY mode (refer to section 3.3). Use the form record navigation buttons to navigate to the desired Finding record (refer to section 3.2). Selecting closes the form and returns to the CISS main menu, and selecting displays the following **Delete Finding** warning message.

Figure 11-18. Delete Finding warning message

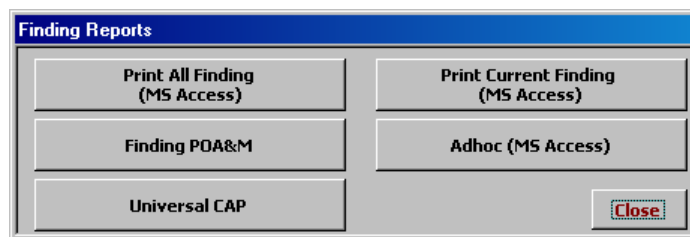


Selecting in this warning message exits from the **Delete Finding** warning and returns to the **Findings** form *without* deleting the finding. However, selecting *deletes* the selected Finding, as well as all links to the selected Finding, *without* any further warnings or confirmations. Selecting in the resultant **Findings** form exits to the main menu.

11.7 Finding Reports



MS Excel[®] PivotTable reports (refer to section 3.11) can be accessed by selecting the button located in the Component region (Figure 3-3) of the CISS menu. In addition, the following **Finding Reports** menu can be accessed from the Treeview region using pop-up menus or from the **Findings** form using the button (Figure 11-1).


Figure 11-19. Finding Reports menu



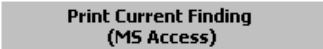
NOTE: The button (Figure 11-19) is active only if the report selection is based on a single Finding selection. For example, double-clicking a specific Finding or selecting the “Reports” pop-up menu from a specific Finding results in an active button because a “current” Finding has been identified. However, when selecting the “Reports” pop-menu from the “Findings” major-level node, the button is inactive because no “current” Finding has been identified.

Any of the following methods can be used to open the **Finding Reports** menu (Figure 11-19):

- a. If the **Findings** form is already open, use the form record navigation buttons to navigate to the desired Finding record (refer to section 3.2), if necessary. Then select  (Figure 11-1) to open the report menu.
- b. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node (refer to section 3.1.5.1). Double-click the desired Finding name node to open the Finding record. Then select  (Figure 11-1) to open the report menu.
- c. Expand the Treeview region “Findings” major-level node or any security element node with a lower-level “Findings” node. Right-click the “Findings” node or any Finding name node to display a pop-up menu that includes a “Reports” option (refer to section 3.4.2). Select “Reports” from the pop-up menu to open the report menu.

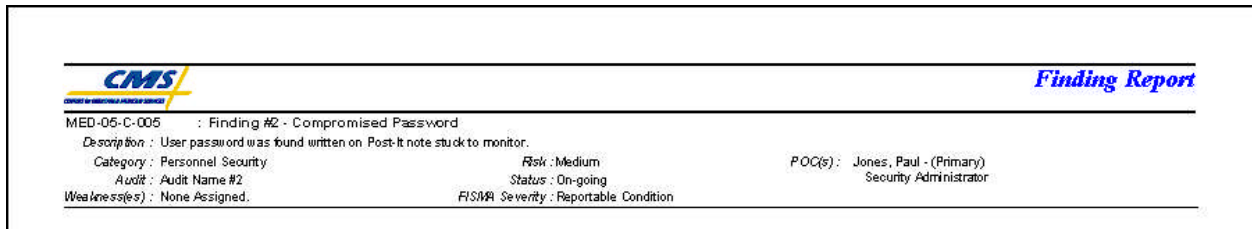
Selecting any of the report menu buttons assembles and displays the respective report (refer to the following sections for an explanation on each report). Selecting  closes the **Finding Reports** menu and returns to the original starting point (i.e., CISS main menu or **Findings** form).

11.7.1 Print Current Finding (MS Access)


Select  from the **Finding Reports** menu (Figure 11-19) to generate a report that includes all information pertaining to the selected Finding. Only the current or selected Finding is included in the report.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.


Figure 11-20. Example Current Finding report



Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 11-19).

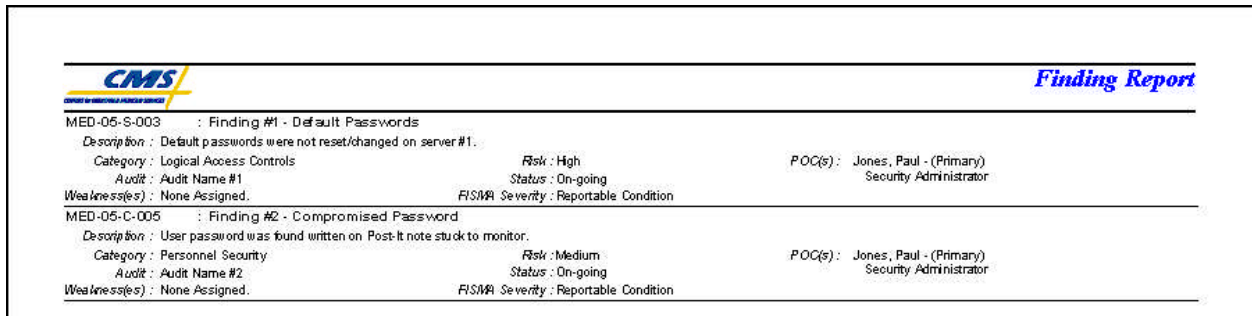
Selecting  in the **Finding Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Findings** form).

11.7.2 Print All Findings (MS Access)

Select  from the **Finding Reports** menu (Figure 11-19) to generate a report that includes all Findings contained in the database. The report includes all information included in all Findings. The Findings are printed one after the other with no page breaks between each Finding.

Once created, a report similar to the following example is available in MS Access® for the user to review or print. The report can only be saved if an application such as Adobe Acrobat® is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 11-21. Example All Findings report



Since this is a MS Access® report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access® report Toolbar controls. Closing the report returns to the report menu (Figure 11-19).

Selecting **Close** in the **Finding Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Findings** form).

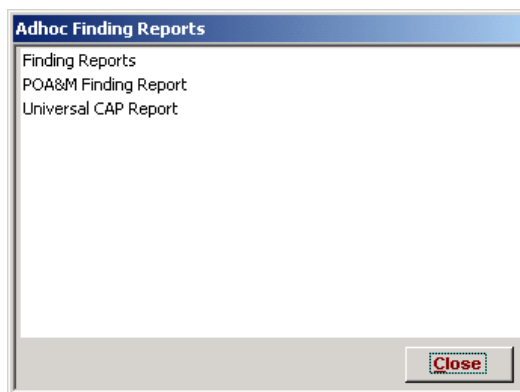
11.7.3 Adhoc (MS Access)


The Adhoc reports feature allows the user to generate a customized report that is based on user-selected filters (or parameters) and includes only user-specified information. For example, an Adhoc report can be created that includes only the Findings assigned to a specific POC(s) or Audit(s). These examples are only a small sample of how reports can be customized to meet specific needs. Although these reports include only the Findings based on user-specified filters, all of the information pertaining to each Finding is included in the report. The Findings are printed one after the other with no page breaks between each Finding.

11.7.3.1 Adhoc Reports

To generate adhoc reports, select **Adhoc (MS Access)** from the **Finding Reports** menu (Figure 11-19). This opens the following **Adhoc Finding Reports** dialog with the following Adhoc report selections.

Figure 11-22. Adhoc Finding Reports dialog



Selecting  closes the dialog and returns to **Finding Reports** menu (Figure 11-19).

11.7.3.2 Adhoc Report Selection

Refer to Figure 11-22 to select and create one of the following Finding report types:


- To generate adhoc reports that contain only selected Finding data, double-click the “Finding Report” selection.
- To generate adhoc reports that contain only selected Finding POA&M data, double-click the “POA&M Finding Report” selection.
- To generate adhoc reports that contain only selected Finding UCAP data, double-click the “Universal CAP Report” selection.

Selecting  closes the **Adhoc Finding Reports** dialog Figure 11-22 and returns to the **Finding Reports** menu (Figure 11-19).

11.7.3.3 Adhoc Report Filter Selection

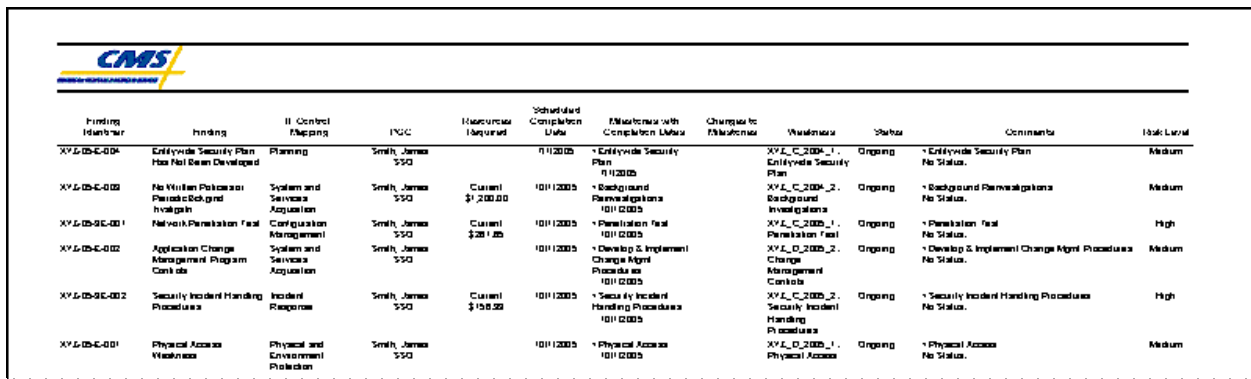
The selection of adhoc report Primary and Secondary parameters (or filters), and the resultant adhoc reports is explained in section 3.12.

11.7.4 Finding POA&M (MS Access)

Select  from the **Finding Reports** menu (Figure 11-19) to generate a report that includes all Findings contained in the database. The report includes all information included in all Findings. The Findings are printed one after the other with no page breaks between each Finding.

Once created, a report similar to the following example is available in MS Access[®] for the user to review or print. The report can only be saved if an application such as Adobe Acrobat[®] is installed on the system so the report can be “printed” to a “.pdf” file.

Figure 11-23. Example Finding POA&M report



Finding Identifier	Finding	II Control Mapping	I/C/C	Resources Required	Scheduled Completion Date	Mitigation with Completion Dates	Changes to Mitigation	Username	Status	Comments	Risk Level
XXJ-05-C-004	Enterprise Security Plan Has Not Been Developed	Planning	Smith, James SSO		11/2005	* Enterprise Security Plan 11/2005		XXJ_C_2005_1 Enterprise Security Plan	Ongoing	* Enterprise Security Plan No Status.	Medium
XXJ-05-C-002	No Written Policies/Procedures/Background	System and Services Acquisition	Smith, James SSO	Current \$1,200.00	10/1/2005	* Background Investigations 10/1/2005		XXJ_C_2005_2 Background Investigations	Ongoing	* Background Investigations No Status.	Medium
XXJ-05-C-001	Network Penetration Test	Configuration Management	Smith, James SSO	Current \$201.00	10/1/2005	* Penetration Test 10/1/2005		XXJ_C_2005_1 Penetration Test	Ongoing	* Penetration Test No Status.	High
XXJ-05-C-002	Application Change Management Program Controls	System and Services Acquisition	Smith, James SSO		10/1/2005	* Develop & Implement Change Mgmt Procedures 10/1/2005		XXJ_D_2005_2 Change Management Controls	Ongoing	* Develop & Implement Change Mgmt Procedures No Status.	Medium
XXJ-05-C-002	Security Incident Handling Procedures	Incident Response	Smith, James SSO	Current \$150.00	10/1/2005	* Security Incident Handling Procedures 10/1/2005		XXJ_C_2005_2 Security Incident Handling Procedures	Ongoing	* Security Incident Handling Procedures No Status.	High
XXJ-05-C-001	Physical Access Weakness	Physical and Environment Protection	Smith, James SSO		10/1/2005	* Physical Access 10/1/2005		XXJ_D_2005_1 Physical Access	Ongoing	* Physical Access No Status.	Medium

Since this is a MS Access[®] report, the report opens as a sub-form inside the CISS. Refer to section 3.12.1.4 for MS Access[®] report Toolbar controls. Closing the report returns to the report menu (Figure 11-19).

Select  multiple times to return to the desired menu or form.

11.7.5 Universal CAP (MS Excel)

Select **Universal CAP** from the **Finding Reports** menu (Figure 11-19) to generate a Universal Corrective Action Plan (CAP) report in MS Excel® that includes all Findings contained in the database. Since the database contains only security-related Electronic Data Processing (EDP) Findings, this report must be combined with other non-security related Findings (i.e., financial) data to create the CMS-required Universal CAP report.

Once created, a report similar to the following example is available in MS Excel® for the user to review, print, or save.

Figure 11-24. Example Universal CAP report

	A	B	C	D	E	F	G	H	I
1									
2	Contractor Name/Number:		Contractor XYZ I, 37503, 92764, 67890, 96573						
3	Date of Submission:								
4	Contact Person Name:		James Smith						
5	Contact Person Phone #:		(703)424-2424						
6	VP for Medicare Operations Name:		John Johnson						
7	VP for Medicare Operations Signature:								
8									
9	CMS Finding Number	Source of Finding	Control Objective(s) Impacted	Exception/Finding/ Material Weakness	Responsible Individual (Name, Email Address, and Phone Number)	Corrective Action Procedure(s)	Target Completion Date	Actual Completion Date	Update/Status of CAP
10	XYZ-05-9E-001	(2005) Section 912 Evaluation		Network Penetration Test	James Smith james.smith@xyz.com (703)424-2424	• Hot Site Penetration Test	10/1/2005		1. Penetration Test: Penetration Test Milestone Description: This is a generic comment or description to create test data for the CISS report and export/import functions.
11	XYZ-05-9E-002	(2005) Section 912 Evaluation		Security Incident Handling Procedures	James Smith james.smith@xyz.com (703)424-2424	• Security Incident Handling Procedures	10/1/2005		1. Security Incident Handling Procedures: Security Incident Handling Procedures Milestone Description: This is a generic comment or description to create test data for the CISS report and export/import functions.
12	XYZ-05-E-001	(2005) CFO EDP Review		Physical Access Weakness	James Smith james.smith@xyz.com (703)424-2424	• Physical Access	10/1/2005		1. Physical Access: Physical Access Milestone Description: This is a generic comment or description to create test data for the CISS report and export/import functions.

Selecting **Close** in the **Finding Reports** menu closes the menu and returns to the original starting point (i.e., CISS main menu or **Findings** form).

12.0 Submissions to CMS

The CISS replaces the CAST in its role as the automatic repository and reporting mechanism for annual Self-Assessment submissions to CMS. As with the CAST, CSR responses must be complete prior to submission. However unlike CAST, the CISS will not allow a Self-Assessment to be submitted until a validation is performed on each Self-Assessment and all noted problems are corrected.

The CISS also incorporates the POA&M submission process to CMS. The CISS replaces the former MS Excel[®] spreadsheet generation and submission process. In addition, the CISS performs validation checks of the POA&M data and formats the POA&M submissions in the CMS-prescribed format.

CMS requires that supporting documentation be included with Self-Assessment and POA&M submissions to corroborate certain non-compliant CSR responses and to corroborate closed Findings. As part of the validation process, the CISS verifies that documentation is included to support the following circumstances:

- **CSR “N/A” Status Counter to Applicability Matrix** – CMS approval documentation is required for all CSR “N/A” responses that are not corroborated by the CSR Applicability matrix. That is, the CSR should be applicable for the contract type but the Business Partner does not agree.
- **Risk-Based Decision Non-Compliant CSR** – CMS concurrence documentation and updated Risk Assessment for all non-compliant CSR responses is required where a risk-based decision was made that no Weakness/Action Plan combination is required nor desired.
- **“Closed Pending” and “Closed” Finding Status** – Appropriate documentation is required to substantiate a “Closed Pending” and “Closed” Finding status, including the letter from CMS confirming the closure status.

The CISS cannot verify the contents of the included supporting documentation nor can it verify that the correct documentation is included. It only verifies that one or more supporting documents are included with the applicable CSR or Finding if supporting documentation is required.

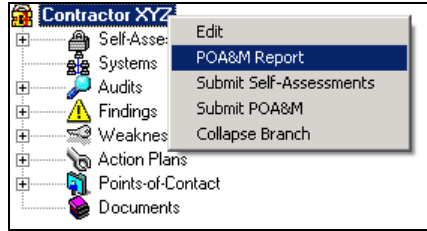
This Chapter explains the mechanics of submitting the Self-Assessment and POA&M data to CMS.

12.1 POA&M Report

The POA&M Report function creates a report representation of the POA&M data sent to CMS in the POA&M submission (refer to section 12.3). This report is *not submitted* to CMS but is provided to document the Business Partner’s POA&M submission.

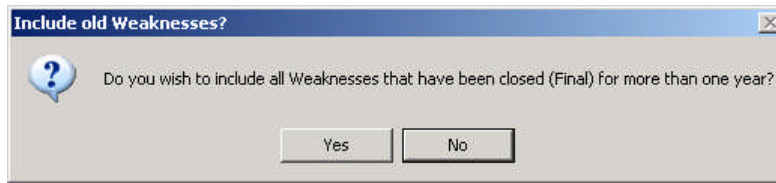
To create the POA&M Report, right-click the Contractor root node in the Treeview region and select “POA&M Report” in the following pop-up menu.

Figure 12-1. Treeview Contractor node “POA&M Report” pop-up menu



The following message displays to determine if closed Weaknesses that are over a year old should be included in the report.

Figure 12-2. Include old Weaknesses message



Selecting **No** *excludes* all closed weaknesses that are more than one year old and selecting **Yes** *includes* all closed weaknesses regardless of how long they have been closed. Once created, a report similar to the following example is available in MS Excel[®] for the user to review, print, or save.

Figure 12-3. Example POA&M Report

	A	B	C	D	E	F	G	H	I	J	K	L
	Weakness Identifier	Weakness	IT Control Mapping	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO audit or other audit review?	Status	Comments	Risk Level
1	XYZ_D_2005_1	Physical Access	Physical Security	James Smith SSO	None	10/1/2005	Physical Access - 10/1/2005		• Audit Findings: XYZ-05-E-001 • CAST Findings: 2.2,15, 2.2,18, 10,1,2	Delayed		Medium
2	XYZ_D_2005_2	Change Management Controls	Documentation	James Smith SSO	None	10/1/2005	Develop & Implement Change Mgmt Procedures - 10/1/2005		• Audit Findings: XYZ-05-E-002 • CAST Findings: 3,5,6	Delayed		Medium
3	XYZ_C_2005_1	Penetration Test	Review of Security Controls	James Smith SSO	Current \$261.65	10/1/2005	Penetration Test - 10/1/2005		• Audit Findings: XYZ-05-SE-001 • CAST Findings: 10,3,5	Delayed		High
4	XYZ_C_2005_2	Security Incident Handling Procedures	Incident Response Capability	James Smith SSO	Current \$156.93	10/1/2005	Security Incident Handling Procedures - 10/1/2005		• Audit Findings: XYZ-05-SE-002 • CAST Findings: 14,5, 16,1, 16,2, 16,3, 13,3, 10,3,6	Delayed		High
5	XYZ_C_2004_1	Entitywide Security Plan	Systems Security Plan	James Smith SSO	None	7/1/2005	Entitywide Security Plan - 7/1/2005		• Audit Findings: XYZ-05-E-004 • CAST Findings: 15,1, 13,4, 13,5, 13,3, 13,10	Delayed		Medium
6	XYZ_C_2004_2	Background Investigations	Documentation	James Smith SSO	Current \$1200.00	10/1/2005	Background Reinvestigations - 10/1/2005		• Audit Findings: XYZ-05-E-003 • CAST Findings: 1,10,5, 2,5,5	Delayed		Medium
7												

NOTE: To remove the “Page” watermark from the report, use the MS Excel[®] top menu bar to select View, then Normal.

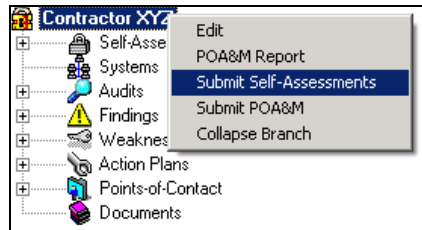
12.2 Self-Assessment Submission

The Self-Assessment Submission function prepares the Business Partner’s back-end database for submission to CMS as part of their annual certification material. (Refer to BPSSM Appendix A for guidance on submitting the CISS Self-Assessment back-end database to CMS.)

IMPORTANT: Before submitting the Self-Assessment to CMS, the SSO must ensure there is no Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the following forms/fields: Weakness “Title,” Milestone “Title,” Projected Date “Note,” and Status Update “Description” (refer to section 3.8).

To begin the Self-Assessment Submission process, right-click the Contractor root node in the Treeview region and select “Submit Self-Assessments” in the following pop-up menu.

Figure 12-4. Treeview Contractor node “Submit Self-Assessments” pop-up menu



After selecting “Submit Self-Assessments,” a notification message is briefly displayed to indicate that a backup copy of the back-end database is being made. The backup copy is created in the same directory as the existing, linked back-end database.

