Office of Inspector General

May 2007
Audit Project 07-001

Information Technology Events Analysis

Office of Audits

FEDERAL DEPOSIT INSURANCE CORPORATION 1933

oig

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: May 11, 2007

MEMORANDUM TO: Michael E. Bartell
Chief Information Officer
Director, Division of Information Technology

/Signed/

FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Information Technology Events Analysis*
(Audit Project 07-001)

The results of the subject analysis are provided for your information and use. Please refer to the Executive Summary for the overall results of the assignment. We appreciate the feedback that you and your staff provided to us on a draft version of the subject analysis and have incorporated those comments as appropriate. A written response was not required.

We are providing copies of this analysis to members of the Board of Directors and Audit Committee. We will also make the analysis publicly available.

If you have any questions concerning the assignment, please contact me at (703) 562-6350 or Mark F. Mulholland, Director, Corporate Management and Security Audits, at (703) 562-6316. I appreciate the courtesies extended to my staff during the assignment.

Attachment

cc: James H. Angel, Jr., Director, OERM
Rack Campbell, DIT

Audit Project 07-001
May 2007

Information Technology Events Analysis

Background and Purpose of Project

The Corporation's risk management program emphasizes guidance provided by the Treadway Commission's Committee of Sponsoring Organizations (COSO)[1] for implementing individual division/office risk management programs. The FDIC's Division of Information Technology (DIT) is in the early stage of adopting the Control Objectives for Information and Related Technology (COBIT©) framework, created by the IT Governance Institute, as part of the division's risk management program. The COBIT© framework links DIT's information technology (IT) control program objectives to the risk management activities defined by COSO.

COBIT© organizes IT activities into business-oriented processes with control objectives to help organizations ensure that IT investments align with business goals and objectives and that IT-related risks and opportunities are appropriately managed.

The purpose of the FDIC's Office of Inspector General (OIG) project was to develop an events-based approach for planning and prioritizing audit coverage of the FDIC's IT program and operations.[2] We considered the principles defined in COBIT© in developing our approach.

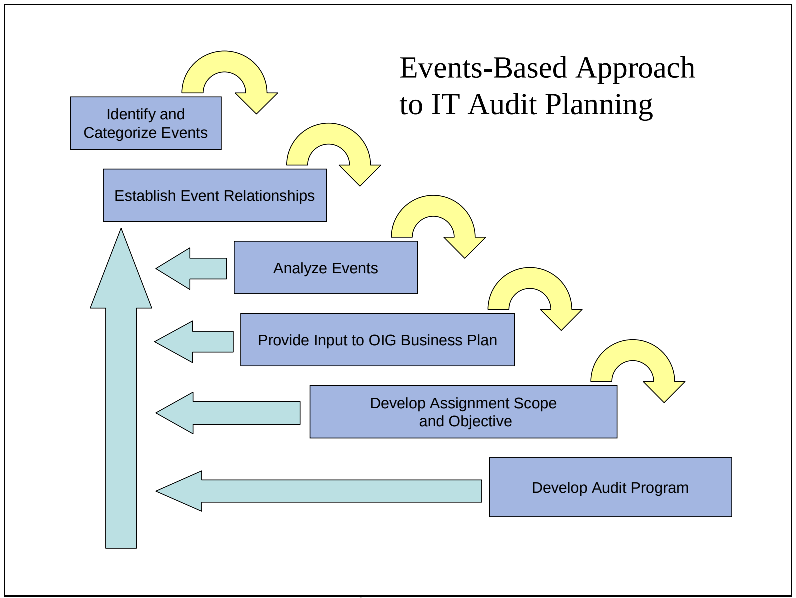
Results of Project

We developed an events-based approach (the Framework) to help plan and prioritize audit coverage of the FDIC's IT program and operations. The Framework is intended to provide increased assurance that IT audit resources are used consistent with, and promote the achievement of, the FDIC's business goals and objectives.

The Framework (see the figure) consists of six phases:

- identifying IT-related events that may warrant audit attention and categorizing these events using defined criteria;
- establishing relationships among IT-related events;
- analyzing IT-related events using various parameters;
- developing, prioritizing, and approving audit proposals as part of the OIG's business planning process;
- leveraging information generated by the Framework and the FDIC's internal control program to scope audits; and
- developing audit programs that leverage COBIT© concepts and the results of the FDIC's internal control assessments.