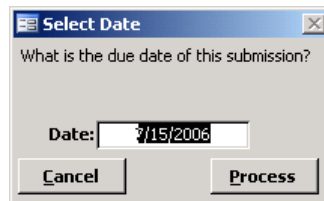
NOTE: The backup database file name consists of the original file name with “(Backup_MM-DD-YYYY hhmmss_AM or PM)” appended to the file name and a “.bak” file extension. The MM-DD-YYYY hhmmss denotes the date and time the backup was created. For example, “DEF(Backup_5-3-2006_090105).bak.”

The date and time format included in the backup file name are dependent on the time and date formats set in the MS Windows® Control Panel Regional Options.

12.2.1 Submission Date

After the back-end database has been backed up, the following **Select Date** dialog and submission confirmation dialog displays.

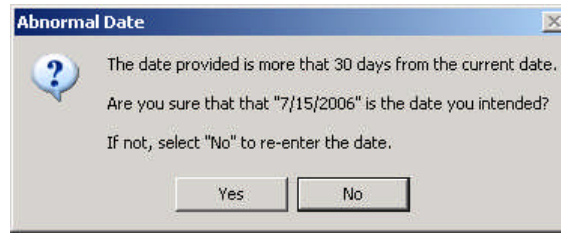
Figure 12-5. Select Date dialog and submission confirmation message



The default date can be changed by double-clicking the “Date” field to display a pop-up calendar where the date can be selected from the displayed calendar. After the date is selected, selecting **Cancel** cancels the submission process and returns to the main menu. Selecting **Process** continues the submission process.

If the submission date is more than 30 days from the current date, the following message displays to confirm that you really want to submit the Self-Assessment so far in advance of the submission date entered in the **Select Date** dialog (Figure 12-5).

Figure 12-6. Abnormal Date submission confirmation message



Selecting returns to the **Select Date** dialog (Figure 12-5) so the submission date can be changed and selecting continues the Self-Assessment validation and submission process.

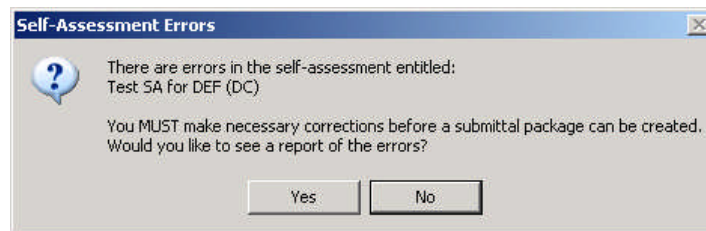
NOTE: If there are multiple Self-Assessments to be submitted, each will be processed one after the other. The submission process cannot be stopped once started; hence the **Select Date** dialog button.

12.2.2 Submission Validation

The validation process performed during the submission process is the same self-check routine that is performed using the **Self-Assessment Reports** menu (refer to section 6.11.2) except here, all Self-Assessments are checked.

If any errors are found during the validation process, the following dialog displays. This dialog identifies which Self-Assessment name has errors. A different dialog displays for each Self-Assessment where errors are found.

Figure 12-7. Self-Assessment validation error message



Selecting closes the dialog and continues the validation process for the next Self-Assessment, if any, or returns to the CISS main menu if there are no other Self-Assessments. However, Self-Assessments cannot be submitted until the necessary corrections are made. Selecting generates an error report similar to the following example in MS Word® and continues the validation process for the next Self-Assessment, if any.

Figure 12-8. Example Self-Assessment validation error report

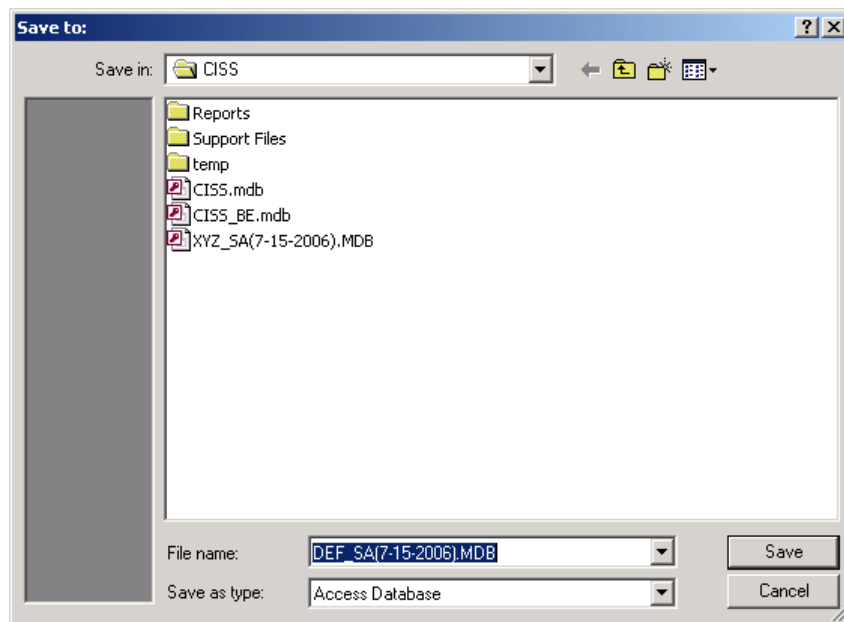
CSR	Test SA for DEF (DC) Response
1.1.1	A CMS Risk Acceptance has been selected. This response requires attached documentation of both CMS concurrence as well as an updated Risk Assessment.
1.1.3	N/A response is contrary to the CSR applicability matrix. This response requires documentation of CMS concurrence to be attached.
1.3.12	A CMS Risk Acceptance has been selected. This response requires attached documentation of both CMS concurrence as well as an updated Risk Assessment.
1.9.1	Action Plan ("Windows NT Server Configuration") needs an update to the Projected Date of Milestone ("Migration of NT Servers"). Currently it is listed as 6/30/2005 with as status of Delayed.
2.5.1	Action Plan ("Monitoring & Logging of Network Devices") needs an update to the Projected Date of Milestone ("Review Device Data for Compliance"). Currently it is listed as 3/31/2005.
	Weakness (DEF_C_2002_1) status should match the status of its Action Plan ("Monitoring & Logging of Network Devices" current status is Delayed).
2.6.1	Action Plan ("Intrusion Detection System") needs an update to the Projected Date of Milestone ("Document IDS"). Currently it is listed as 8/31/2004.
	Action Plan Intrusion Detection System does not have a current Status Update.

NOTE: If there are multiple Self-Assessments being submitted/validated, the individual error reports may not display until the validation process has completed for all Self-Assessments. Instead, each report displays as a document icon in the Windows® Taskbar (e.g., Document1 -..., Document2 -..., etc.). Each of these error reports can be selected for reviewing and printing after the validation process has completed.

12.2.3 Submission File

If no errors are found during the validation self-check process, the process continues through each Self-Assessment being submitted. When the process has completed, the following **Save to** dialog displays with the default file name and default location (i.e., CISS installation folder) for saving the Self-Assessment back-end database.

Figure 12-9. Save to dialog

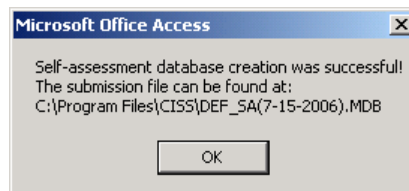


If a different location is desired, navigate to the desired folder. The file name defaults to the Business Partner’s short name abbreviation (refer to Figure 12-9) followed by “_SA” (for Self-Assessment) and the submission date selected in Figure 12-5 (e.g., DEF_SA(7-15-2006).MDB in this example). Selecting saves the Self-Assessment back-end database in the selected folder and selecting does not save the back-end database. Both selections exit the submission process and return to the main menu.

NOTE: The date format included in the file name is dependent on the date format set in the MS Windows® Control Panel Regional Options.

After the Self-Assessment submission process has successfully completed, the following dialog displays.

Figure 12-10. Self-Assessment submission success message



Selecting opens the following **Encrypt Submission File** dialog.

Figure 12-11. Encrypt Submission File dialog



Selecting closes the dialog and returns to the CISS main menu. The Self-Assessment submission can be encrypted later (if supported by the computer operating system) by selecting the button on the **Database Administration** menu (Figure 13-19). Selecting opens the **Encrypt a File** dialog (Figure 13-23) so the submission file can be encrypted (refer to section 13.2.4).

Refer to BPSSM Appendix A for guidance on submitting the CISS Self-Assessment back-end database to CMS.

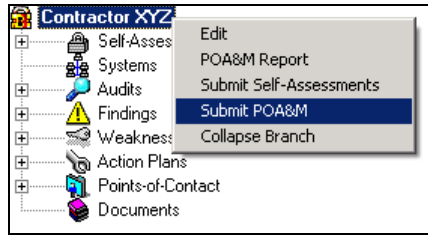
12.3 POA&M Submission

The POA&M Submission function prepares the Business Partner’s POA&M data for submission to CMS as part of their reporting requirement. (Refer to BPSSM Appendix A for guidance on submitting the POA&M data to CMS.)

IMPORTANT: Before submitting the POA&M to CMS, the SSO must ensure there is no Weakness-related contractor-, location-, or system-specific information, or other sensitive or identifying information in the following forms/fields: Weakness “Title,” Milestone “Title,” Projected Date “Note,” and Status Update “Description” (refer to section 3.8).

To begin the POA&M Submission process, right-click the Contractor root node in the Treeview region and select “Submit POA&M” in the following pop-up menu.

Figure 12-12. Treeview Contractor node “Submit POA&M” pop-up menu



After selecting “Submit POA&M,” a notification message is briefly displayed to indicate that a backup is being made. The backup database copy is created in the same directory as the existing, linked back-end database.

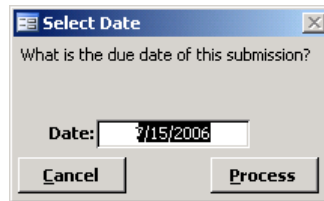
NOTE: The backup database file name consists of the original file name with “(Backup_MM-DD-YYYY hhmmss_AM or PM)” appended to the file name and a “.bak” file extension. The MM-DD-YYYY hhmmss denotes the date and time the backup was created. For example, “DEF(Backup_5-3-2006_090105).bak.”

The date and time format included in the backup file name are dependent on the time and date formats set in the MS Windows® Control Panel Regional Options.

12.3.1 Submission Date

After the back-end database has been backed up, the following **Select Date** dialog and submission confirmation dialog displays.

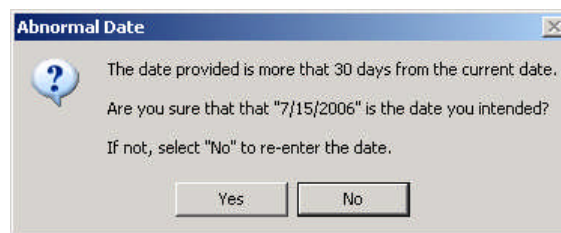
Figure 12-13. Select Date dialog and submission confirmation message



The default date can be changed by double-clicking the “Date” field to display a pop-up calendar where the date can be selected from the displayed calendar. After the date is selected, selecting **Cancel** cancels the submission process and returns to the main menu. Selecting **Process** continues the submission process.

If the submission date is more than 30 days from the current date, the following message displays to confirm that you really want to submit the POA&M so far in advance of the submission date entered in the **Select Date** dialog (Figure 12-13).

Figure 12-14. Abnormal Date submission confirmation message

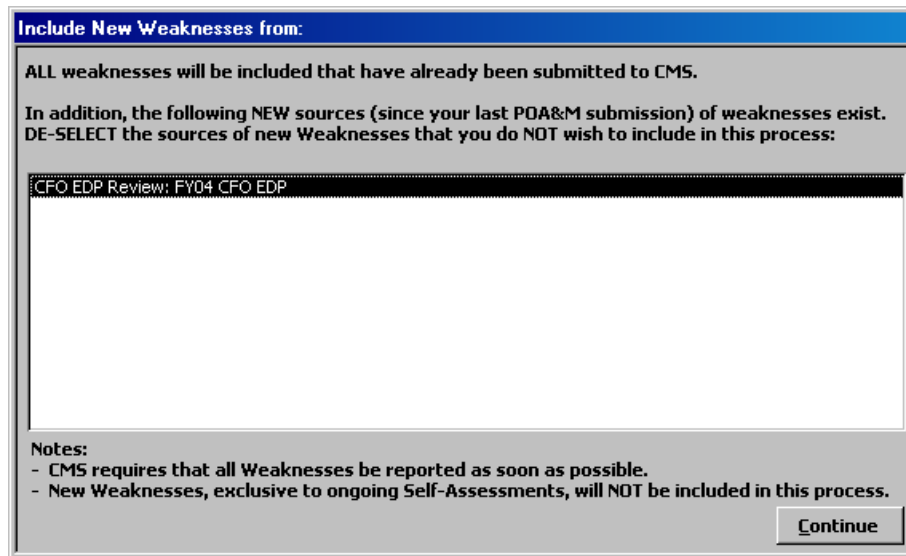


Selecting returns to the **Select Date** dialog (Figure 12-13) so the submission date can be changed and selecting continues the POA&M validation and submission process.

12.3.2 Weakness Source Selection

After selecting , the following dialog displays. All new Audit sources for Weaknesses since the last POA&M submission, if any, will be listed in the dialog window for selection or deselection. If a new Audit source is included and highlighted in the dialog window, it is selected for submission in the POA&M you are currently submitting. To exclude a new Audit source from this POA&M submission, select the source in the dialog window to deselect it (i.e., unhighlight it). Select to resume the submission process.

Figure 12-15. Include New Weaknesses form dialog

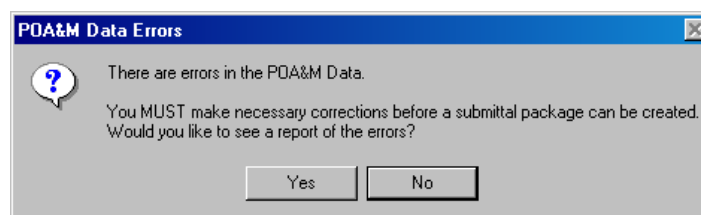


NOTE: One example for excluding an Audit source from the POA&M submission would be when the source is a draft Audit report used to populate the CISS database and the final Audit report has not been submitted/received. Also, as stated in the Figure 12-15 dialog “Notes” area, new Weaknesses resulting from an on-going Self-Assessment are not included in the POA&M submission until the Self-Assessment is submitted to CMS (refer to section 12.2).

12.3.3 Submission Validation

If any errors are found during the POA&M validation process, the following dialog displays.

Figure 12-16. POA&M validation error message



Selecting closes the dialog and ends the POA&M submission process, returning to the CISS main menu. However, the POA&M cannot be submitted until the necessary corrections are

made. Selecting generates an error report similar to the following example in MS Word® for review and printing.

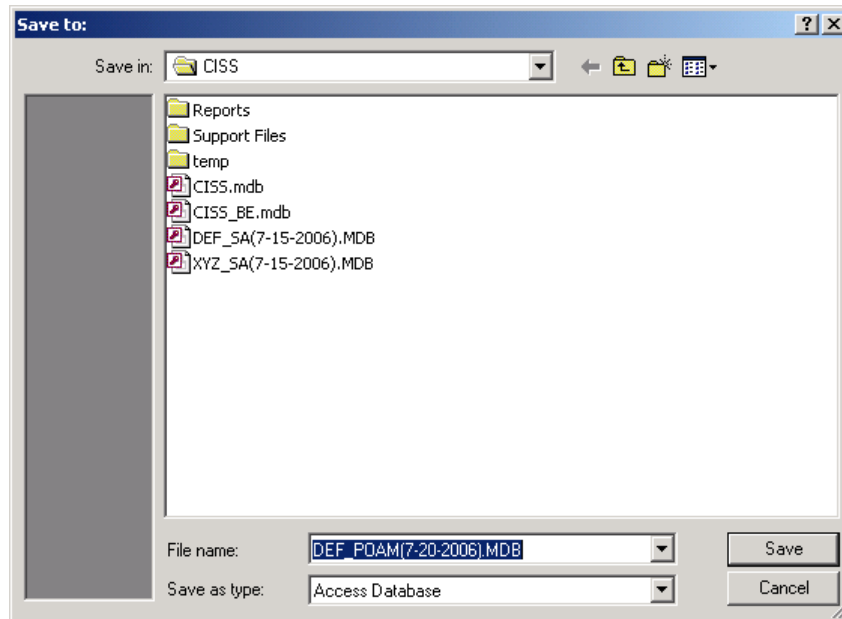
Figure 12-17. Example POA&M error report

Weakness	Error
DEF_C_2002_1	Action Plan ("Monitoring & Logging of Network Devices") needs an update to the Projected Date of Milestone ("Review Device Data for Compliance"). Currently it is listed as 3/31/2005. Weakness (DEF_C_2002_1) status should match the status of its Action Plan ("Monitoring & Logging of Network Devices" current status is Delayed).
DEF_C_2002_2	Action Plan ("Intrusion Detection System") needs an update to the Projected Date of Milestone ("Document IDS"). Currently it is listed as 8/31/2004. Action Plan Intrusion Detection System does not have a current Status Update. Weakness (DEF_C_2002_2) status should match the status of its Action Plan ("Intrusion Detection System" current status is Delayed).
DEF_C_2002_4	Action Plan ("Cisco PIX Firewall Issues") needs an update to the Projected Date of Milestone ("Map Hardening Documents to NIST"). Currently it is listed as 6/30/2005 with as status of Delayed.
DEF_C_2002_6	Action Plan ("Windows NT Server Configuration") needs an update to the Projected Date of Milestone ("Migration of NT Servers"). Currently it is listed as 6/30/2005 with as status of Delayed.

12.3.4 Submission File

If no errors are found during the validation process, the process continues through the POA&M submission process. When the process has completed, the following **Save to** dialog displays with the default file name and default location for saving the POA&M file.

Figure 12-18. POA&M Save to dialog

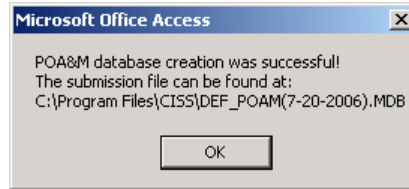


If a different location is desired, navigate to the desired folder. The file name defaults to the Business Partner’s short name abbreviation (refer to Figure 12-18) followed by “_POAM” (for POA&M) and the submission date selected in Figure 12-13 (e.g., DEF_POAM(7-20-2006).MDB in this example). Selecting saves the POA&M file in the selected folder and selecting

does not save the file. Both selections exit the submission process and return to the main menu.

After the POA&M submission process has successfully completed, the following dialog displays.

Figure 12-19. POA&M submission success message



Selecting opens the following **Encrypt Submission File** dialog.

Figure 12-20. Encrypt Submission File dialog



Selecting closes the dialog and returns to the CISS main menu. The POA&M submission can be encrypted later (if supported by the computer operating system) by selecting the button on the **Database Administration** menu (Figure 13-19). Selecting opens the **Encrypt a File** dialog (Figure 13-23) so the submission file can be encrypted (refer to section 13.2.4).

Refer to BPSSM Appendix A for guidance on submitting the POA&M data to CMS.

13.0 Database Administration

This Chapter explains the mechanics of maintaining the back-end database, maintaining supporting documents, and selecting the CISS update option.

13.1 Managing the Back-End Database

The front-end (i.e., CISS application data) and back-end (i.e., Business Partner data) database files must be linked to function properly. These links must be established the first time the CISS application is run, and whenever the back-end file name or location is changed, or a new back-end database is created. Select one of the following appropriate methods to establish a connection to the back-end database.

13.1.1 Back-end Database Connection Error

If the database links are not established (such as when running the CISS application for the first time, when there is no existing back-end database, or when an existing back-end database is relocated or renamed), the following **Connection Error** message dialog displays over the CISS “WARNING” statement dialog.

Figure 13-1. Connection Error warning message



Select to close the **Connection Error** message and display the **Connect to Back-end Database** dialog (Figure 13-2).

NOTE: All existing CISS database links remain resident within the front-end database (or CISS application). They are *not* resident in the back-end database. This means that if a network version of the back-end database is renamed or relocated, all workstation CISS applications must be individually re-linked to the correct back-end database.

Proceed to the section 13.1.3.

13.1.2 Changing the Back-end Database

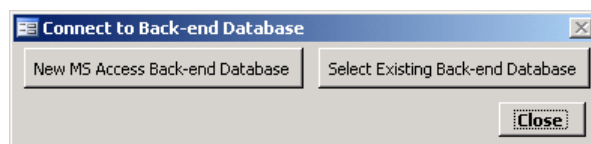
To change an existing, linked back-end database to a different back-end database, open the CISS (if not already open) and select the button from the Application Control region of the main menu (Figure 3-4) to display the **Connect to Back-end Database** dialog (Figure 13-2).

Proceed to the next section, 13.1.3.

13.1.3 Connecting to the Back-end Database

The following **Connect to Back-end Database** dialog allows the user to create a new back-end database or connect to an existing back-end database.

Figure 13-2. Connect to Back-end Database dialog



If the CISS is already linked to a back-end database, selecting **Close** returns to the main menu (Figure 3-3) without making any changes. Otherwise, selecting **Close** displays the following two message dialogs.

Figure 13-3. Back-end connection problem dialog

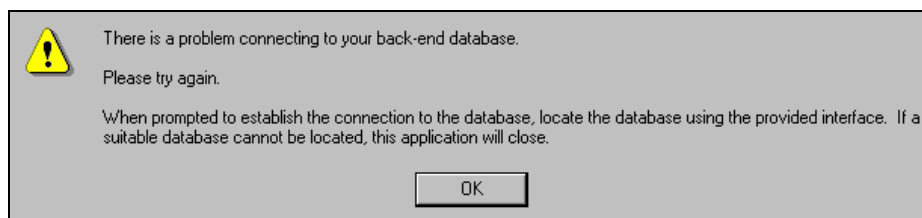
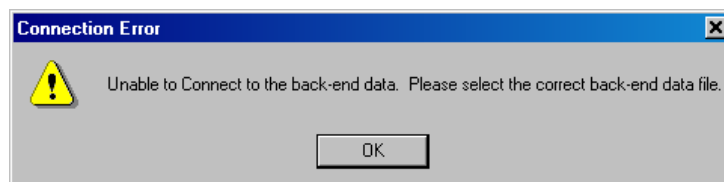


Figure 13-4. Connection Error warning message

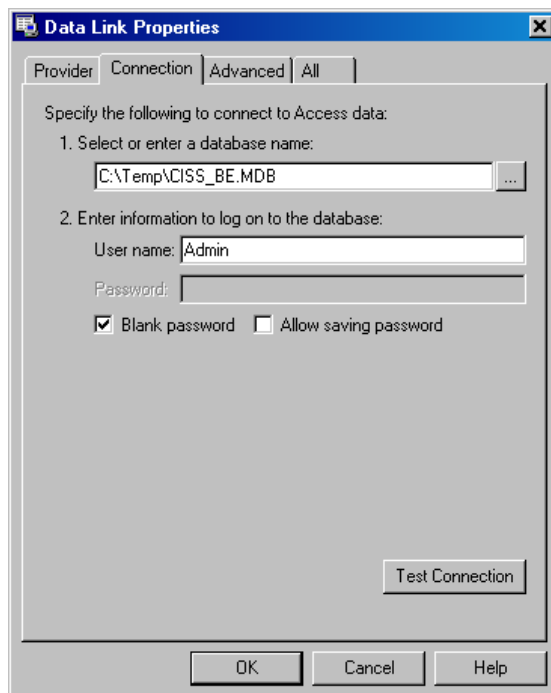


Selecting **OK** in each of the two message dialogs returns to the **Connect to Back-end Database** dialog (Figure 13-2). Selecting **Close** in the **Connect to Back-end Database** dialog closes the application. The CISS cannot run until it is connected/linked to an existing or new back-end database.

13.1.3.1 Selecting an Existing Back-end Database

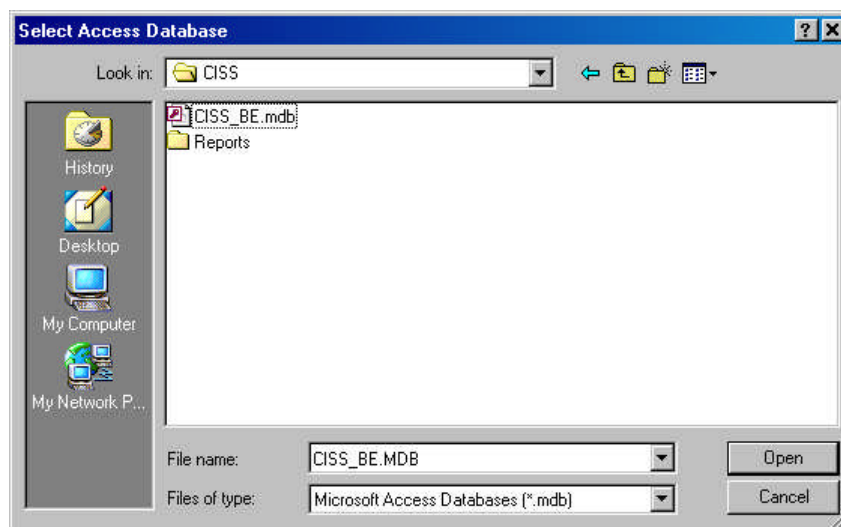
To connect to an existing back-end database, select **Select Existing Back-end Database** in the **Connect to Back-end Database** dialog (Figure 13-2) to open the following initial **Data Link Properties** at the **Connection** tab. The steps following the figure explain how to select an existing back-end database.

Figure 13-5. First Data Link Properties dialog



- a. Selecting **Cancel** exits the CISS if a valid database link does not already exist, or closes the dialog and returns to the CISS main menu (Figure 3-3) without making any database link changes if a valid link already exists. Selecting **...** at the end of the “Select or enter a database name” field opens the following **Select Access Database** dialog.

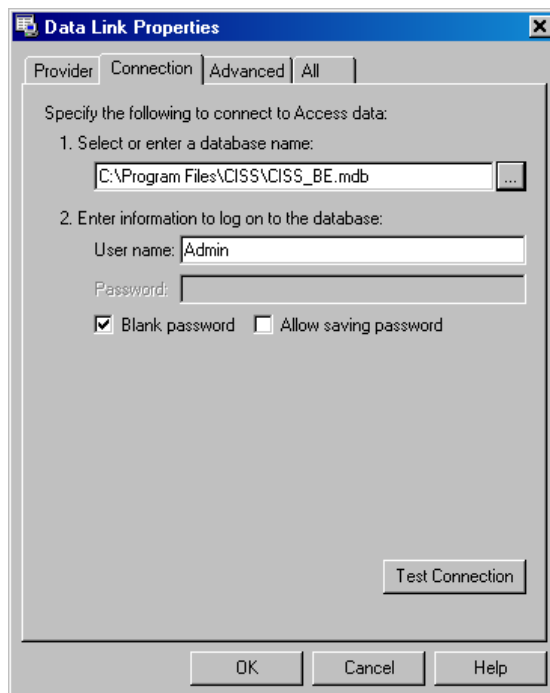
Figure 13-6. Select Access Database dialog



- b. Selecting **Cancel** returns to the **Data Link Properties** at the **Connection** tab (Figure 13-5). Otherwise, locate and select the desired back-end database and select **Open**.

After a back-end database file is selected, the CISS establishes all the necessary table links and opens the following **Data Link Properties** dialog. The selected back-end database file name along with its folder location path are displayed in the “Select or enter a database name” field on the **Connection** tab.

Figure 13-7. Second Data Link Properties dialog

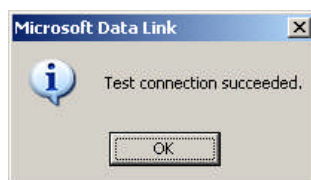


NOTE: For the current CISS release, the “User name” field in the *Data Link Properties* dialog (Figure 13-7) should be left as “Admin” and the password selection as “Blank password.” If this log-on capability changes in a future release, the User Guide will be updated accordingly.

- c. Selecting exits the CISS if a valid database link does not already exist, or closes the dialog and returns to the CISS main menu (Figure 3-3) without making any database link changes if a valid link already exists. Selecting closes the *Data Link Properties* dialog.

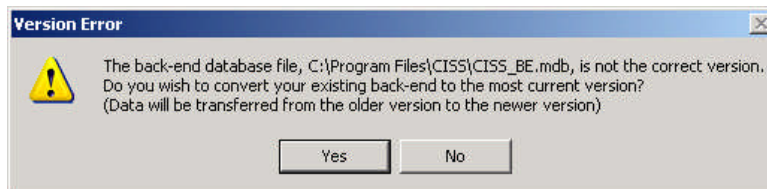
If is selected, the following success message that results is only an indication that the back-end is a MS Access® database and a connection can be established. It does not evaluate the database contents or format (that occurs in the next step).

Figure 13-8. Testing the back-end file connection



- d. The CISS then evaluates the back-end database structure to determine whether it is in the proper format. If an update to the back-end database is required (e.g., selecting a back-end that predates the current CISS release), a **Version Error** message similar to the following displays.

Figure 13-9. Back-end database Version Error message dialog



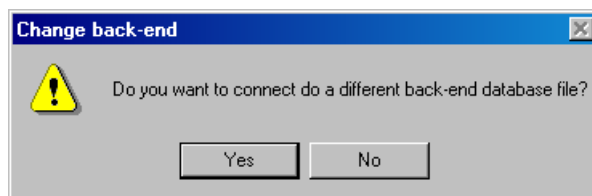
- e. Selecting updates the back-end database structure as necessary. While the back-end database is being updated, an **Updating backend database** dialog displays, after which time the CISS returns to the main menu.

NOTE: Before the back-end database is updated, the CISS saves a backup copy of the original database in its current location. The backup database file name consists of the original file name with “(MM-DD-YYYY hhmm)” appended to the file name and a “.bak” file extension. The MM-DD-YYYY hhmm denotes the date and time the backup was created. For example, “Contractor XYZ(01-11-2005 0835).bak.”

The date and time format included in the backup file name are dependent on the time and date formats set in the MS Windows® Control Panel Regional Options.

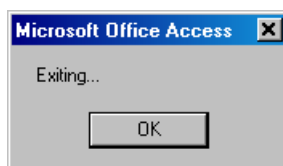
- f. Selecting displays the following message.

Figure 13-10. Change back-end message



- g. Selecting opens the **Data Link Properties** at the **Connection** tab (Figure 13-5). Return to step a. above to select a different back-end database file. Selecting displays the following message.

Figure 13-11. Exiting message

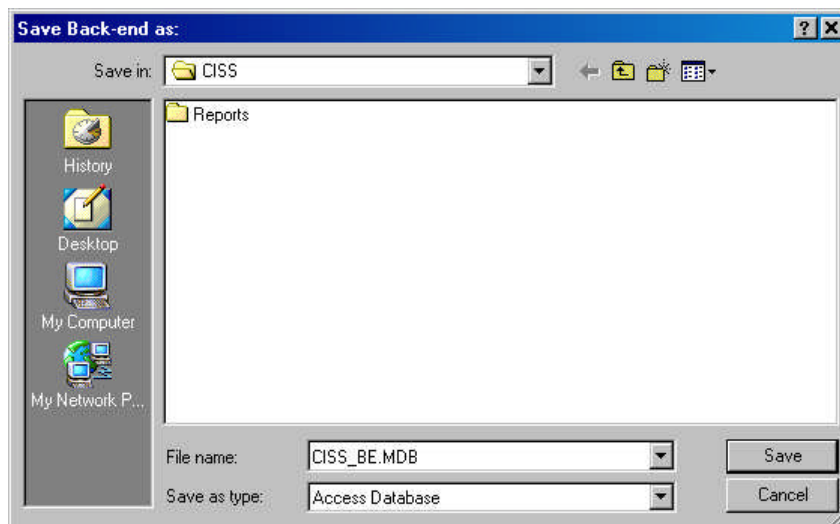


- h. Selecting exits the CISS. The CISS will not run until the selected back-end database file is updated.

13.1.3.2 Creating a New Back-end Database

To create a new back-end database, select in the **Connect to Back-end Database** dialog (Figure 13-2) to open the following **Save Back-end as** dialog. The steps following the figure explain how to create a new back-end database.

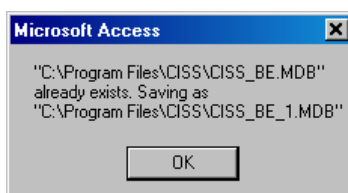
Figure 13-12. Default Save Back-end as dialog



- a. Selecting exits the CISS if a valid database link does not already exist, or closes the dialog and returns to the CISS main menu (Figure 3-3) without making any database selection changes if a valid link already exists.
- b. The **Save Back-end as** dialog displays the default file name and location for the new database. If a different file name or location is desired, change the file name and navigate to the desired folder. When finished, select to create the new back-end database.

If the default or specified file name already exists in the same folder, a message similar to the following displays.

Figure 13-13. Pre-existing file name message dialog



Selecting adds a one-up number (i.e., “_1”) to the new file name so the original file is not overwritten.

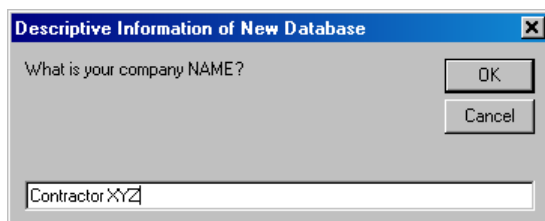
- c. Before the new back-end database can be created, the CISS requires additional user input to configure the back-end database. Proceed to the next section, 13.1.3.3, to complete the new back-end database configuration and creation.

13.1.3.3 Completing the New Back-end Database Setup

After creating a new back-end database, the CISS requires unique Business Partner descriptive information to configure the back-end database. The following steps explain how to complete the back-end configuration process:

- a. At the following company name **Descriptive Information of New Database** dialog, input the company name (e.g., Contractor XYZ) and select to continue. The name entered here is used throughout the CISS as the primary Business Partner identifier. However, this name can be changed later (refer to section 2.4.1).

Figure 13-14. Company name Descriptive Information of New Database dialog



- b. Selecting with a blank input field or selecting displays the following dialog because the back-end database cannot be created without this company name information. Both selections return to the above **Descriptive Information of New Database** dialog.

Figure 13-15. Company name Required Information dialog

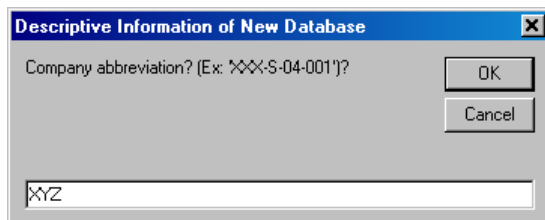


Selecting returns to the company name **Descriptive Information of New Database** dialog (Figure 13-14).

- c. At the following company abbreviation **Descriptive Information of New Database** dialog, input the CMS-approved company abbreviation (e.g., XYZ) and select to continue. The abbreviation entered here is used throughout the CISS to identify Business Partner audit Findings and Weaknesses. However, this abbreviation can be changed later (refer to section 2.4.1).

NOTE: The company abbreviation is the three- or four-letter Business Partner identifier listed in the *Medicare Financial Manual* (CMS Pub 100-6) under “Contractor Abbreviations” in Chapter 7 - *Internal Control Requirements*, Section 40.3, *CMS Finding Numbers*.


Figure 13-16. Company abbreviation Descriptive Information of New Database dialog



- d. Selecting with a blank input field or selecting displays the following dialog because the back-end database cannot be created without this company abbreviation information. Both selections return to the above **Descriptive Information of New Database** dialog.

Figure 13-17. Company name Required Information dialog



- e. Selecting  returns to the company abbreviation **Descriptive Information of New Database** dialog (Figure 13-16).


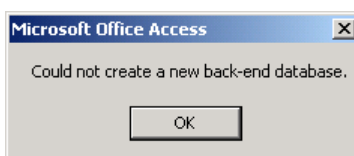
NOTE: If multiple blank company name or abbreviation inputs, or multiple cancellations are selected, the following dialog displays. Selecting  returns to the **Connect to Back-end Database** dialog (Figure 13-2) without creating a new back-end database.

Figure 13-18. Cannot create back-end database dialog



If the CISS was already linked to an existing back-end database prior to successfully completing both **Descriptive Information of New Database** dialogs, the CISS returns to the main menu (Figure 3-3) and displays the new back-end database at the main menu.

If no back-end database existed prior to successfully completing both **Descriptive Information of New Database** dialogs (i.e., new installation), the CISS redisplay the logon “WARNING” message without the connection error warning message (Figure 3-2). The “WARNING” message is the entry point to the CISS application (proceed to Chapter 3.0).

13.2 Database Administration Menu

The CISS includes a Database Administration menu that provides easy access to database administrative functions. To access this menu, select the Application Control region

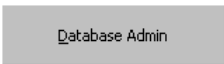
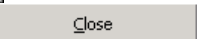
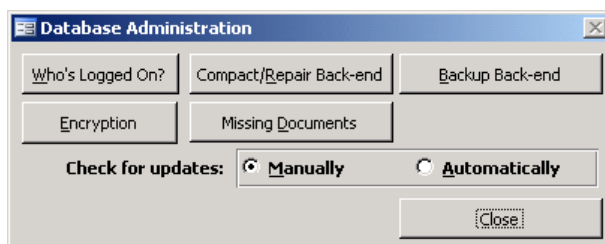
 button (refer to section 3.1.4) to open the following **Database Administration** menu. Selecting  returns to the CISS main menu.

Figure 13-19. Database Administration menu

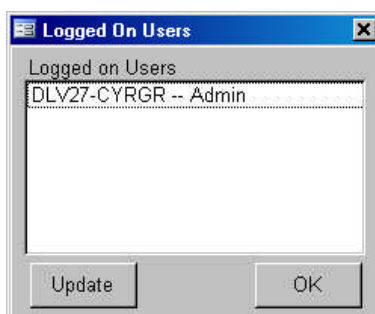


NOTE: The button is active only if a FIPS-compliant Triple Data Encryption Algorithm (TDEA) cryptography support file is available (refer to section 13.2.4 for additional information). The button is active only when supporting documentation is missing (refer to Chapter 4.0 for an explanation of CISS supporting documentation and section 4.7.1 for instructions on using this button).

13.2.1 Who's Logged On?

Selecting the button (Figure 13-19) opens the following **Logged On Users** dialog. This dialog displays which users are currently using the back-end database. Selecting closes this dialog and returns to the **Database Administrative** menu. Selecting refreshes the dialog to display any users who may have logged on since the dialog was opened.

Figure 13-20. Logged On Users dialog

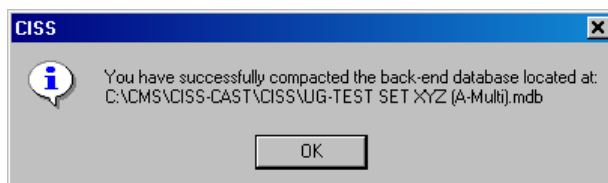


13.2.2 Compact/Repair Back-end

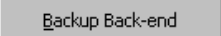
MS Access® includes an automatic function that compacts and repairs the back-end database. This automatic capability removes temporary information from the database file (reducing the overall file size) as well as performs minor corrections to a slightly corrupted database. This process is initiated automatically, as necessary, by the CISS each time the user exits the application.

In addition, the CISS includes this on-demand capability to compact and repair the back-end database. To perform these functions, select the button (Figure 13-19). Selecting it displays a message that the database is being compacted, followed by a message dialog similar to the following to indicate its successful completion. Selecting closes the message dialog and returns to the **Database Administrative** menu.

Figure 13-21. Successful compaction message



13.2.3 Backup Back-end

The CISS automatically creates backups of the back-end database before certain critical functions are performed (i.e., before submissions to CMS, back-end release updates). In addition, the CISS includes an on-demand capability to backup the back-end database. To perform a backup, select the  button (Figure 13-19).


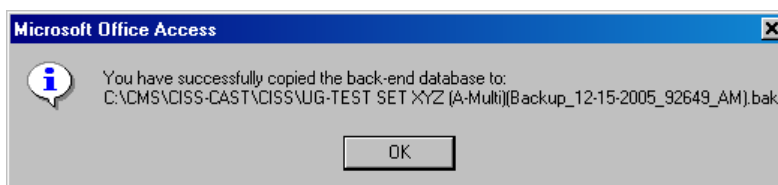
A notification message is briefly displayed to indicate that a backup is being made, followed by a message dialog similar to the following to indicate its successful completion. Selecting  closes the message dialog and returns to the *Database Administrative* menu.

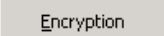
Figure 13-22. Successful backup message



The backup database copy is created in the same directory as the existing, linked back-end database. The backup database file name consists of the original file name with “(Backup_*MM-DD-YYYY_hhmmss_AM* or *PM*)” appended to the file name and a “.bak” file extension. The *MM-DD-YYYY hhmmss* denotes the date and time the backup was created. For example, “ABC(Backup_12-14-2005_12655_PM).bak.”

NOTE: The date and time format included in the backup file name are dependent on the time and date formats set in the Windows Control Panel Regional Options.

13.2.4 Encryption

Before the CISS uses encryption on a workstation, it first verifies that a FIPS-compliant TDEA (a.k.a, Triple Data Encryption Standard [Triple DES or 3DES]) operating system Dynamic Link Library (dll) cryptography file is installed and enabled on the workstation. If a FIPS-compliant TDEA algorithm is NOT found or NOT installed on a workstation, the  button will NOT be active; thus, encryption will NOT be available.

FIPS-compliant TDEA algorithms are distributed and available with MS Windows XP or later operating system versions (i.e., MS Windows 2003) (refer to the following article for additional information: <http://support.microsoft.com/kb/811833/en-us>). It is up to the Business Partner to upgrade to an operating system that includes a FIPS-compliant TDEA algorithm in order to use encryption. It is not a function of the CISS or CMS to provide such an algorithm.