The Framework


Events-Based Approach to IT Audit Planning
Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Source: OIG analysis of COBIT© and IT-related events.

The Framework links corporate goals and initiatives and IT practices impacted by IT events and will be used to identify areas where IT audit resources can most effectively address IT opportunities and help mitigate risks. The events-based approach to IT audit planning is an iterative process, and potential enhancements may include expanding the framework to other audit areas.

Management Response

We received feedback on a draft of our project results from the FDIC's Chief Information Officer and DIT staff and incorporated those comments as appropriate.

[1] COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

[2] An event affects achievement of objectives and can have a negative impact, a positive impact, or both. Events with negative impact represent risks. Events with positive impact may offset negative impacts or represent opportunities.

To view the full report, go to www.fdicig.gov/2007reports.asp

Information Technology Events Analysis

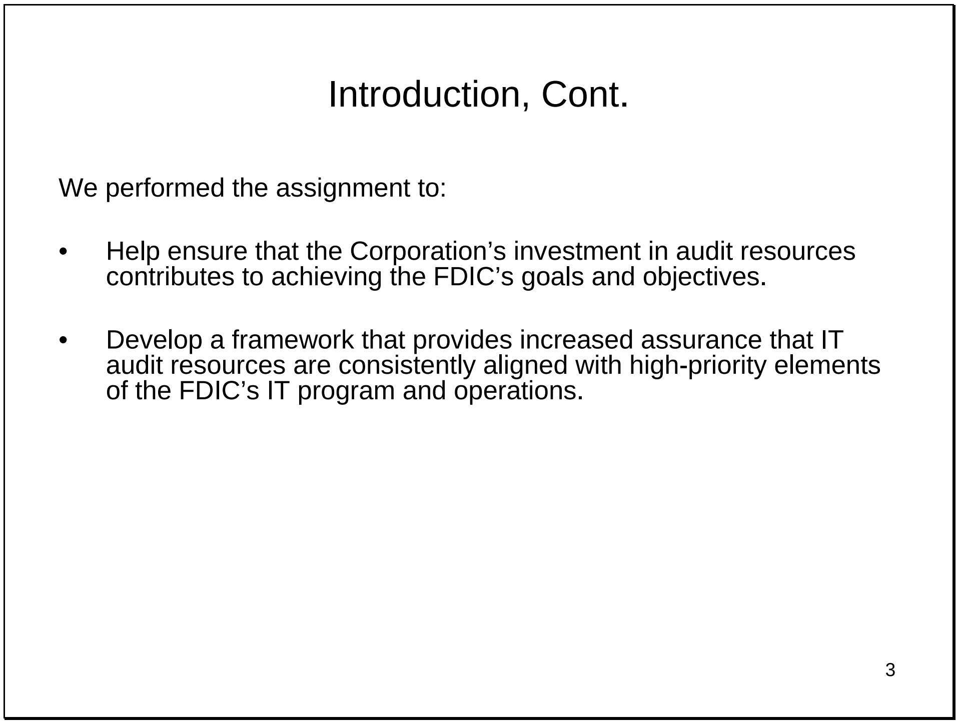
Audit Project 07-001

FDIC Office of Inspector General
Office of Audits
Corporate Management and Security Audits

May 11, 2007

Introduction

- The purpose of the assignment was to develop an events-based approach for planning and prioritizing audit coverage of the FDIC's information technology (IT) program and operations.
- According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), an event is an incident or occurrence, from internal or external sources, that affects achievement of objectives. Events can have negative impact, positive impact, or both. Events with negative impact represent risks. Events with positive impact may offset negative impacts or represent opportunities. The FDIC emphasizes corporate-wide use of guidance provided by COSO.
- We conducted our work from January through April 2007.