13.2.4.1 Encrypt Files

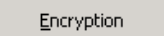

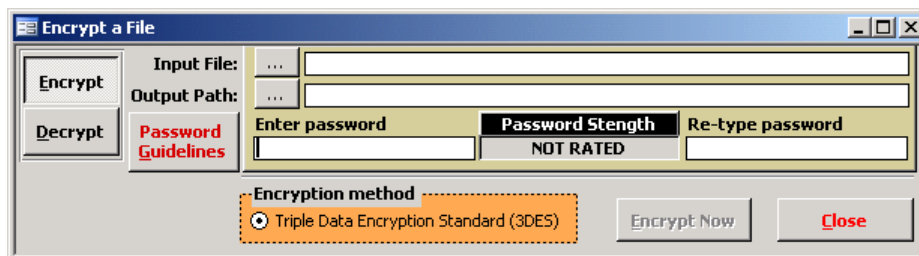
Selecting the  button (Figure 13-19) opens the following *Encrypt a File* dialog with the  button activated.

Figure 13-23. Encrypt a File dialog

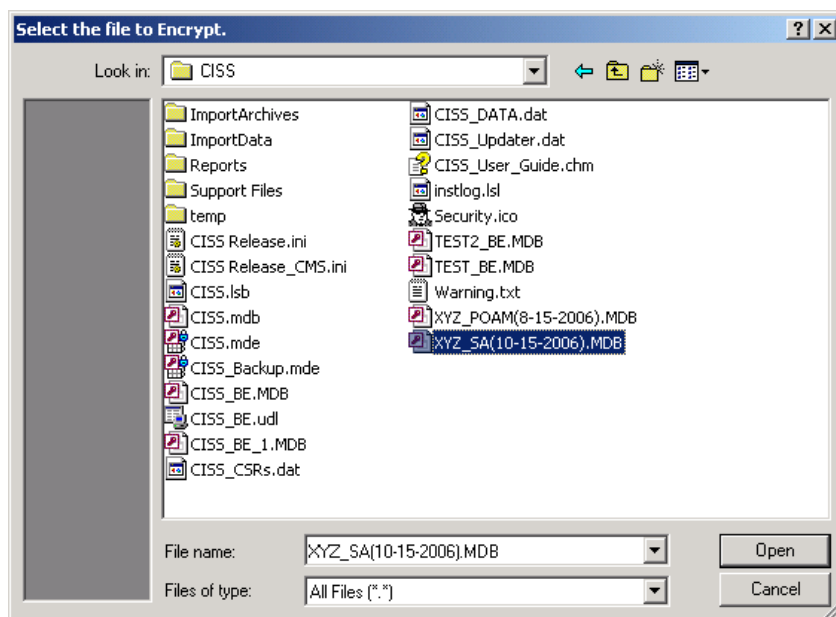


Selecting **Close** closes the dialog and returns to the **Database Administrative** menu.

13.2.4.2 File Encryption Selection

Selecting the **...** button to the right of the “Input File” field name opens the following **Select the file to Encrypt** dialog.

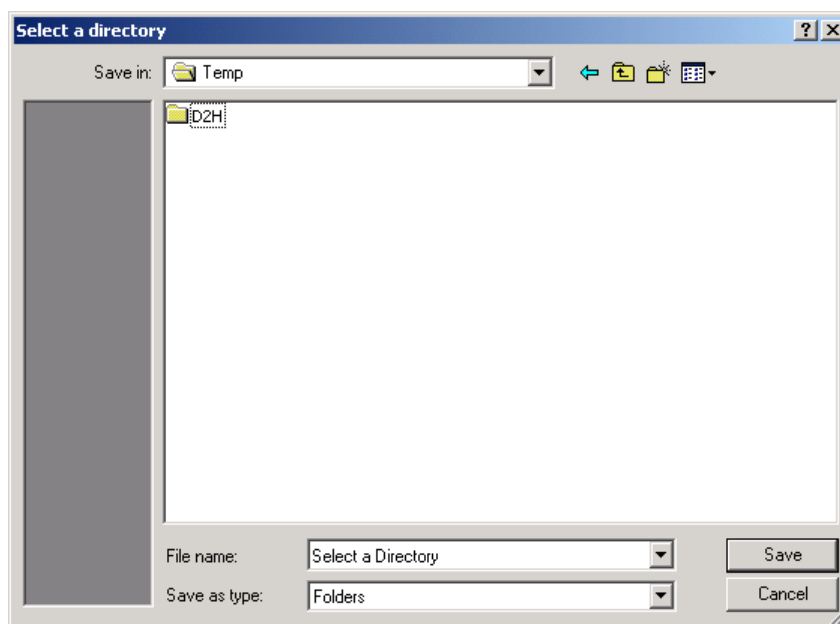
Figure 13-24. Select the file to Encrypt dialog



Selecting **Cancel** closes the dialog and returns to the **Encrypt a File** dialog. Otherwise, locate and select the file to encrypt, and select **Open** to input the selected path/file into the “Input File” field.

The encrypted file output path defaults to the same path as the selected input file. If a different path is desired, selecting the **...** button to the right of the “Output Path” opens the following **Select a directory** dialog.

Figure 13-25. Select a directory dialog

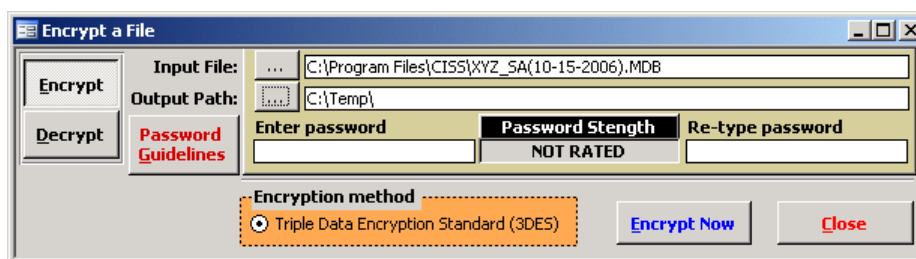


Selecting closes the dialog and returns to the **Encrypt a File** dialog.

After navigating to the desired output file directory, selecting pastes the selected directory/folder into the “Output Path” field in the **Encrypt a File** dialog (Figure 13-26). The encrypted output file name is not included in the “Output Path” field. The output file name consists of the original file name with the file extension “.enc” (i.e., encrypted) instead of the original input file extension (e.g., “XYZ_SA(10-15-2006).enc” in this example).

NOTE: If another encrypted file with the same file name already exists in the output path folder, the original file is *overwritten* with the new one.

Figure 13-26. Encryption Input File/Output Path selections

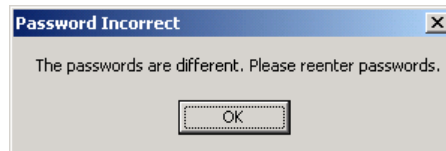


NOTE: The “Password Strength” dialog (i.e.,) evaluates the strength of the password as it is being entered into the “Enter password” field. Passwords are rated in order of strength as: “Weak,” “Medium,” “Strong,” and “Very Strong” based on the length and strength of the password. A password must consist of at least 8 characters before it is evaluated because that is the minimum length allowed. Before a file can be encrypted, the password must be evaluated and rated as *at least* “**Strong**.” To review the CMS password requirements, select the button.

Enter a password into the “Enter password” field, and re-enter the same password into the “Re-type password” field to confirm the password. Use the **Tab** or **Enter** keys to exit the “Re-type password” field. If the two passwords match *and* the password strength is evaluated as at least “Strong,” the **Encrypt Now** button in the **Encrypt a File** dialog is activated (Figure 13-29).

- a. If the two passwords do *not* match, the following dialog is displayed and both password fields are cleared when **OK** is selected. Re-enter matching “Strong” or “Very Strong” passwords to continue.

Figure 13-27. Password Incorrect message



- b. If the two passwords match but are *not* rated as at least “Strong” or “Very Strong,” the following dialog is displayed and both password fields are cleared when **OK** is selected. Re-enter matching “Strong” or “Very Strong” passwords to continue.

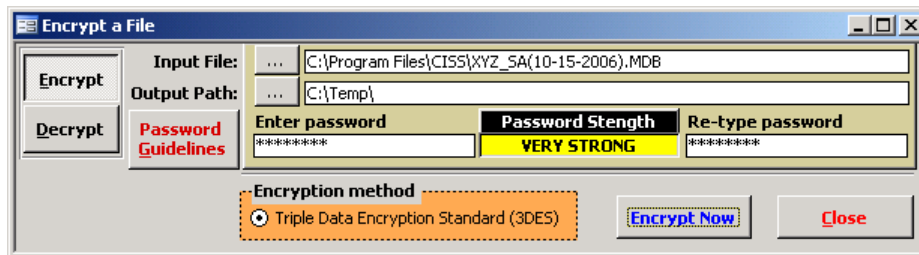
Figure 13-28. Password Strength Error message



IMPORTANT: Since the same password is required to decrypt an encrypted file, record and store all encryption passwords in a secure location (e.g., in an envelope in a locked cabinet). Neither CMS nor the CMS Help Desk can assist in recovering encrypted files if the correct password is not known.

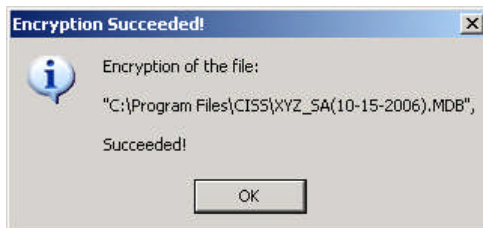
Select the **Encrypt Now** button in the **Encrypt a File** dialog to begin the 3DES encryption process.

Figure 13-29. Encrypt Now button



After the file is encrypted, the following encryption success message displays.

Figure 13-30. Encryption Succeeded message



Selecting opens the **Compress Encrypted File** dialog (Figure 13-31).

13.2.4.2.1 File Compression

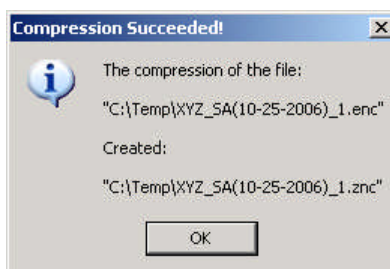
The following **Compress Encrypted File** dialog provides an opportunity to compress the submission file with industry standard compression; thereby, reducing the submission file size substantially.

Figure 13-31. Compress Encrypted File dialog



Selecting returns to the **Encrypt a File** dialog without compressing the submission file. Selecting compresses the submission file and displays the following **Compression Succeeded** message after the file has been compressed.

Figure 13-32. Compression Succeeded message



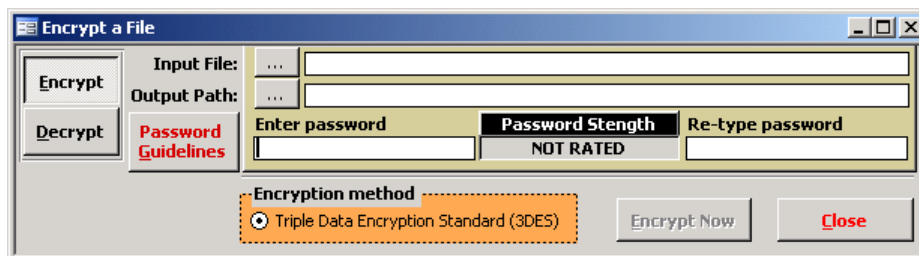
Selecting closes the message dialog and returns to the **Encrypt a File** dialog.

NOTE: Only the contents of the compressed file are encrypted—not the compressed file itself. The compressed file can be renamed with a “.zip” extension and uncompressed with any compatible uncompressing utility. However, the resultant uncompressed file remains encrypted with 3DES cryptography and requires the applicable password to decrypt it.

13.2.4.3 Decrypt Files

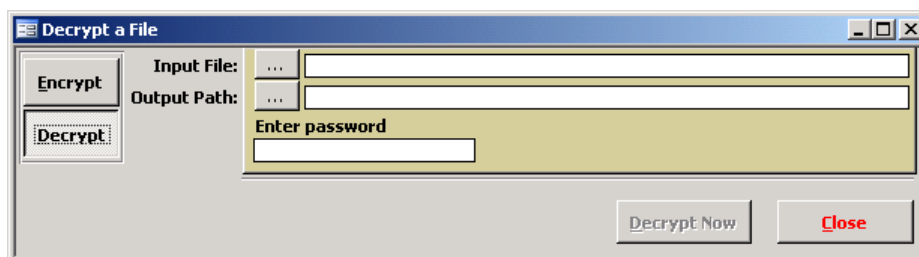
Selecting the button (Figure 13-19) opens the following **Encrypt a File** dialog.

Figure 13-33. Encrypt a File dialog



Selecting **Close** closes the dialog and returns to the **Database Administrative** menu. Selecting the **Decrypt** button opens the following **Decrypt a File** dialog.

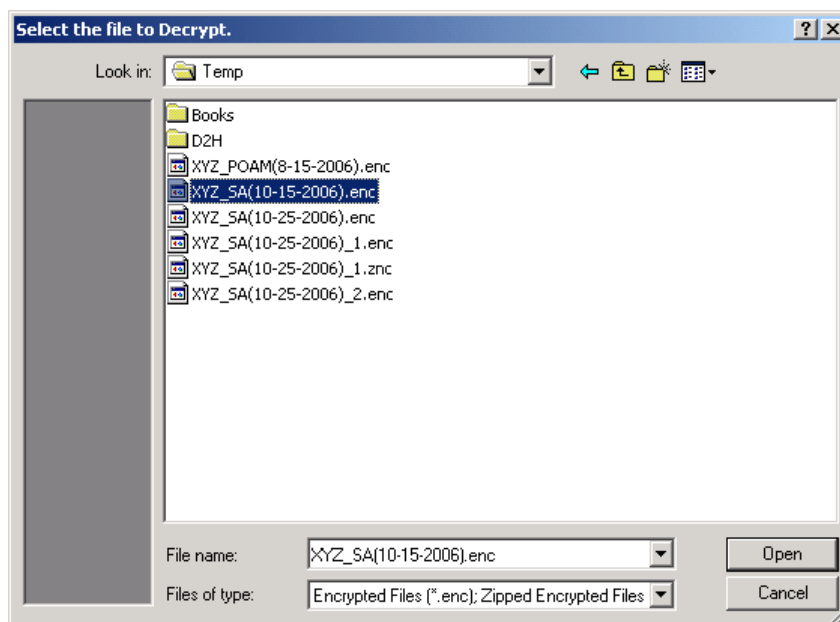
Figure 13-34. Decrypt a File dialog



13.2.4.4 File Decryption Selection

Selecting the **...** button to the right of the “Input File” field name opens the following **Select the file to Decrypt** dialog. Note that this dialog displays only encrypted (“**.enc**”) and compressed, encrypted (“**.znc**”) files for selection.

Figure 13-35. Select the file to Decrypt dialog



Selecting **Cancel** closes the dialog and returns to the **Decrypt a File** dialog. Otherwise, locate and select the file to decrypt, and select **Open** to input the selected path/file into the “Input File” field.

NOTE: If a compressed, encrypted file (“.znc”) is selected for decryption, the decompression process is transparent to the user. The CISS temporarily decompresses the file so it can verify the decryption password before the file can be decrypted.


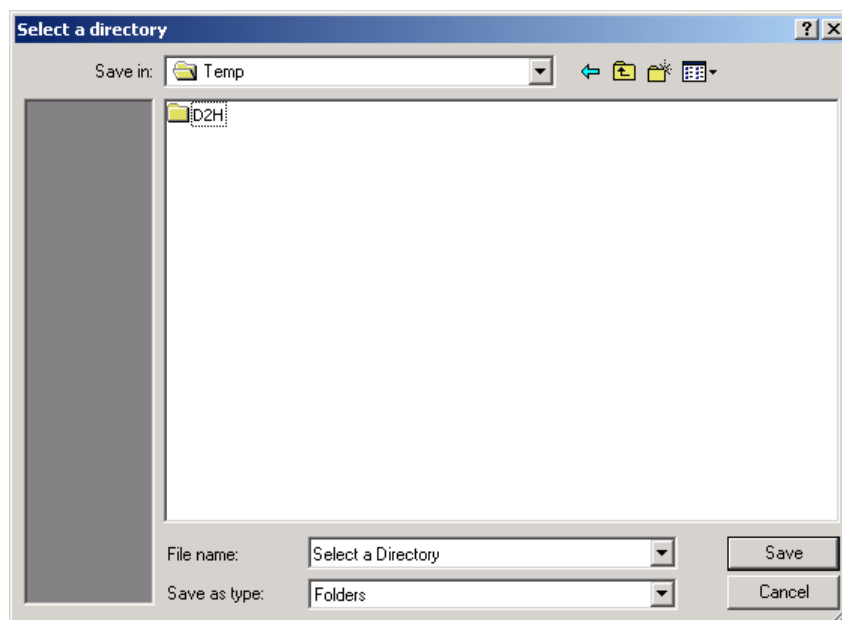


The decrypted file output path defaults to the same path as the selected input file. If a different path is desired, selecting the  button to the right of the “Output Path” opens the following **Select a directory** dialog.

Figure 13-36. Select a directory dialog

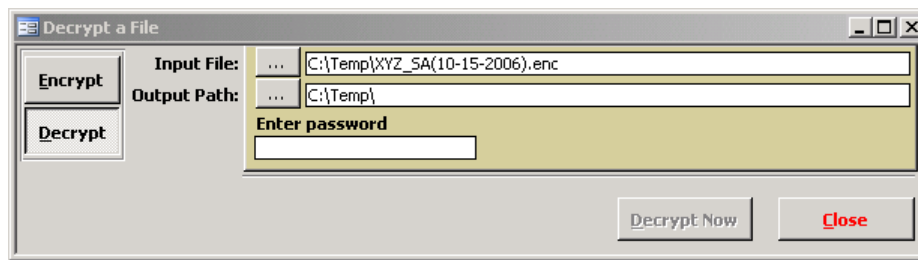


Selecting  closes the dialog and returns to the **Decrypt a File** dialog.

After navigating to the desired output file directory, selecting  pastes the selected directory/folder into the “Output Path” field in the **Decrypt a File** dialog (Figure 13-34). The decrypted output file name is not included in the “Output Path” field. The output file name consists of the selected file name with the file extension returned to its original unencrypted file extension (e.g., “XYZ_SA(10-15-2006).MDB” in this example).

NOTE: If another file with the same file name already exists in the output path folder, the CISS appends a 1-up number to the end of the file name (e.g., “XYZ_SA(10-15-2006)1.MDB” in this example) so the original file is *not* overwritten.

Figure 13-37. Decrypt Input File/Output Path selections



Enter the password used to encrypt the file into the “Enter password” field. As soon as the first password character is entered into the field, the **Decrypt Now** button is activated. After entering the complete password, select **Decrypt Now** to validate the password and decrypt the file.

If the password entered does *not* match the encryption password, the following message is displayed and the file is *not* decrypted. Select **OK** to clear the “Enter password” field and re-enter the correct password.

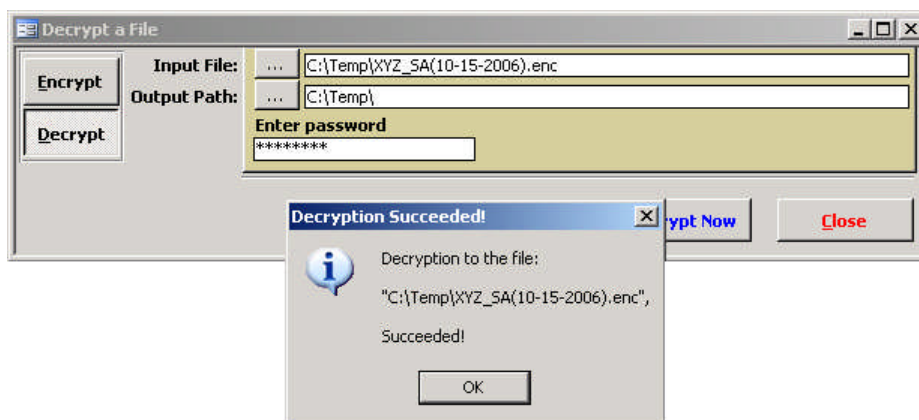
Figure 13-38. Password Incorrect message



NOTE: Neither CMS nor the CMS Help Desk can assist in recovering encrypted files if the correct password is not known.

After the password entered is validated by comparing it to the encrypted, imbedded password included in the input file, the file is decrypted and the following decryption success message displays.

Figure 13-39. Decryption Succeeded message



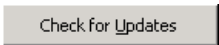
Selecting **OK** closes the message dialog and returns to the **Decrypt a File** dialog.

13.2.5 Missing Documents

The **Missing Documents** button (Figure 13-19) is only active when supporting documentation previous inserted into the CISS is missing. Refer to Chapter 4.0 for an explanation of CISS supporting documentation and section 4.7.1 for instructions on using this button.

13.2.6 Check for Updates

The following CISS update configuration settings require that the computer with the CISS application have access to the Internet. If the computer does not have Internet access, refer to section 3.1.2 for the procedure on checking for updates using a different computer, one that is connected to the Internet.

The “Check for updates” selection options (Figure 13-19) configure the CISS to either check for updated releases of the CISS each time it is opened (i.e., “Automatically”) or to only check for updated releases when the  button on the main menu (Figure 3-3) is selected (i.e., “Manually”).

13.2.6.1 Manually

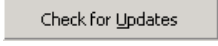
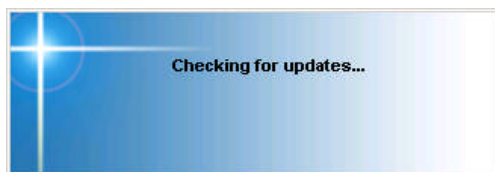
When the “Check for updates” option is set to “Manually” (Figure 13-19), the user must select the  button on the CISS main menu (Figure 3-3) to check for updates. This briefly displays the following message box while the CISS checks for the latest release.

Figure 13-40. Checking for updates message



13.2.6.2 Automatically

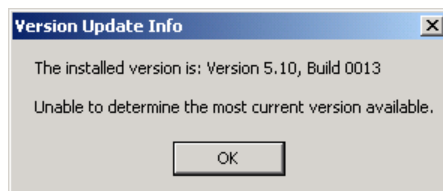
When the “Check for updates” option is set to “Automatically” (Figure 13-19), each time the CISS application is run it checks for updates after the user selects “Accept” in the opening screen WARNING statement (Figure 3-2). This briefly displays the above message box (Figure 13-40) while the CISS checks for the latest release.

13.2.6.3 Manual and Automatic Updates

Both manual and automatic updates perform the following same functions:

- a. If the latest release is currently installed, the CISS returns to the main menu without displaying any other dialog. If the CISS cannot determine the most current release (e.g., the update web site is down), it displays the following *Version Update Info* dialog.

Figure 13-41. Version Update Info dialog message




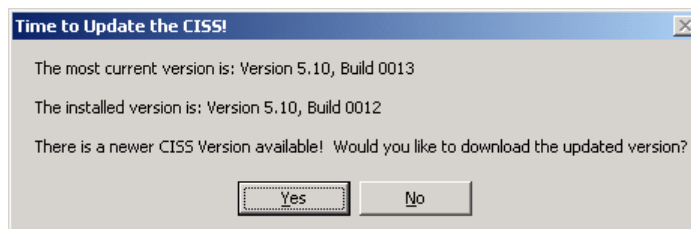
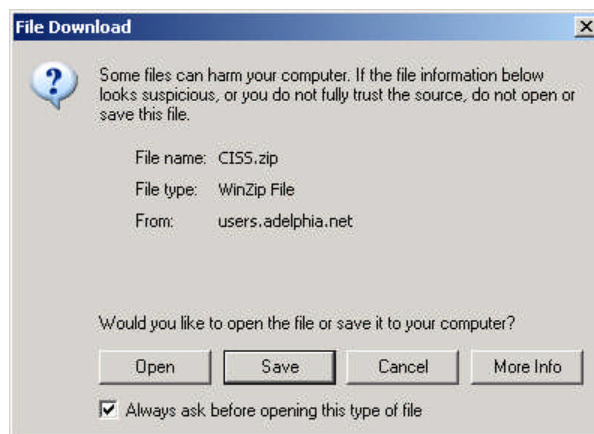
- b. Selecting  returns to the CISS main menu. If the CISS determines there is a more current release available, it displays the following dialog.

Figure 13-42. Time to Update the CISS! dialog



- c. Selecting returns to the main menu without downloading the updated CISS version. Selecting closes the CISS application, opens the default web browser, and displays a dialog similar to the following.

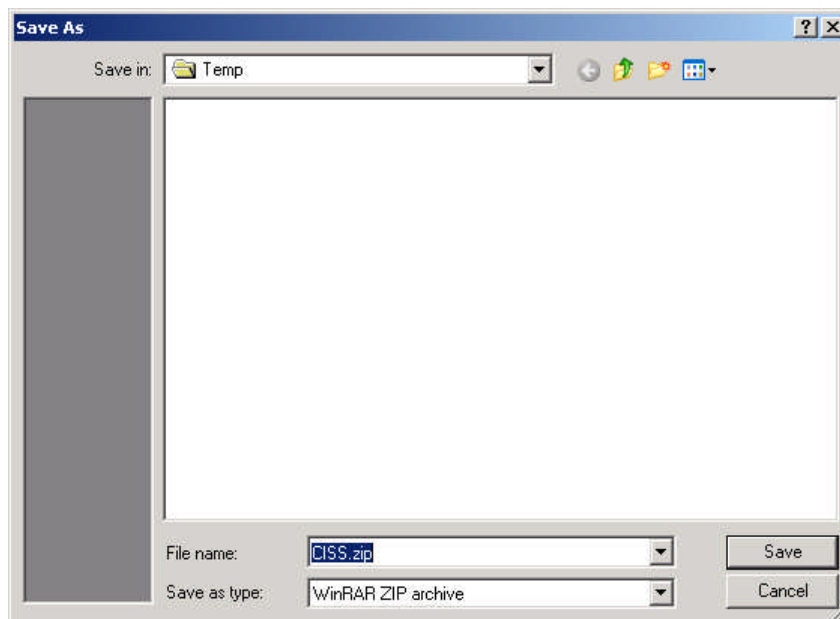
Figure 13-43. File Download dialog



NOTE: The CMS CISS version displays a different file name and “From” location than the contractor version but all other dialog functions are the same as shown in these steps.

- d. Selecting ends the update download process and return to the Windows® desktop. Selecting opens the following **Save As** dialog with the default file name and folder location displayed.

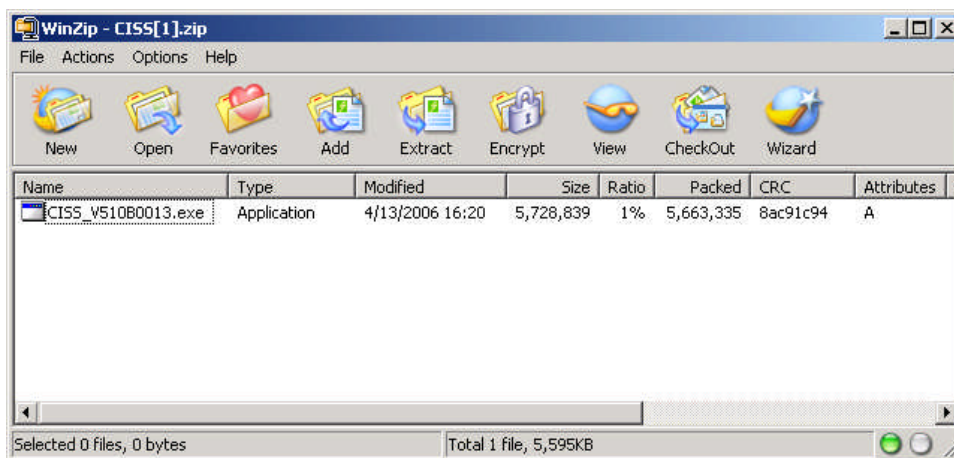
Figure 13-44. Save As dialog



- e. If a different file name or folder location is desired, change the file name and/or navigate to the desired folder. When finished, select to download the compressed installation file to the specified folder.

- f. If **Open** is selected, the compressed installation file is downloaded to the default download folder location and the file is opened in the default “.zip” program, such as in the following **WinZip®** dialog.

Figure 13-45. WinZip® dialog



Locate the updated installation file, uncompress it if necessary, and refer to section 13.3.1 for installation procedures.

13.3 Updating the CISS Application

Updates are provided for the CISS as improvements or updates are made to the application. Business Partners should configure the CISS to check for updates automatically or they should manually check for updates on a regular basis to ensure they are using the most up-to-date release. Refer to section 13.2.6 for the CISS update configuration options.

To determine which CISS version/build number and CSR version is currently installed, check the version information located in the lower area of the main menu below the Treeview region (Figure 3-6).

Figure 13-46. CISS / CSR version information



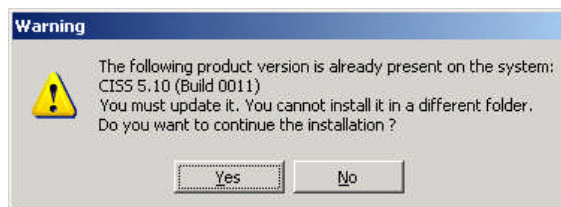
13.3.1 Installing a CISS Application Update

IMPORTANT: The following update procedures apply to the contractor version of the CISS application. Some of the update procedures for the CMS version of the CISS may differ from those shown in this section. Use only established CMS update procedures for performing all CISS application updates.

To install an updated CISS release over an existing CISS version:

- a. Double-clicking the CISS installation file (CISS_Vxxx.exe), where “xxx” is the version number, displays the following **Warning** dialog message.

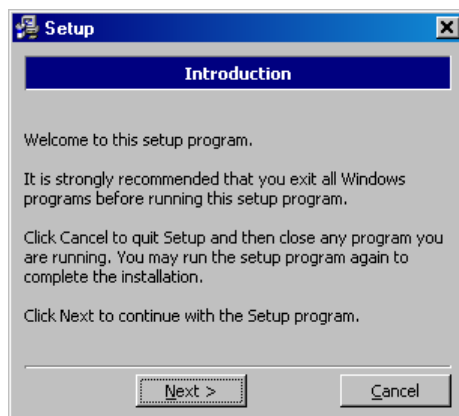
Figure 13-47. Update Warning dialog message



NOTE: When updating from a previous CISS version to a newer release, it is not necessary to update incrementally. That is, a newer release can be installed over an older version even if the newer release is one or more versions or builds more recent than the current version.

- b. Selecting terminates the update process. Selecting continues the update process and displays the following **Setup** "Introduction" dialog.

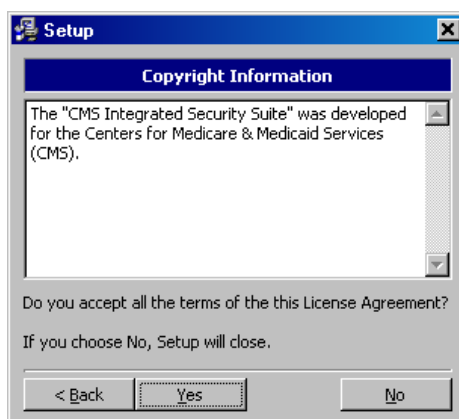
Figure 13-48. Setup "Introduction" dialog



NOTE: Since the purpose of these instructions is to update the CISS application, only the updating steps are explained. Canceling the update process retains the previous CISS version and is self-explanatory.

- c. Selecting terminates the installation process after displaying a confirmation dialog. Selecting continues the installation process and displays the following **Setup** "Copyright Information" dialog.

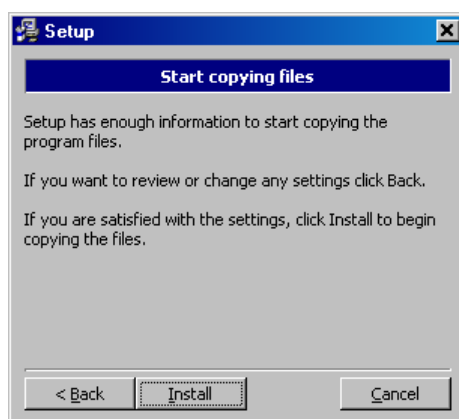
Figure 13-49. Setup "Copyright Information" dialog



WARNING: On some systems the user may not have sufficient privileges to update software. In such a case the default directory may be set to a system directory such as “WinNT\System\CISS\.” If this occurs, STOP immediately, and have your administrator update the CISS on your PC.

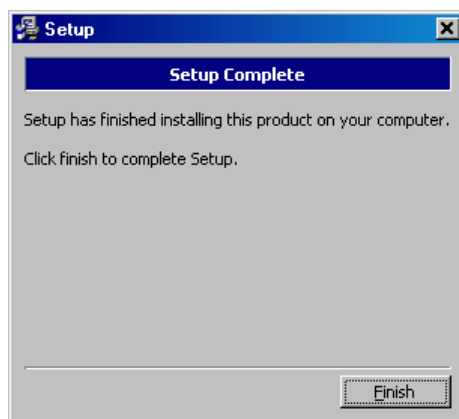
- d. Selecting terminates the installation process. Selecting displays the following **Setup** “Start copying files” dialog.

Figure 13-50. Setup “Start copying files” dialog



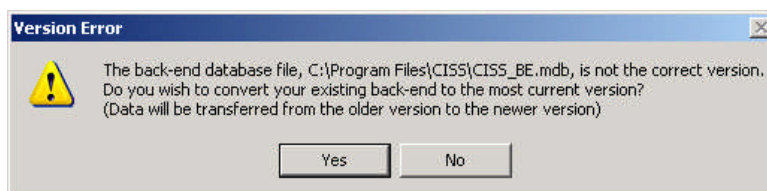
- e. Selecting starts the update process, after which the following **Setup** “Setup Complete” dialog displays.

Figure 13-51. Setup “Setup Complete” dialog



- f. Selecting completes the update process and closes the application.
- g. When CISS is initially opened after an update, it evaluates the back-end data structure to determine whether it is in the proper format. If an update to the back-end database is required, the following **Version Error** dialog message displays.

Figure 13-52. Back-end database Version Error dialog message



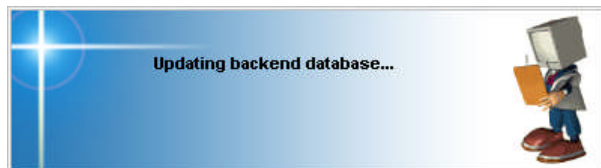
- h. Selecting updates the back-end database to the updated CISS structure and selecting exits the application since it cannot run unless the database is updated. Before the back-end database is updated, the CISS saves a backup copy of the original database in the same directory as the updated database.

NOTE: The backup database file name consists of the original file name with “(MM-DD-YYYY hhmm)” appended to the file name and a “.bak” file extension. The *MM-DD-YYYY hhmm* denotes the date and time the backup was created. For example, “Contractor XYZ(01-11-2005 0835).bak.”

The date and time format included in the backup file name are dependent on the time and date formats set in the MS Windows® Control Panel Regional Options.

- i. While the back-end database is being updated, a message box similar to the following dialog displays.

Figure 13-53. Updating backend database message



After the back-end database has been updated, the CISS is ready for data input.

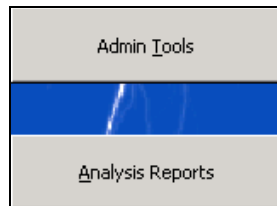
14.0 CMS Administrative Functions (For CMS Use Only)

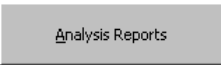
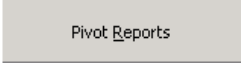
This Chapter explains the mechanics of using the CMS administrative functions that are included in the CMS-only version of the CISS application. There are no CISS functional instructions in this chapter that pertain to Business Partners or their version of the CISS application.

The CMS-only version of the CISS application allows CMS management to import the Business Partner-submitted Self-Assessment and POA&M back-end databases into a master database. Using their master database, CMS is able to review all Self-Assessment and POA&M submissions, analyze various reports; and perform the administrative functions necessary to manage, prepare, and submit the annual FISMA POA&M report. The CISS performs validation checks of the POA&M data and formats the POA&M submission in the FISMA-prescribed format.

These CMS functions are performed using the two buttons shown in the following figure which are located in the CISS main menu Component region buttons (Figure 3-4).

Figure 14-1. CMS-only Component region buttons



In addition to the above  button, the  button located in the Component region (Figure 3-3) of the CISS main menu is also available to create custom Pivot Table Reports (refer to section 3.11).

14.1 Admin Tools

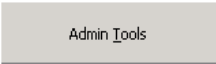
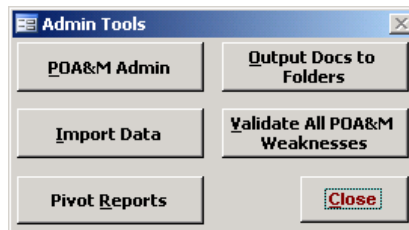

Selecting the  button displays the following **Admin Tools** menu.

Figure 14-2. Admin Tools menu



Selecting  returns to the CISS menu.

14.1.1 POA&M Admin Button


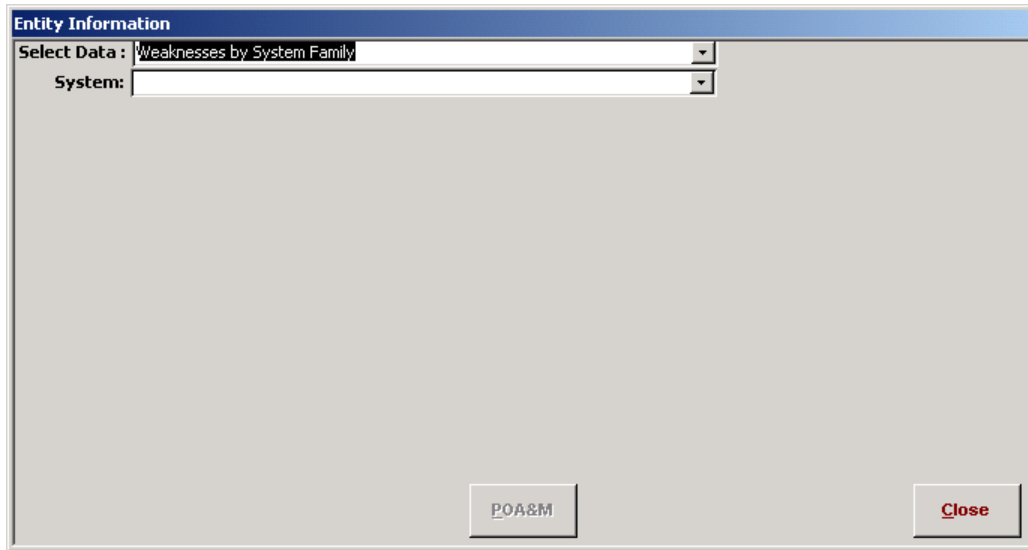
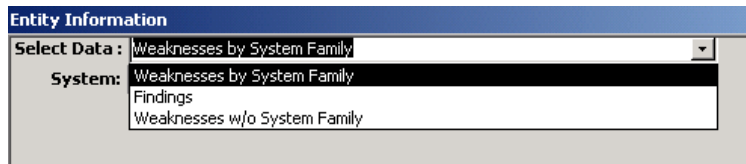
To obtain reports of Weaknesses by CMS System Family assignments, and to review all Findings and the Weaknesses without CMS System Family assignments, select the **Admin Tools** menu  button (Figure 14-2) to open the following **Entity Information** dialog.

Figure 14-3. Entity Information dialog



Select **Close** to return to the **Admin Tools** menu (Figure 14-2) or select a report data-type option from the following “Select Data” drop-down menu.

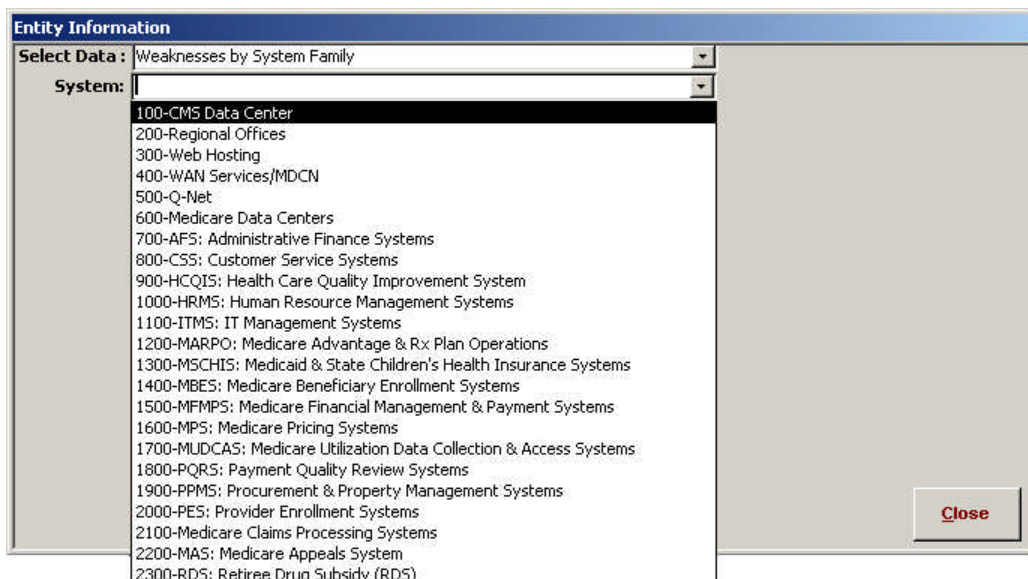
Figure 14-4. Entity Information dialog “Select Data” drop-down menu



14.1.1.1 Weaknesses by System Family Report

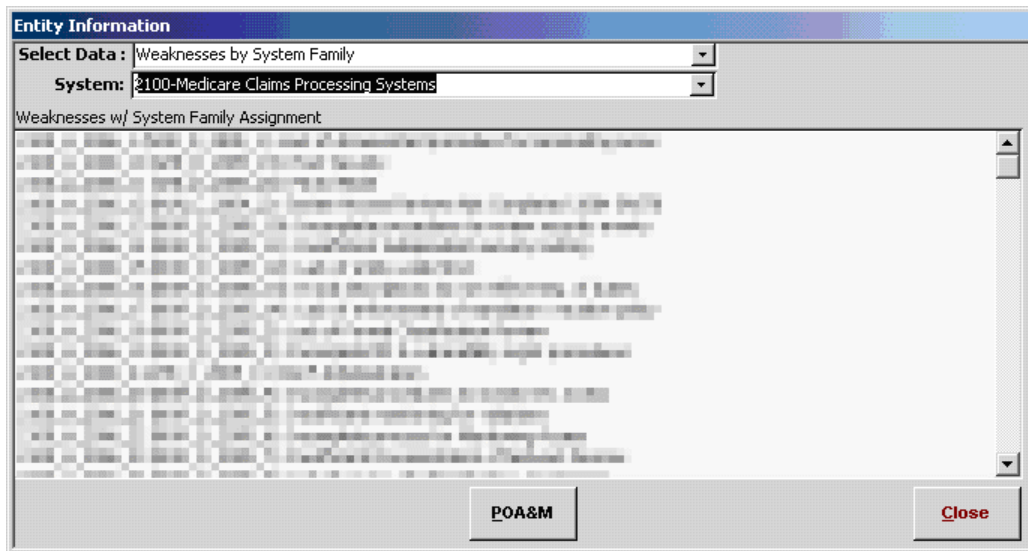
If “Weaknesses by System Family” is selected in the **Entity Information** dialog “Select Data” field (Figure 14-4), select a CMS System Family from the following “System” field drop-down menu.