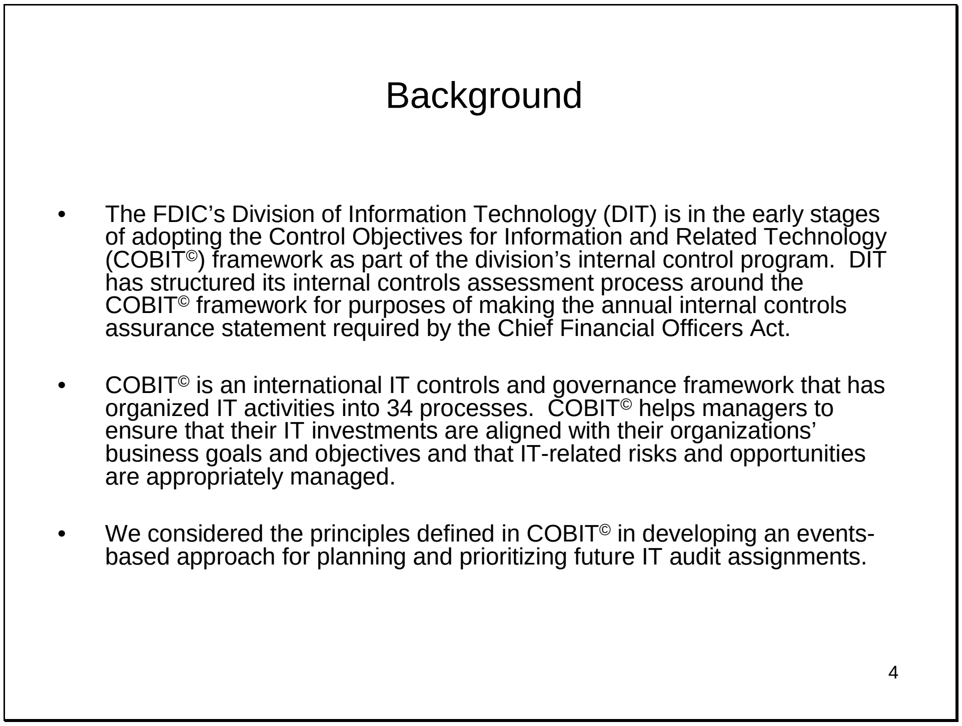


Introduction, Cont.

We performed the assignment to:

- Help ensure that the Corporation's investment in audit resources contributes to achieving the FDIC's goals and objectives.
- Develop a framework that provides increased assurance that IT audit resources are consistently aligned with high-priority elements of the FDIC's IT program and operations.

3

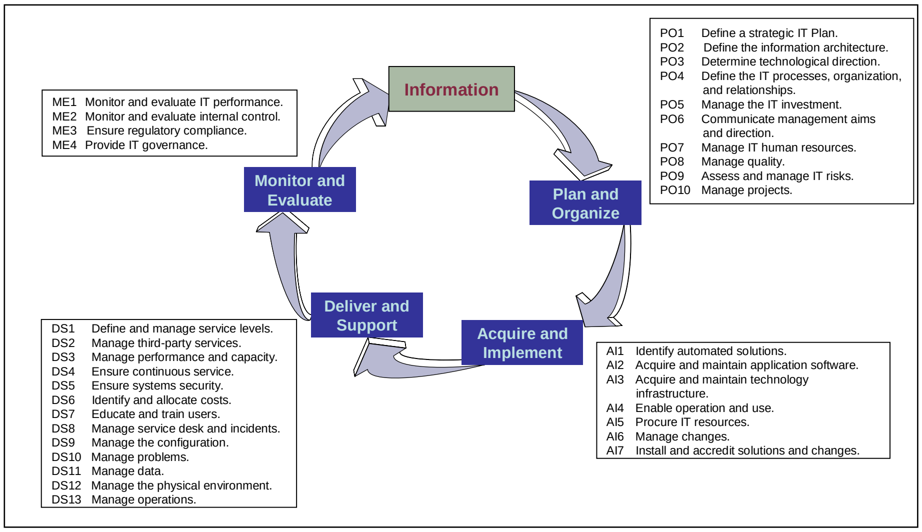


Background

- The FDIC's Division of Information Technology (DIT) is in the early stages of adopting the Control Objectives for Information and Related Technology (COBIT$^{©}$) framework as part of the division's internal control program. DIT has structured its internal controls assessment process around the COBIT$^{©}$ framework for purposes of making the annual internal controls assurance statement required by the Chief Financial Officers Act.
- COBIT$^{©}$ is an international IT controls and governance framework that has organized IT activities into 34 processes. COBIT$^{©}$ helps managers to ensure that their IT investments are aligned with their organizations' business goals and objectives and that IT-related risks and opportunities are appropriately managed.
- We considered the principles defined in COBIT$^{©}$ in developing an events-based approach for planning and prioritizing future IT audit assignments.