Figure 14-5. Entity Information dialog “System” drop-down menu



If the master database contains Weaknesses assigned to the selected CMS System Family, the Weaknesses will be listed in the following **Entity Information** “Weaknesses w/ System Family Assignment” dialog window.

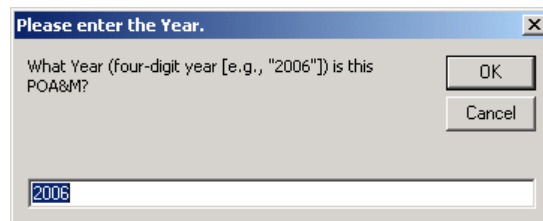
Figure 14-6. Entity Information “Weaknesses w/ System Family Assignment” dialog window



NOTE: The Weaknesses displayed in the above **Entity Information** dialog are purposely distorted to hide any real Weakness titles submitted by Business Partners.

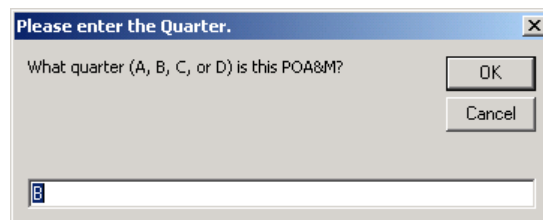
Select one of the listed Weaknesses, followed by the **POA&M** button. This displays the following **Please enter the Year** dialog.

Figure 14-7. Please enter the Year dialog



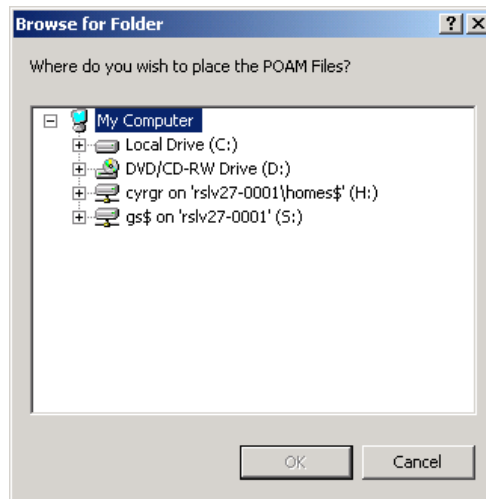
Selecting **Cancel** returns to the **Entity Information** “Weaknesses w/ System Family Assignment” dialog window (Figure 14-6). Entering the Year desired and selecting **OK** displays the following **Please enter the Quarter** dialog.

Figure 14-8. Please enter the Quarter dialog



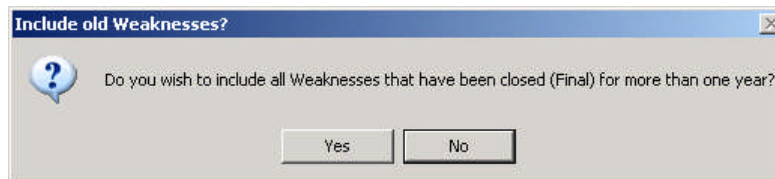
Selecting returns to the **Entity Information** “Weaknesses w/ System Family Assignment” dialog window (Figure 14-6). Entering the Quarter desired and selecting displays a **Browse for Folder** dialog similar to the following.

Figure 14-9. Browse for Folder dialog



Selecting returns to the **Entity Information** “Weaknesses w/ System Family Assignment” dialog window (Figure 14-6). Otherwise, browse to the folder where you wish to save the resultant report and select to display the following **Include old Weaknesses** dialog.

Figure 14-10. Include old Weaknesses dialog



Selecting *excludes* all closed weaknesses that are more than one year old and selecting *includes* all closed weaknesses regardless of how long they have been closed (Final) and generates the requested MS Excel[®] report.

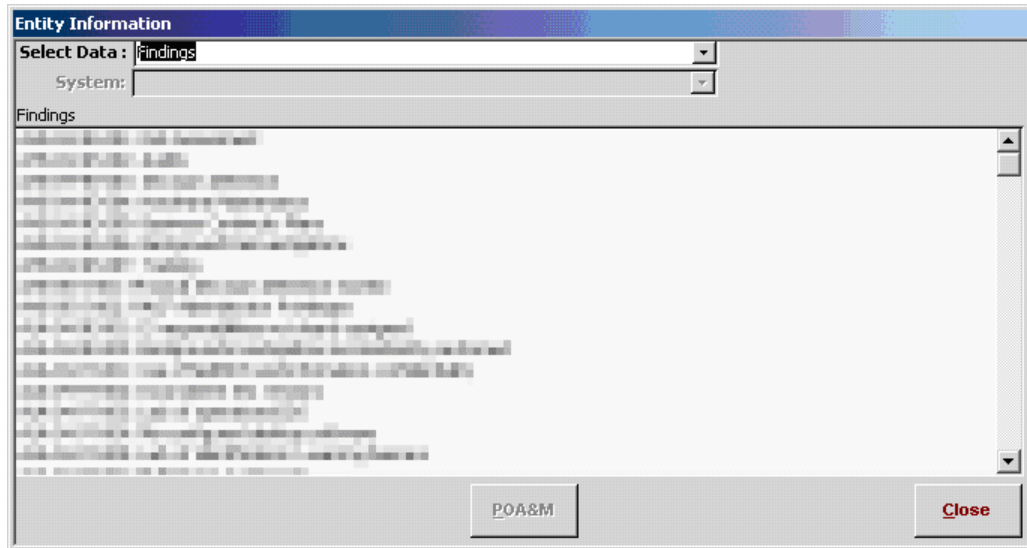
After the report is created, Windows Explorer[®] opens to the folder selected in the **Browser for Folder** dialog (Figure 14-7) and displays a file listing for that folder. The file names created during this report process consist of the selected Year (Figure 14-7), Quarter (Figure 14-8), and CMS System Family (Figure 14-6) (i.e. “2006B CMS OIS Medicare Claims Processing Systems_MASTER.xls”).

There will always be a “_MASTER.xls” file which contains all Weaknesses based on the selection criteria. Since the CMS ProSight tool cannot import more than 100 MS Excel[®] rows at a time, the “_MASTER.xls” file is broken into smaller files, each containing up to 100 rows. These files use the same naming convention as previous stated except each file name ends with “_1.xls,” “_2.xls,” “_3.xls” etc. instead of “_MASTER.xls.”

14.1.1.2 Finding(s) Review

If “Finding(s)” is selected in the **Entity Information** dialog “Select Data” field (Figure 14-4), the “System” field is disabled and a list all Findings contained in the master database displays in the following **Entity Information** “Findings” dialog window.

Figure 14-11. Entity Information “Findings” dialog window



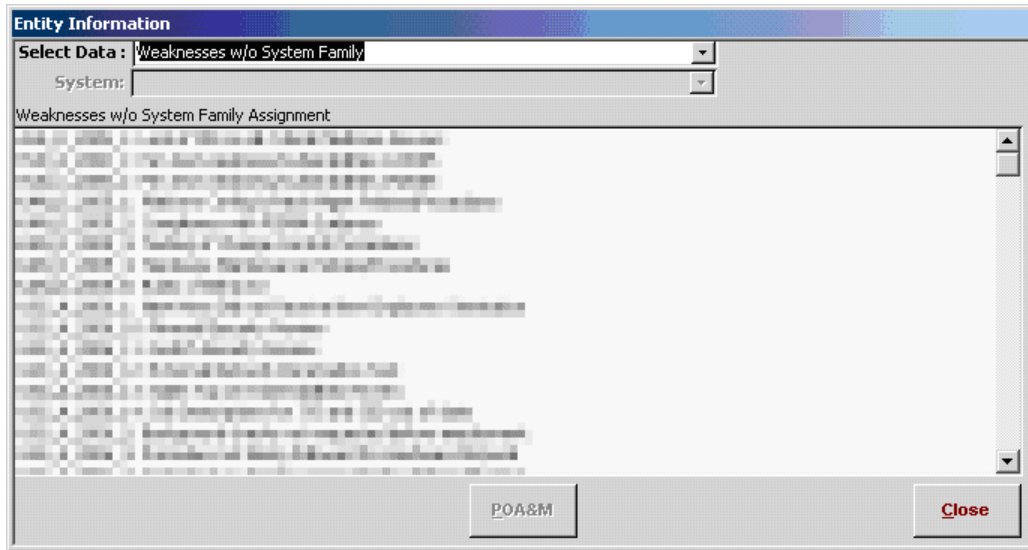
NOTE: The Findings displayed in the above **Entity Information** dialog are purposely distorted to hide any real Findings titles submitted by Business Partners.

Selecting returns to the **Admin Tools** menu (Figure 14-2) or double-clicking on a Finding listed in the **Entity Information** “Findings” dialog window opens that Finding for review. Selecting in the **Findings** form returns to the **Entity Information** “Findings” dialog window (Figure 14-11).

14.1.1.3 Weaknesses w/o System Family Review

If “Weaknesses w/o System Family” is selected in the **Entity Information** dialog “Select Data” field (Figure 14-4), the “System” field is disabled and a list of all Weaknesses that have no CMS System Family assignment displays in the following **Entity Information** “Weaknesses w/o System Family Assignment” dialog window.

Figure 14-12. Entity Information dialog “Weaknesses w/o System Family” selection



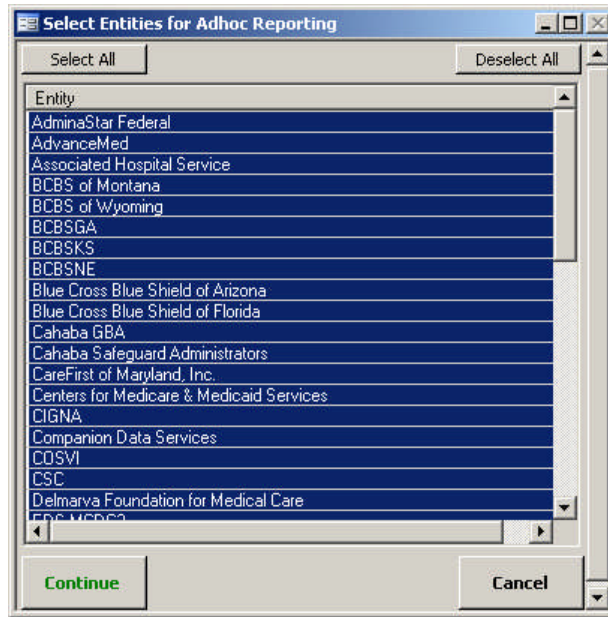
NOTE: The Weaknesses displayed in the above *Entity Information* dialog are purposely distorted to hide any real Weakness titles submitted by Business Partners.

Selecting **Close** returns to the *Admin Tools* menu (Figure 14-2) or double-clicking on a Weakness listed in the *Entity Information* “Weaknesses w/o System Family Assignment” dialog window opens that Weakness for review. Selecting **Close** in the *Weakness* form returns to the following *Entity Information* “Weaknesses w/o System Family” dialog window.

14.1.2 Output Docs to Folders Button

To output (or export) documentation submitted to support Findings and non-compliant Self-Assessment CSRs, select the *Admin Tools* menu **Output Docs to Folders** button (Figure 14-2) to open the following *Select Entities for Adhoc Reporting* dialog.

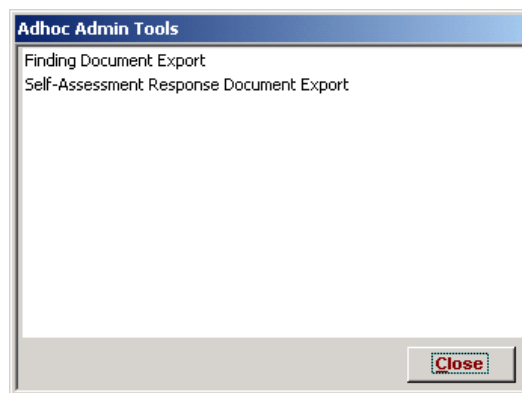
Figure 14-13. Select Entities for Adhoc Reporting dialog



Selecting returns to the **Admin Tools** menu (Figure 14-2). When the **Select Entities for Adhoc Reporting** dialog opens, all entities are selected by default (i.e., all are highlighted). To deselect all entities, select or single-click on a single entity to select it which also deselects all other entities. Or, to deselect a single entity or multiple entities while all entities are selected (i.e., highlighted) *without* deselecting all entities, select the entity(ies) with a single-click while holding down the **Ctrl** key. This removes the entity(ies) selection highlight without deselecting all other entities.

After all entity selections are completed, selecting opens the following **Adhoc Admin Tools** dialog with the following adhoc selections.

Figure 14-14. Adhoc Admin Tools dialog

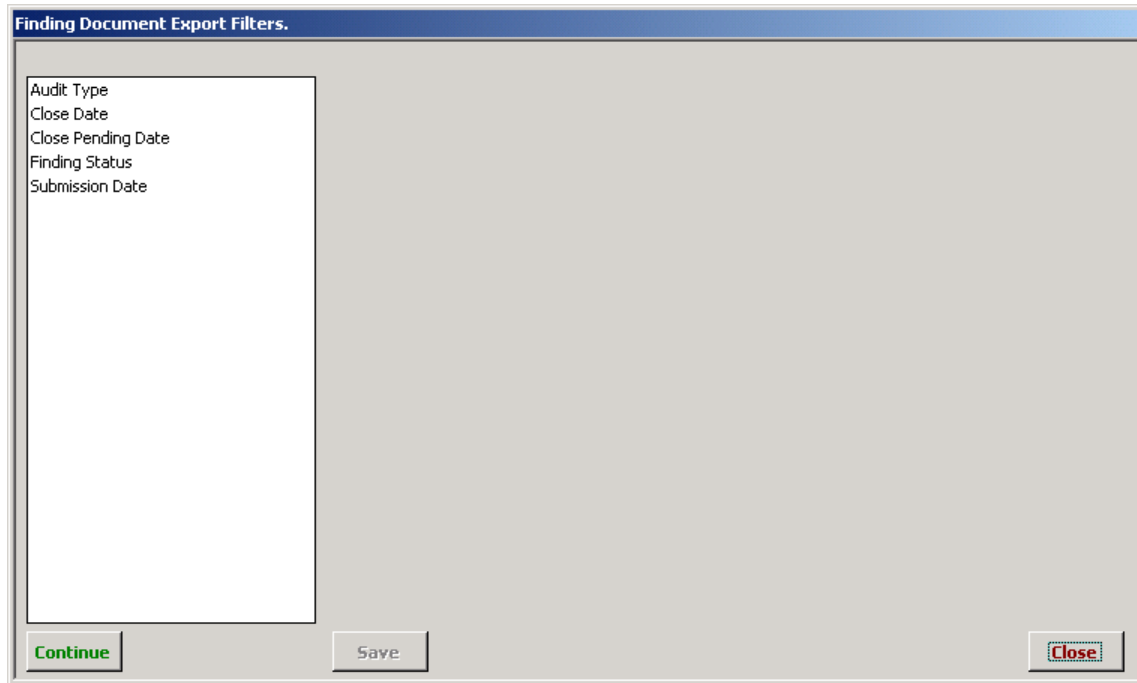


Selecting returns to the **Admin Tools** menu (Figure 14-2).

14.1.2.1 Finding Document Export

Double-clicking on the “Finding Document Export” selection (refer to Figure 14-14) opens the following **Finding Document Export Filters** selection form.

Figure 14-15. Finding Document Export Filters selection form



Selecting **Close** returns to the **Admin Tools** menu (Figure 14-2). Selecting any of the Primary filter selections opens a Secondary filter selection dialog window.

14.1.2.1.1 Document Export Filter Selection

Refer to Findings section 11.7.3 for instructions on selecting Primary and Secondary Finding filters. The filter selections may be different but the selection process is the same. When finished selecting the Primary and Secondary filters, return to this section to complete the document export process.

After the filter selections are completed, select **Continue** in the **Finding Document Export Filters** selection form (Figure 14-15). Once **Continue** is selected, whether it results in documents being exported or no records being found, all filters are reset and must be reselected to export other documents.

Some filter selection combinations may result in no Finding records being found that meet all of the selection criteria; consequently, the following message displays.

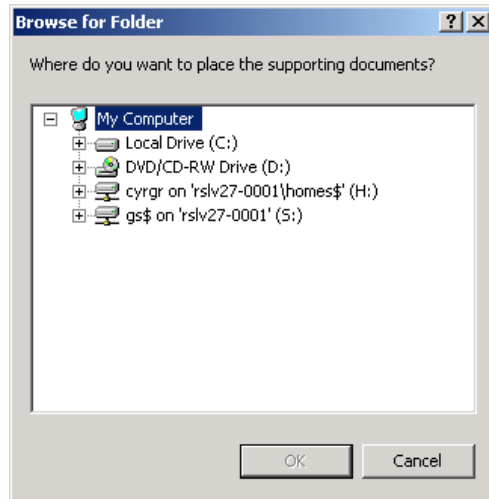
Figure 14-16. No records found message



14.1.2.1.2 Document Export Folder Selection

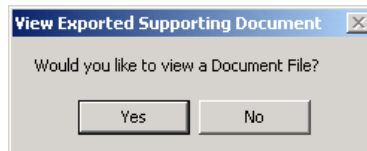
If records are found matching the selected criteria, a **Browse for Folder** dialog similar to the following displays.

Figure 14-17. Browse for Folder dialog



Selecting returns to the **Finding Document Export Filters** selection form (Figure 14-15). Otherwise, browse to the folder where you wish to save the exported documents and select to export the selected documents. After the documents are exported, the following **View Exported Supporting Document** dialog displays.

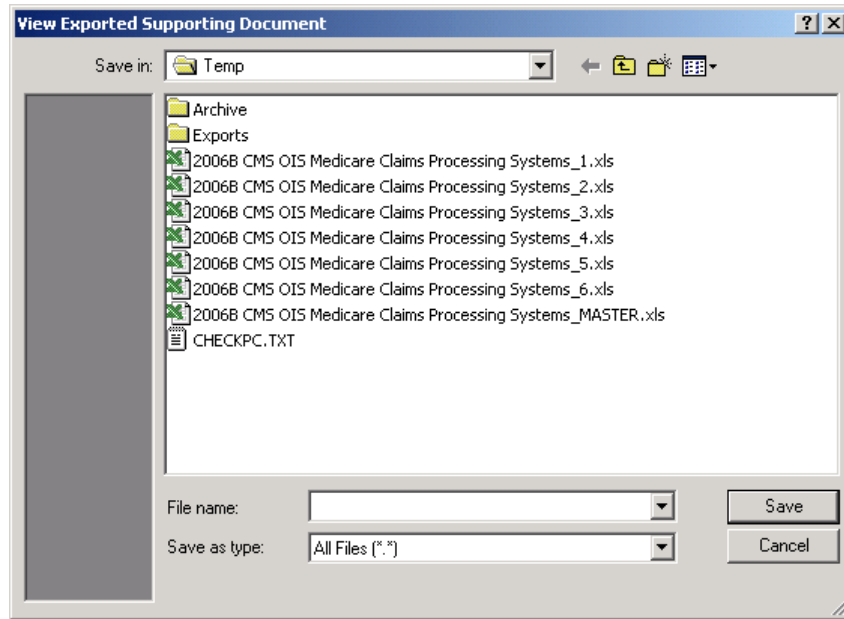
Figure 14-18. View Exported Supporting Document dialog



14.1.2.1.3 Document Export Viewing Selection

Selecting returns to the **Finding Document Export Filters** selection form (Figure 14-15). Selecting opens the following **View Exported Supporting Document** dialog so the user can browse and view exported documents.

Figure 14-19. View Exported Supporting Document dialog

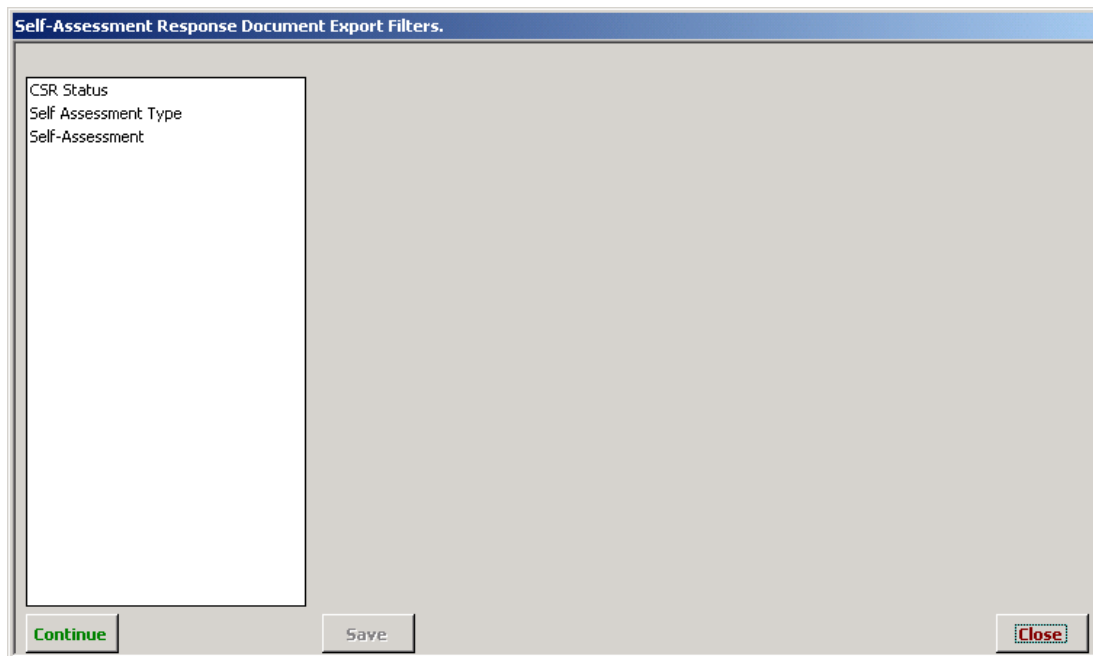


Selecting **Cancel** returns to the *View Exported Supporting Document* dialog (Figure 14-18). Otherwise, browse to the desired Business Partner export folder and Finding, and select the document you wish to view. When finished viewing the selected document, close it and the CISS returns to the *View Exported Supporting Document* dialog (Figure 14-18).

14.1.2.2 Self-Assessment Response Document Export

Double-clicking on the “Self-Assessment Response Document Export” selection (refer to Figure 14-14) opens the following *Self-Assessment Response Document Export Filters* selection form.

Figure 14-20. Self-Assessment Response Document Export Filters selection form



Selecting **Close** returns to the **Admin Tools** menu (Figure 14-2). Selecting any of the Primary filter selections opens a Secondary filter selection dialog window.

Refer to Weaknesses section 7.7.3 for instructions on selecting Primary and Secondary Finding filters. The filter selections may be different but the selection process is the same. When finished selecting the Primary and Secondary filters, return to this section to complete the document export process.

Some filter selection combinations may result in no Self-Assessment records being found that meet all of the selection criteria; consequently, the following message displays.

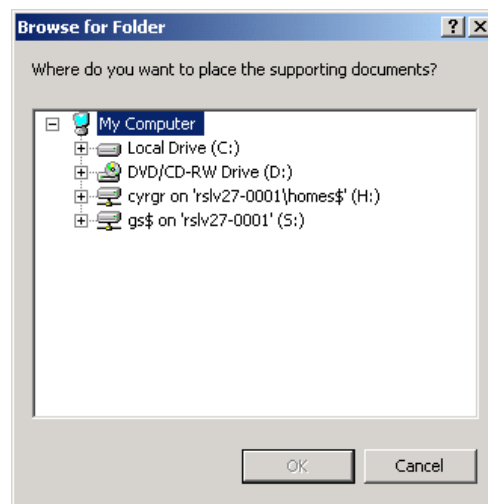
Figure 14-21. No records found message



14.1.2.2.1 Document Export Folder Selection

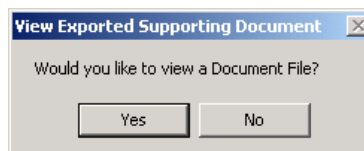
If records are found matching the selected criteria, a **Browse for Folder** dialog similar to the following displays.

Figure 14-22. Browse for Folder dialog



Selecting **Cancel** returns to the **Self-Assessment Response Document Export Filters** selection form (Figure 14-20). Otherwise, browse to the folder where you wish to save the exported documents and select **OK** to export the selected documents. After the documents are exported, the following **View Exported Supporting Document** dialog displays.

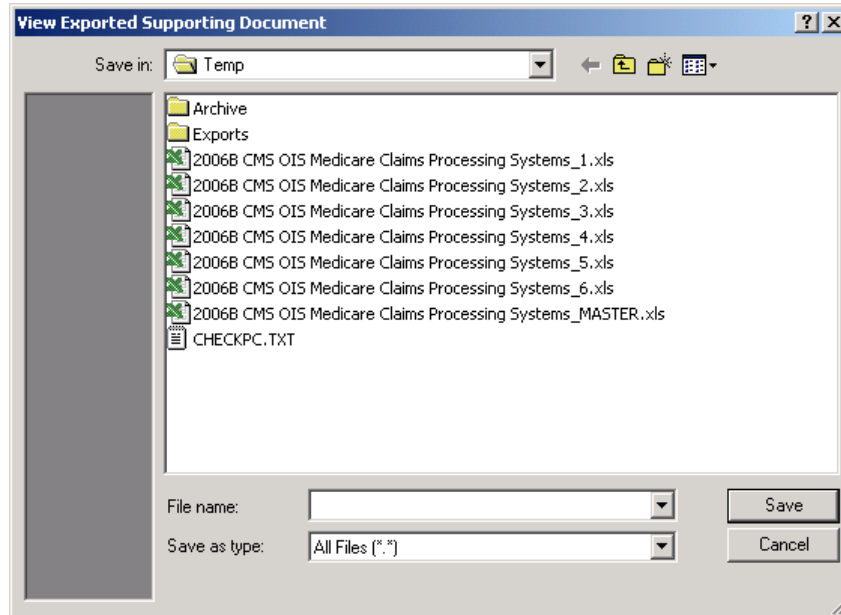
Figure 14-23. View Exported Supporting Document dialog



14.1.2.2.2 Document Export Viewing Selection

Selecting returns to the **Self-Assessment Response Document Export Filters** selection form (Figure 14-20). Selecting opens the following **View Exported Supporting Document** dialog so the user can browse and view exported documents.

Figure 14-24. View Exported Supporting Document dialog

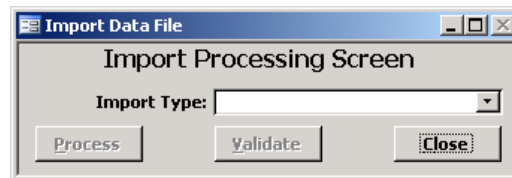


Selecting returns to the **View Exported Supporting Document** dialog (Figure 14-23). Otherwise, browse to the desired Business Partner export folder and Self-Assessment, and select the document you wish to view. When finished viewing the selected document, close it and the CISS returns to the **View Exported Supporting Document** dialog (Figure 14-23).

14.1.3 Import Data Button

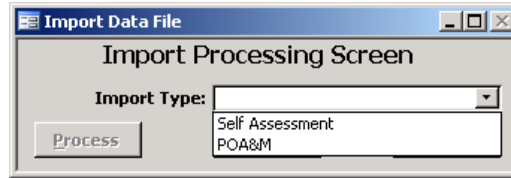
To import Business Partner Self-Assessments or POA&M submissions into the CMS master database, select the **Admin Tools** menu button (Figure 14-2) to open the following **Import Data File** dialog.

Figure 14-25. Import Data File dialog



Open the “Import Type” drop-down menu to display the following two available selections: Self-Assessment and POA&M. Selecting returns to the **Admin Tools** menu (Figure 14-2).

Figure 14-26. “Import Type” drop-down menu

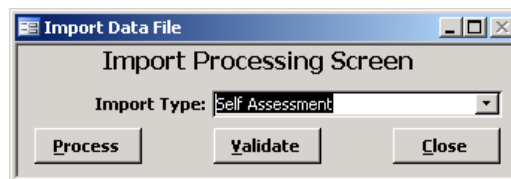


To import Self-Assessments, proceed to the next section, 14.1.3.1 and to import POA&Ms, proceed to section 14.1.3.2.

14.1.3.1 Self-Assessments

To import Self-Assessments, select “Self-Assessment” at the following *Import Data File* drop-down menu. Selecting returns to the *Admin Tools* menu (Figure 14-2).

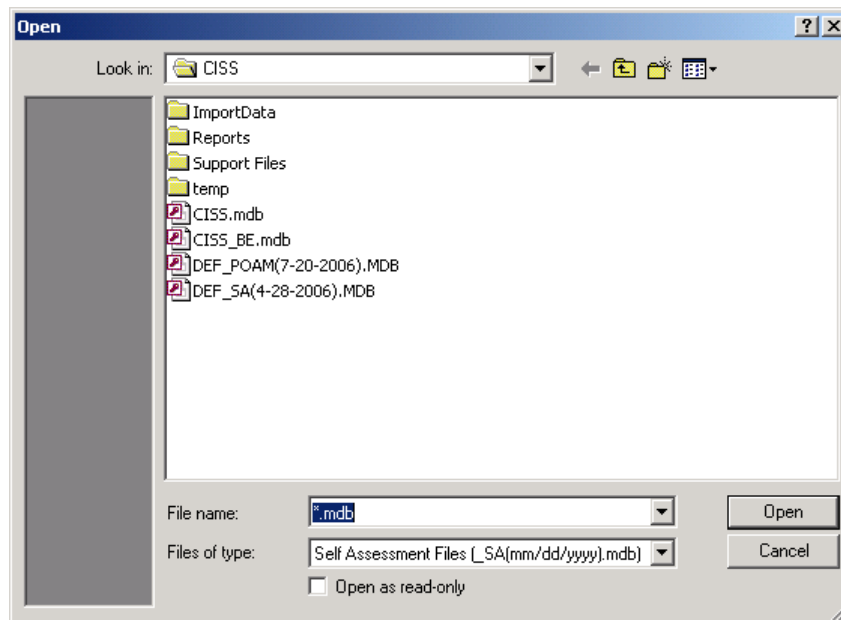
Figure 14-27. “Import Type” Self-Assessment selection



14.1.3.1.1 Validating Self-Assessments

To validate a Self-Assessment before importing it into the master database, select to open the following *Open* file dialog.

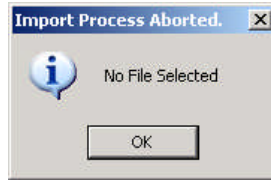
Figure 14-28. Self-Assessment Open file dialog



NOTE: The Self-Assessment file name defaults to the Business Partner’s short name abbreviation followed by “_SA” (for Self-Assessment) and the submission date formatted as “mm/dd/yyyy.”

Selecting displays the following message and selecting in the message dialog returns to the Import Data File drop-down menu (Figure 14-27).

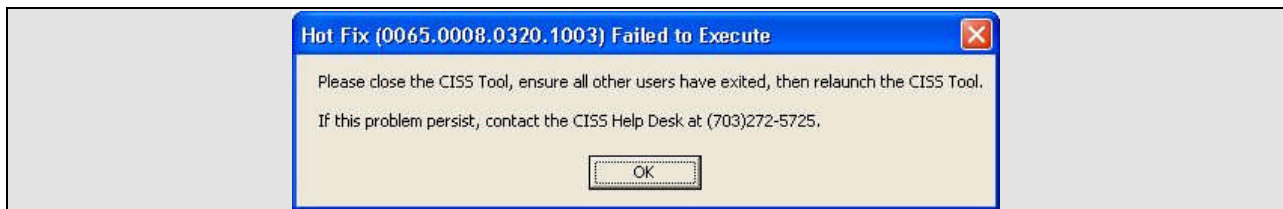
Figure 14-29. No File Selected message



Otherwise, locate and select the Self-Assessment file you wish to validate and select to begin the validation process.

NOTE: If a “Hot Fix” error message such as shown in Figure 14-30 displays, there is a possible problem with the CMS CISS release that must be corrected before the Self-Assessment(s) can be imported. Selecting closes the CISS.

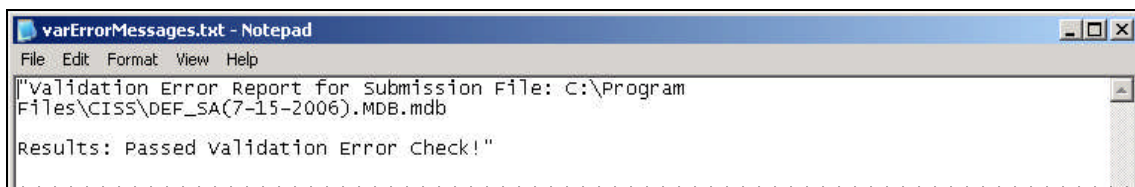
Figure 14-30. Hot Fix error message



To ensure that CMS has the latest CISS release, reopen the CISS and select the button located above the right portion of the main menu (Figure 3-3). If there is an updated release available, install the update (refer to section 3.1.2), then try validating the Self-Assessment again. If the problem continues, call the Help Desk at (703) 272-5725.

If the Self-Assessment passes the validation checks, a message similar to the following displays in Notepad.

Figure 14-31. Validation success message



If the Self-Assessment contains any structural errors, error messages similar to the following display. These errors indicate that the Business Partner is using an older release of the CISS application. A newer release is available that may contain some business rule or database structural differences. Inform the Business Partner to update their CISS application and resubmit their Self-Assessment.

Figure 14-32. Self-Assessment validation table structure error message

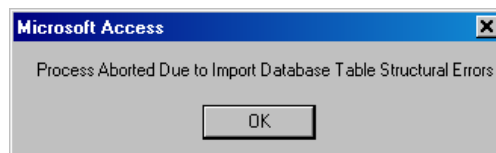
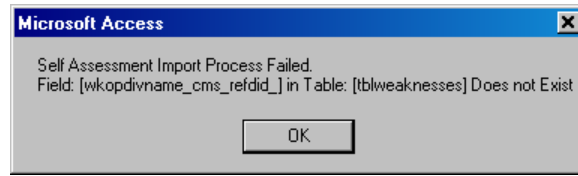


Figure 14-33. Self-Assessment validation process field error message

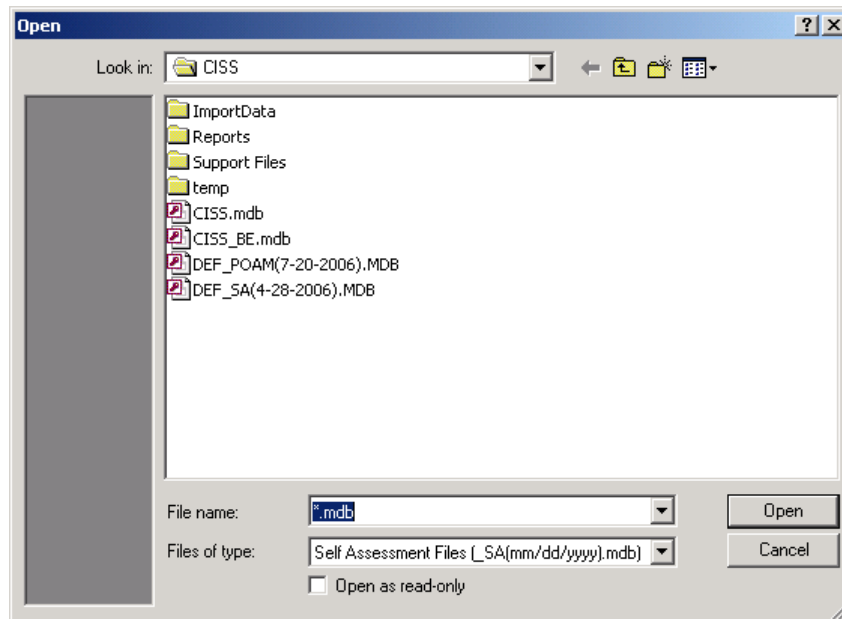


Selecting **OK** in each of the above error messages returns to the *Import Data File* dialog (Figure 14-27).

14.1.3.1.2 Processing Self-Assessments

Before importing a Self-Assessment into the master database, refer to the previous section, 14.1.3.1.1, to validate it. To process (i.e., import) a Self-Assessment into the master database, select **Process** to open the following *Open* file dialog.

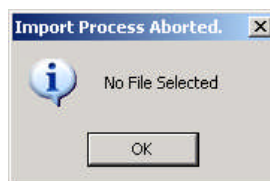
Figure 14-34. Self-Assessment Open file dialog



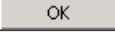
NOTE: The Self-Assessment file name defaults to the Business Partner’s short name abbreviation followed by “_SA” (for Self-Assessment) and the submission date formatted as “mm/dd/yyyy.”

Selecting **Cancel** displays the following message and selecting **OK** in the message dialog returns to the Import Data File drop-down menu (Figure 14-27).

Figure 14-35. No File Selected message

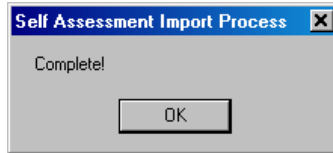


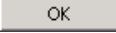
Otherwise, locate and select the Self-Assessment file you wish to import, and select **Open** to begin import process.

NOTE: If a “Hot Fix” error message such as shown in Figure 14-30 displays, there is a possible problem with the CMS CISS release that must be corrected before the Self-Assessment(s) can be imported. Refer to the “Note” text after Figure 14-30 for additional information. Selecting  closes the CISS.

When the Self-Assessment import process has completed, the following message displays.

Figure 14-36. Self-Assessment Import Process complete message



Selecting  in the message dialog returns to the **Admin Tools** menu (Figure 14-2). The imported Self-Assessment is now included in the CMS master back-end database and is available for display in the main menu Treeview nodes.

14.1.3.2 POA&Ms

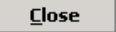
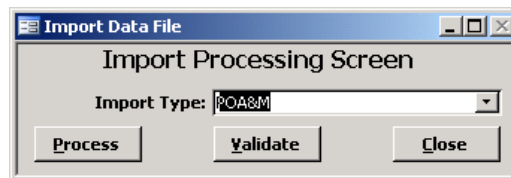
To import POA&Ms, select “POA&M” at the following **Import Data File** drop-down menu. Selecting  returns to the **Admin Tools** menu (Figure 14-2).

Figure 14-37. “Import Type” POA&M selection



14.1.3.2.1 Validating POA&Ms


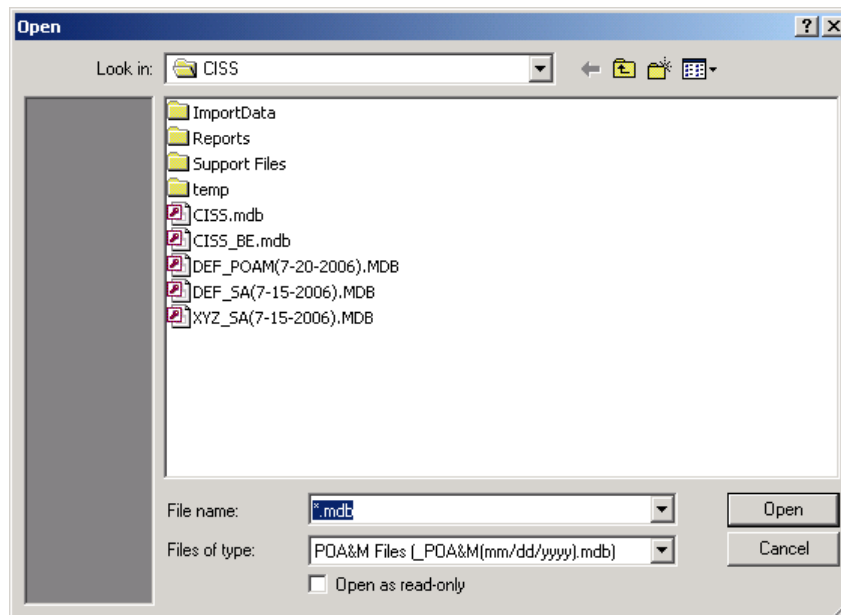
To validate a POA&M before importing it into the master database, select  to open the following **Open** file dialog.

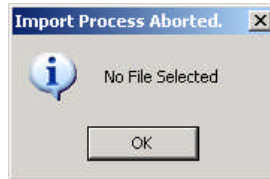
Figure 14-38. POA&M Open file dialog



NOTE: The POA&M file name defaults to the Business Partner’s short name abbreviation followed by “_POAM” (for POA&M) and the submission date formatted as “mm/dd/yyyy.”

Selecting displays the following message and selecting in the message dialog returns to the Import Data File drop-down menu (Figure 14-37).