4

COBIT© organizes information into 4 domains that collectively contain 34 processes



PO1 Define a strategic IT Plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organization, and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure regulatory compliance.
ME4 Provide IT governance.

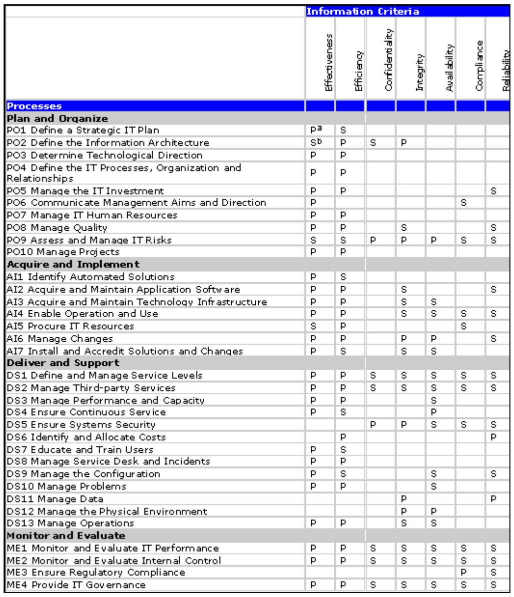
Source: COBIT©.

COBIT© defines Information Criteria for IT governance and control

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. Availability also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance** deals with complying with those laws, regulations, and contractual arrangements to which the business process is subject, i.e., externally-imposed business criteria as well as internal policies.
- **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Source: COBIT©.

COBIT© Links IT Processes to Information Criteria



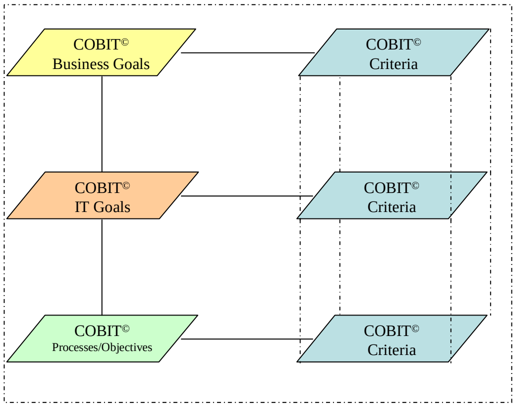
	Information Criteria						
	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Processes							
Plan and Organize							
PO1 Define a Strategic IT Plan	P[a]	S					
PO2 Define the Information Architecture	S[b]	P	S	P			
PO3 Determine Technological Direction	P	P					
PO4 Define the IT Processes, Organization and Relationships	P	P					
PO5 Manage the IT Investment	P	P					S
PO6 Communicate Management Aims and Direction	P					S	
PO7 Manage IT Human Resources	P	P					
PO8 Manage Quality	P	P		S			S
PO9 Assess and Manage IT Risks	S	S	P	P	P	S	S
PO10 Manage Projects	P	P					
Acquire and Implement							
AI1 Identify Automated Solutions	P	S					
AI2 Acquire and Maintain Application Software	P	P		S			S
AI3 Acquire and Maintain Technology Infrastructure	P	P		S	S		
AI4 Enable Operation and Use	P	P		S	S	S	S
AI5 Procure IT Resources	S	P				S	
AI6 Manage Changes	P	P		P	P		S
AI7 Install and Accredit Solutions and Changes	P	S		S	S		
Deliver and Support							
DS1 Define and Manage Service Levels	P	P	S	S	S	S	S
DS2 Manage Third-party Services	P	P	S	S	S	S	S
DS3 Manage Performance and Capacity	P	P			S		
DS4 Ensure Continuous Service	P	S			P		
DS5 Ensure Systems Security			P	P	S	S	S
DS6 Identify and Allocate Costs		P					P
DS7 Educate and Train Users	P	S					
DS8 Manage Service Desk and Incidents	P	P					
DS9 Manage the Configuration	P	S			S		S
DS10 Manage Problems	P	P			S		
DS11 Manage Data				P			P
DS12 Manage the Physical Environment				P	P		
DS13 Manage Operations	P	P		S	S		
Monitor and Evaluate							
ME1 Monitor and Evaluate IT Performance	P	P	S	S	S	S	S
ME2 Monitor and Evaluate Internal Control	P	P	S	S	S	S	S
ME3 Ensure Regulatory Compliance						P	S
ME4 Provide IT Governance	P	P	S	S	S	S	S

Source: COBIT©.