Figure 14-39. No File Selected message

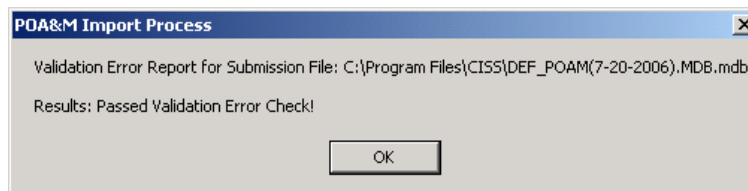


Otherwise, locate and select the POA&M file you wish to validate and select to begin the validation process.

NOTE: If a “Hot Fix” error message such as shown in Figure 14-30 displays, there is a possible problem with the CMS CISS release that must be corrected before the Self-Assessment(s) can be imported. Refer to the “Note” text after Figure 14-30 for additional information. Selecting closes the CISS.

If the POA&M passes the validation checks, a message similar to the following displays:

Figure 14-40. Validation success message



If the POA&M contains any structural errors (i.e., missing fields), error messages similar to the following display. These errors indicate that the Business Partner is using an older release of the CISS application. A newer release is available that may contain some business rule or database structural differences. Inform the Business Partner to update their CISS application and resubmit their POA&M.

Figure 14-41. POA&M validation table structure error message

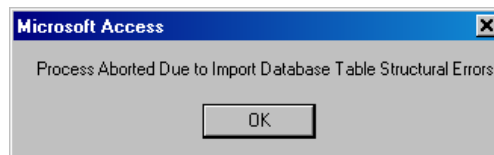
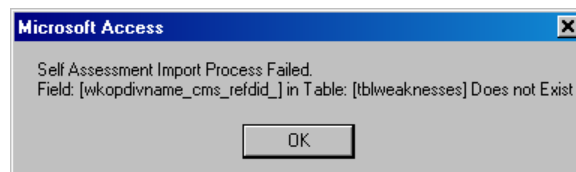


Figure 14-42. POA&M validation process field error message

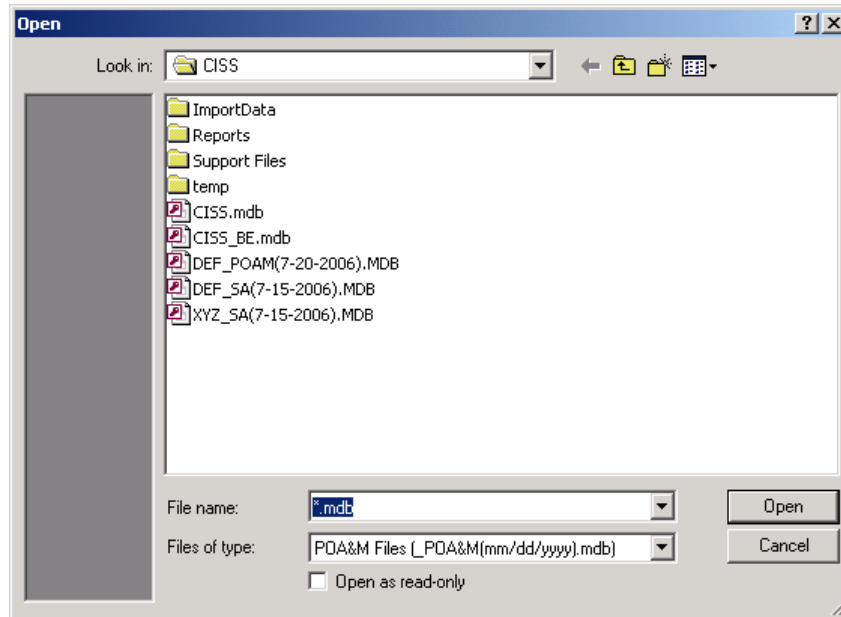


Selecting in each of the above error messages returns to the **Import Data File** dialog (Figure 14-37).

14.1.3.2.2 Processing POA&Ms

Before importing a POA&M into the master database, refer to the previous section, 14.1.3.2.1, to validate it. To process (i.e., import) a POA&M into the master database, select **Process** to open the following **Open** file dialog.

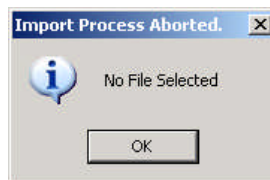
Figure 14-43. POA&M Open file dialog



NOTE: The POA&M file name defaults to the Business Partner’s short name abbreviation followed by “_POAM” (for POA&M) and the submission date formatted as “mm/dd/yyyy.”

Selecting **Cancel** displays the following message (Figure 14-44) and selecting **OK** in the message dialog returns to the Import Data File drop-down menu (Figure 14-37).

Figure 14-44. No File Selected message

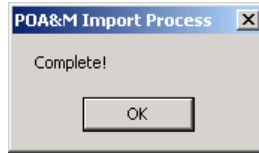


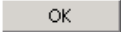
Otherwise, locate and select the POA&M file you wish to import, and select **Open** to begin import process.

NOTE: If a “Hot Fix” error message such as shown in Figure 14-30 displays, there is a possible problem with the CMS CISS release that must be corrected before the Self-Assessment(s) can be imported. Refer to the “Note” text after Figure 14-30 for additional information. Selecting **OK** closes the CISS.


When the POA&M import process has completed, the following message displays.

Figure 14-45. POA&M Import Process complete message



Selecting  in the message dialog returns to the **Admin Tools** menu (Figure 14-2). The imported Self-Assessment is now included in the CMS master back-end database and is available for display in the main menu Treeview nodes.

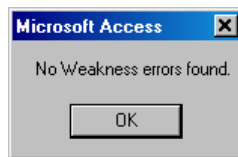
14.1.4 Validate All POA&M Weaknesses Button

To validate all POA&M Weaknesses in the CMS master database, select the **Admin Tools** menu  button (Figure 14-2). When this button is selected, the CISS begins its internal validation process on all POA&M Weaknesses.

NOTE: This validation process can take a considerable amount of time depending on the number of Weaknesses in the master database.

If no errors are found during the validation process, the following dialog displays.

Figure 14-46. Weakness Validate confirmation message



Otherwise, an error report similar to the following example is prepared in MS Word[®] and displayed for the user to review. This error report can be printed or saved for further review.

Figure 14-47. Example Weakness validation error report

Weakness	Error
XYZ 2100_A_2006_3 (XYZ_B_2005_7)	No documents are provided for Finding XYZ-05-S-002 Closed Pending status date.
	No documents are provided for Finding XYZ-05-S-001 Closed status date.
2100_D_2005_8 (XYZ_B_2005_6)	Action Plan ("Physical Access Controls") needs an update to the Projected Date of Milestone ("Configuration"). Currently it is listed as 4/30/2006 with a status of Ongoing.

14.1.5 Pivot Reports Button

Refer to section 3.11 for an explanation of MS Word[®] Pivot Reports.

14.2 Validate Support Documents

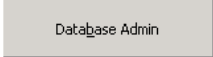
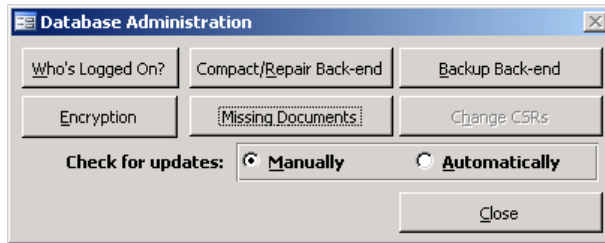
To validate that all required support documents were submitted and are available to the CMS master database, select the  button from the Application Control region of the main menu (Figure 3-3) to display the following dialog menu.

Figure 14-48. Database Administration dialog



Selecting **Close** returns to the main menu. Selecting **Missing Documents** opens the following **Missing Documents** dialog.


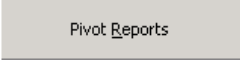
Figure 14-49. Missing Documents dialog



If any documents are listed in the **Missing Documents** dialog, CMS should request that the appropriate Business Partner correct the documentation error (refer to section 4.7.1) and resubmit the applicable Self-Assessment or POA&M.

NOTE: The missing documents displayed in the above **Missing Documents** dialog are purposely distorted to hide any real document file names submitted by Business Partners.

14.3 Analysis Reports

In addition to the  button explained in this section, the  button located in the Component region (Figure 3-3) of the CISS main menu is also available to create custom Pivot Table Reports (refer to section 3.11).

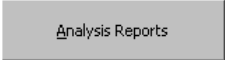
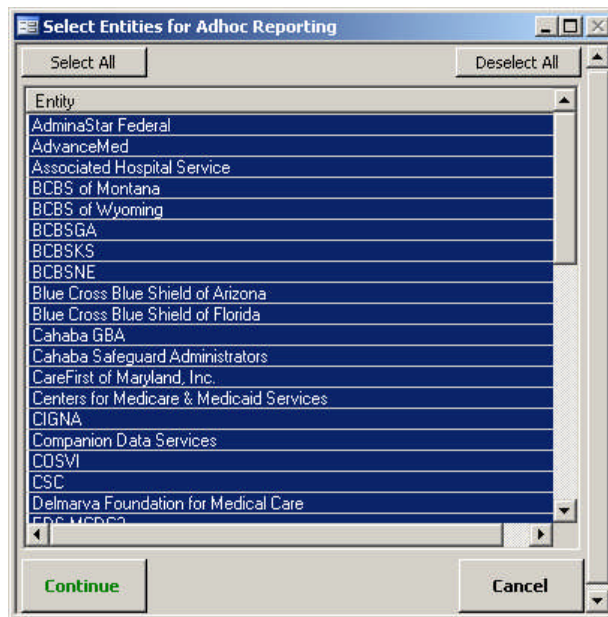
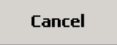
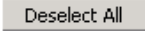
To perform adhoc analysis and obtain reports of selected data in the CMS master database, select the Component region  button (refer to section 3.4.1) to open the following **Select Entities for Adhoc Reporting** dialog.

Figure 14-50. Select Entities for Adhoc Reporting dialog



Selecting  returns to the CISS main menu. When the **Select Entities for Adhoc Reporting** dialog opens, all entities are selected by default (i.e., all are highlighted). To deselect all entities, select  or single-click on a single entity to select it which also deselects all other entities. Or, to deselect a single entity or multiple entities while all entities are selected (i.e., highlighted) *without* deselecting all entities, select the entity(ies) with a single-click while holding down the **Ctrl** key. This removes the entity(ies) selection highlight without deselecting all other entities.


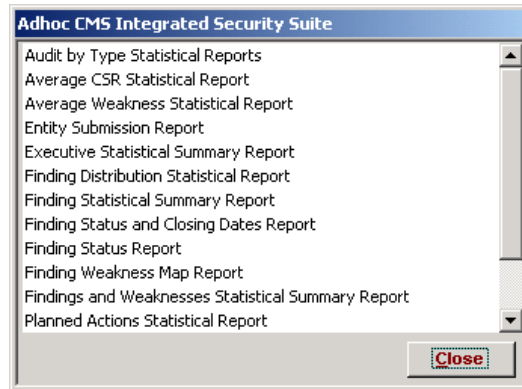
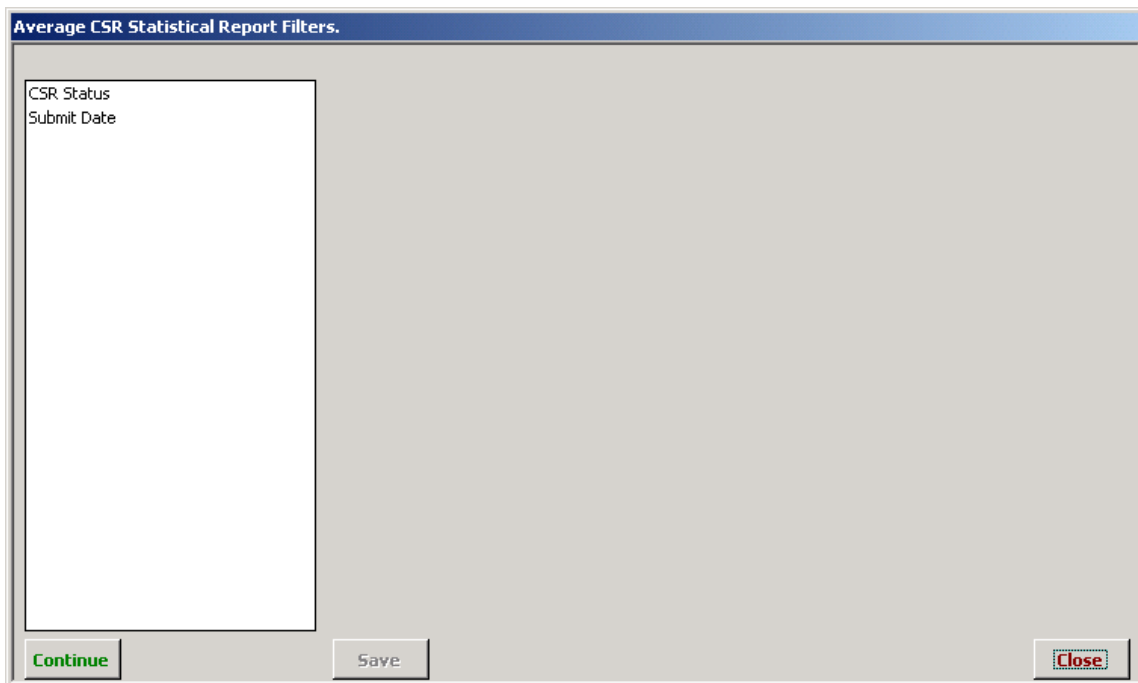
After all entity selections are completed, selecting  opens the following **Adhoc CISS** dialog with the following adhoc selections.

Figure 14-51. Adhoc CISS dialog



The **Adhoc CISS** dialog allows users to generate customized reports and statistics that are based on user-selected filters (or parameters). For example, double-clicking the “Average CSR Statistical Report” selection opens the following **Average CSR Statistical Report Filters** selection form.

Figure 14-52. Average CSR Statistical Report Filters selection form



Selecting **Close** closes the **Average CSR Statistical Report Filters** form and returns to the **Adhoc CISS** dialog (Figure 14-51). Selecting the “CSR Status” Primary filter displays the following Secondary filter sections dialog.

Figure 14-53. Average CSR Statistical Report Filters Secondary filters

The left side of the form lists the Primary filters that are available for selection. Selecting any of the Primary filters opens additional selection-based Secondary filters in a separate window on the right side of the form.

After selecting a Primary filter from the left side of the filters selection form, select one or more Secondary filters (i.e., multiple filters can be selected) from the right side of the form. To select a Secondary filter, highlight the filter(s) by single-clicking the desired filter(s). To remove a selected Secondary filter(s), click the filter again to deselect it. To select all the Secondary filters, select and to deselect all Secondary filters, select .

When finished selecting the Secondary filter(s) for a selected Primary filter, select to save the filter selection(s) or to exit *without* saving the Secondary filters. Both selections return to the Primary filter selection form for the selected report type.

Additional Primary and Secondary filters can be selected by repeating the above procedures until all desired filters are selected. After the filter selections are completed, select to generate a report based on the specified filter selections or to exit *without* creating a report. Once is selected, whether it results in a report or no records being found, all filters are reset and must be reselected to generate another report.

The process for selecting Primary and Secondary filters is the same for all Adhoc CISS reports. The same or similar Primary and Secondary filter functions have been covered in their respective security element chapters. Refer to the Adhoc reporting sections within each of these chapters for guidance in selecting their respective Primary and Secondary filters. For reference purposes, the security element adhoc reporting sections are listed below:

- Self-Assessments – Section 6.11.9
- Weaknesses – Section 7.7.3
- Actions Plans – Section 8.8.3
- Audits – Section 10.7.3
- Findings – Section 11.7.3

14.4 Updating Imported Weaknesses

After Business Partner-submitted Weaknesses are imported into the master database, each Weakness must be renumbered to incorporate the CMS POA&M numbering schema and the Weakness projected closed date may need to be updated.

14.4.1 Assigning CMS Weakness Numbers

After the Business Partner POA&M submission is imported into the CMS master database, open the applicable Weakness submission to enter the CMS numbering schema into the “CMS” fields in the yellow highlighted area depicted in the following figure.

Figure 14-54. Imported Weakness form

The screenshot shows a 'Weakness' form with the following details:

- Entity:** DEF
- Quarter:** C
- Year:** 2002
- Number:** 7
- CMS:** (Yellow highlighted field)
- Title:** Several SANS Top20 Vulnerabilities
- Description:** Internal vulnerability scans showed that several of the SANS Top20 vulnerabilities exist for platforms residing on the internal network. This is a generic comment or description to create test data for the CISS report and export/import functions. Sufficient data should be included in the comment and description fields to permit oversight and tracking. However, since some CISS form fields are reported outside CMS (see the CISS User Guide), caution should be used when including contractor-, location-, or system-specific information, or other sensitive or identifying information in those fields.
- Category:** Incident Response
- Action Plan:** SANS Top20 Vulnerabilities
- Risk:** High
- Type:** System
- Status:** Delayed
- CMS Projected Date:** 4/1/2006
- Likelihood:** High
- Impact:** High
- FISMA Severity:** Weakness
- POCs:** Miller, Richard - (Primary), Wilson, Charles
- Findings:** DEF-03-E-007: Several SANS Top20 Vulnerabilities
- CSRs:** (Empty)
- Systems - (Disabled):** (Empty)

A red error message is present: "There are errors on this form. Click 'Validate' to see the errors!". The form is in a 'READONLY' state, as indicated by the blue bar at the bottom.

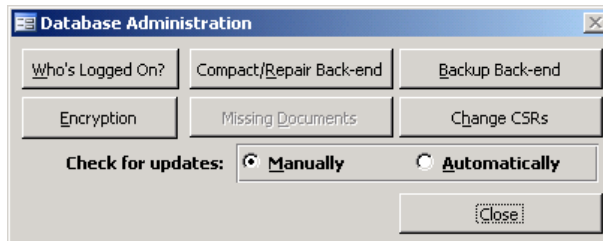
14.4.2 Updating CMS Projected Dates

After the Business Partner POA&M submission is imported into the CMS master database, open the applicable Weakness submission to update the closed date, if necessary, in the “CMS Projected Date” field in the blue highlighted area depicted in the above figure.

14.5 Change CSR Version

If the CSR version displayed in the CMS master database needs to be changed to an older version in order to perform an in-depth review or analysis, select the **Database Admin** button in the Application Control region of the main menu (Figure 3-3) to display the following menu.

Figure 14-55. Database Administration menu



Selecting **Close** returns to the main menu.

NOTE: The **Change CSRs** button is active only when the required CISS CSR change files are provided by the CISS developer and the files are located on the appropriate computer.

14.5.1 Change CSRs

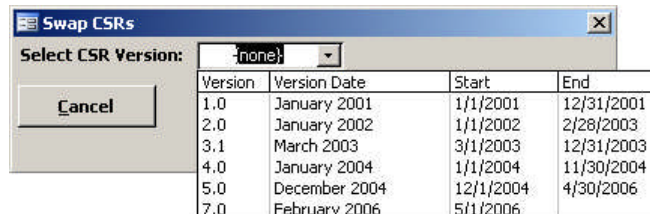
Selecting the **Change CSRs** button (Figure 14-55) opens the following **Swap CSRs** dialog.

Figure 14-56. Swap CSRs dialog



Selecting **Cancel** closes the dialog and returns to the **Database Administration** menu. Selecting the “Select CSR Version” field drop-down menu option displays a CSR version dialog similar to the following:

Figure 14-57. Swap CSRs dialog version drop-down menu



After selecting the desired CSR version (e.g., Version 5.0), the **Swap CSRs** dialog displays the selected CSR version in the “Select CSR Version:” field (Figure 14-58):

Figure 14-58. Swap CSRs dialog CSR version display

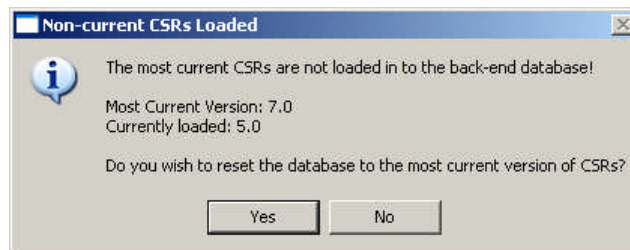


Selecting closes the dialog and returns to the **Database Administration** menu. Selecting changes the CSRs in the CMS master database to the version selected in the above process. After the CISS finishes changing the CSR version, it returns to the **Database Administration** menu (Figure 14-55).

14.5.2 Non-Current CSR Version Warning

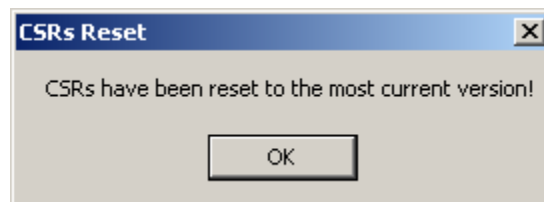
Whenever a non-current CSR version is active in the CMS master database, the following warning message displays each time the user exits or opens the CISS.

Figure 14-59. Non-current CSRs Loaded warning message



Selecting retains the previously selected non-current CSR version. Selecting resets the non-current CSRs to the current version and displays the following message after the CSRs have been reset.

Figure 14-60. CSRs Reset message



Selecting in the message dialog continues the respective exit or open CISS process.

After the back-end database has been updated, the CISS is ready for data input.