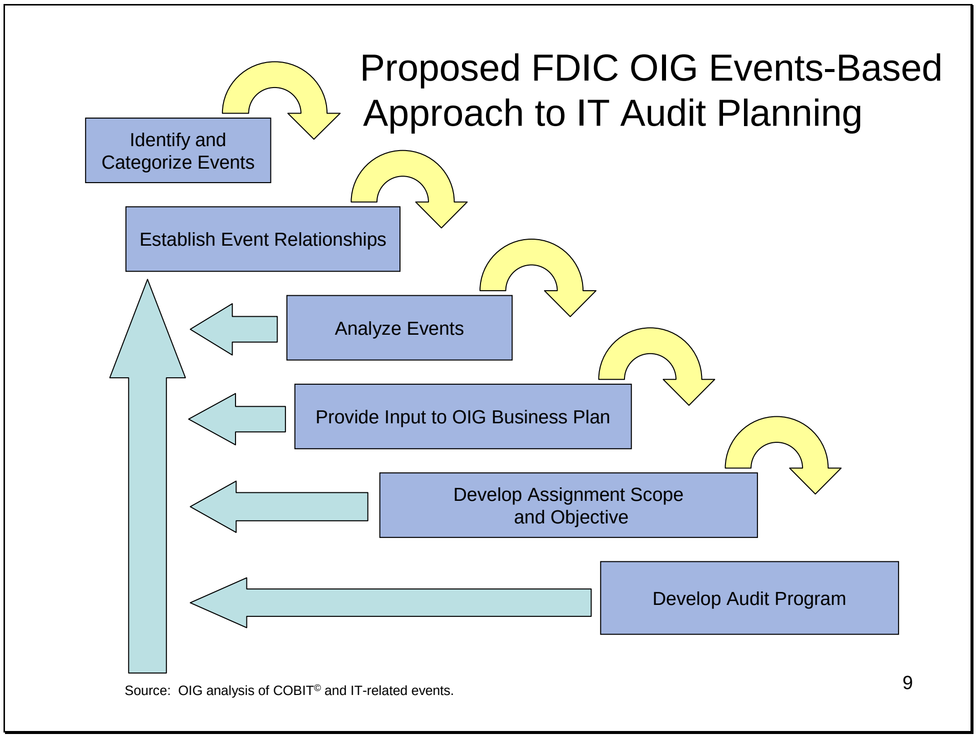
[a] P = a primary process focus.

[b] S = a secondary process focus.

COBIT© IT Governance Framework



Source: Office of Inspector General (OIG) analysis of COBIT©.



Proposed FDIC OIG Events-Based Approach to IT Audit Planning

Identify and Categorize Events

Establish Event Relationships

Analyze Events

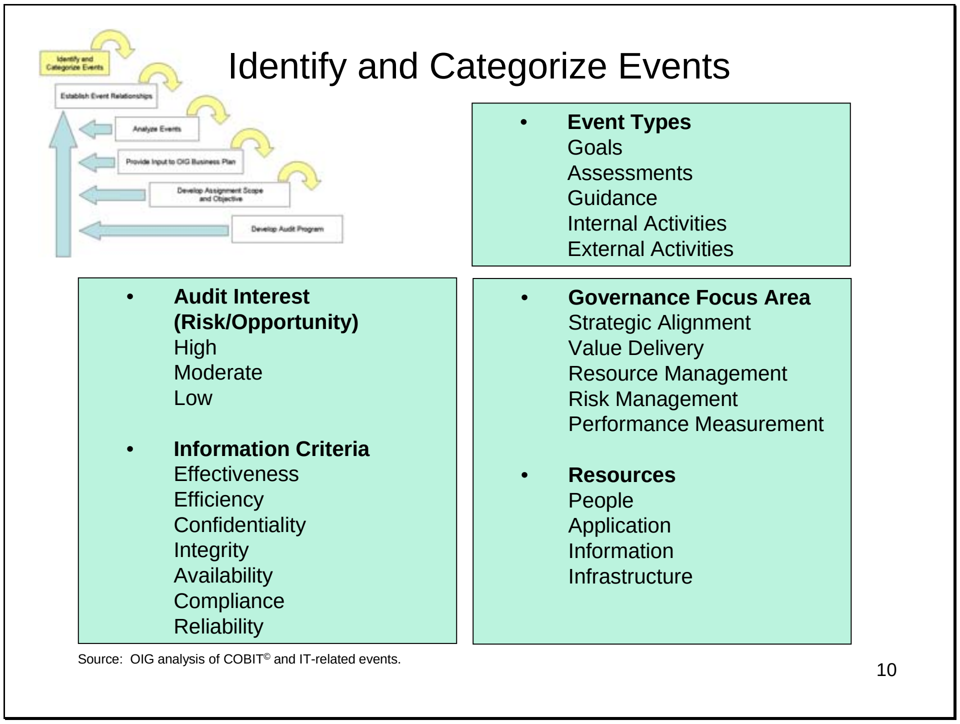
Provide Input to OIG Business Plan

Develop Assignment Scope and Objective

Develop Audit Program

Source: OIG analysis of COBIT© and IT-related events.

9



Identify and Categorize Events

- **Event Types**
  Goals
  Assessments
  Guidance
  Internal Activities
  External Activities

- **Audit Interest (Risk/Opportunity)**
  High
  Moderate
  Low

- **Information Criteria**
  Effectiveness
  Efficiency
  Confidentiality
  Integrity
  Availability
  Compliance
  Reliability

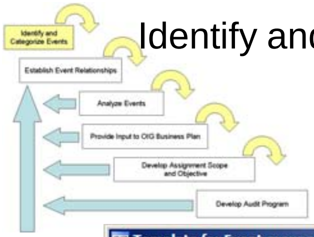
- **Governance Focus Area**
  Strategic Alignment
  Value Delivery
  Resource Management
  Risk Management
  Performance Measurement

- **Resources**
  People
  Application
  Information
  Infrastructure

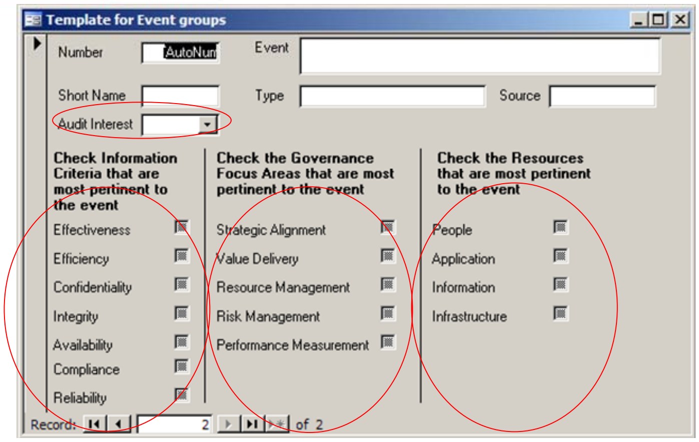
Source: OIG analysis of COBIT© and IT-related events.

10

Identify and Categorize Events, Cont.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Information captured for an IT Event



Template for Event groups

Number AutoNum

Event

Short Name

Type

Source

Audit Interest

Check Information Criteria that are most pertinent to the event

- Effectiveness ☐
- Efficiency ☐
- Confidentiality ☐
- Integrity ☐
- Availability ☐
- Compliance ☐
- Reliability ☐

Check the Governance Focus Areas that are most pertinent to the event

- Strategic Alignment ☐
- Value Delivery ☐
- Resource Management ☐
- Risk Management ☐
- Performance Measurement ☐

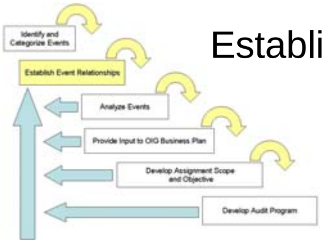
Check the Resources that are most pertinent to the event

- People ☐
- Application ☐
- Information ☐
- Infrastructure ☐

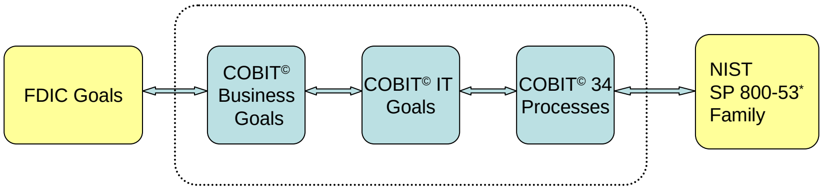
Record: 2 of 2

Source: OIG.

Establish Event Relationships

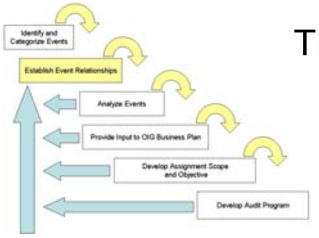

Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Event Types
> Goals
Assessments
> Guidance
Internal Activities
External Activities
COBIT©

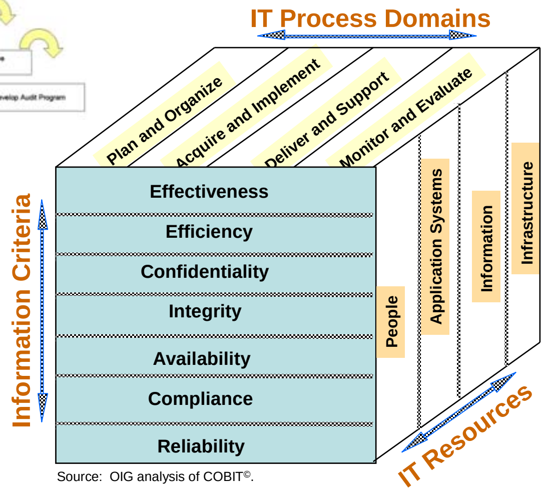


Source: OIG analysis of COBIT© and IT-related events.

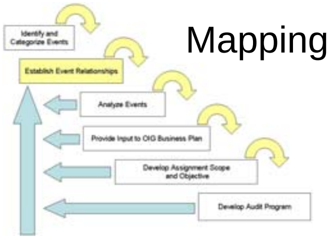
*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, identifies security controls that are organized into classes and families. There are 17 families that contain security controls related to the security function of each family.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

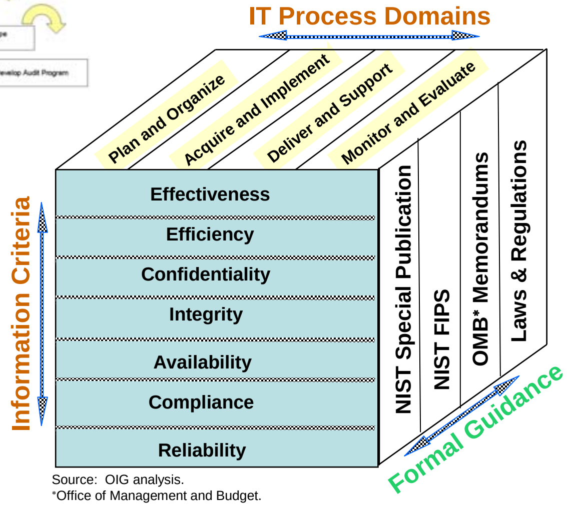
The COBIT© Cube



Source: OIG analysis of COBIT©.

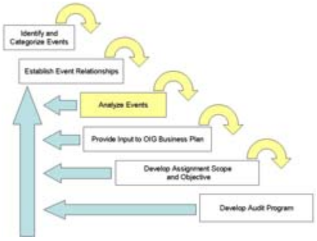

Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Mapping COBIT© and IT Events



Source: OIG analysis.
*Office of Management and Budget.

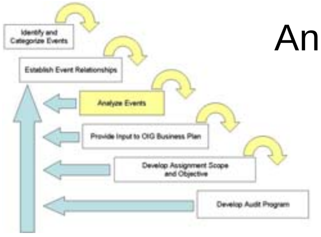
Analyze Events


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Analyze events using various parameters such as common audit interest or event characteristics.

The following information illustrates how a set of IT events can be grouped using "Availability" as a common information criterion. This set of events then can be analyzed for consideration during the OIG's business planning.

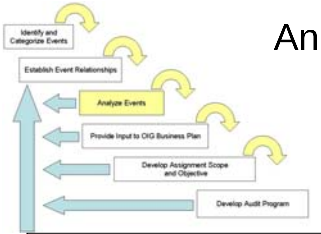
Analyze Events, Cont.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

COBIT© processes involving Availability can be identified.

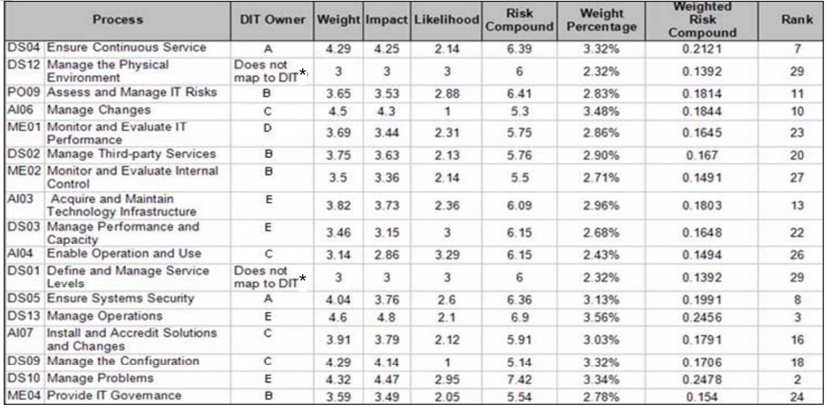
Process ID	Process Name	Availability	People	Information	Application	Infrastructure
DS01	Define and Manage Service Levels	Secondary	☑	☑	☑	☑
ME01	Monitor and Evaluate IT Performance	Secondary	☑	☑	☑	☑
DS02	Manage Third-party Services	Secondary	☑	☑	☑	☑
ME02	Monitor and Evaluate Internal Control	Secondary	☑	☑	☑	☑
AI03	Acquire and Maintain Technology Infrastructure	Secondary	□	□	□	☑
DS03	Manage Performance and Capacity	Secondary	□	□	☑	☑
AI04	Enable Operation and Use	Secondary	☑	□	☑	☑
DS04	Ensure Continuous Service	Primary	☑	☑	☑	☑
ME04	Provide IT Governance	Secondary	☑	☑	☑	☑
DS05	Ensure Systems Security	Secondary	☑	☑	☑	☑
AI06	Manage Changes	Primary	☑	☑	☑	☑
AI07	Install and Accredit Solutions and Changes	Secondary	☑	☑	☑	☑
PO09	Assess and Manage IT Risks	Primary	☑	☑	☑	☑
DS09	Manage the Configuration	Secondary	□	☑	☑	☑
DS10	Manage Problems	Secondary	☑	☑	☑	☑
DS12	Manage the Physical Environment	Primary	□	□	☑	☑
DS13	Manage Operations	Secondary	☑	☑	☑	☑

Source: COBIT©.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Analyze Events, Cont.

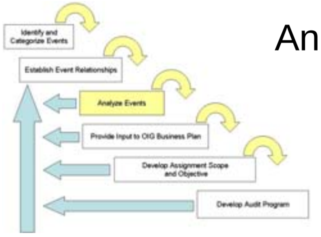
DIT's annual risk analysis of COBIT© processes involving Availability can be identified.



Process		DIT Owner	Weight	Impact	Likelihood	Risk Compound	Weight Percentage	Weighted Risk Compound	Rank
DS04	Ensure Continuous Service	A	4.29	4.25	2.14	6.39	3.32%	0.2121	7
DS12	Manage the Physical Environment	Does not map to DIT*	3	3	3	6	2.32%	0.1392	29
PO09	Assess and Manage IT Risks	B	3.65	3.53	2.88	6.41	2.83%	0.1814	11
AI06	Manage Changes	C	4.5	4.3	1	5.3	3.48%	0.1844	10
ME01	Monitor and Evaluate IT Performance	D	3.69	3.44	2.31	5.75	2.86%	0.1645	23
DS02	Manage Third-party Services	B	3.75	3.63	2.13	5.76	2.90%	0.167	20
ME02	Monitor and Evaluate Internal Control	B	3.5	3.36	2.14	5.5	2.71%	0.1491	27
AI03	Acquire and Maintain Technology Infrastructure	E	3.82	3.73	2.36	6.09	2.96%	0.1803	13
DS03	Manage Performance and Capacity	E	3.46	3.15	3	6.15	2.68%	0.1648	22
AI04	Enable Operation and Use	C	3.14	2.86	3.29	6.15	2.43%	0.1494	26
DS01	Define and Manage Service Levels	Does not map to DIT*	3	3	3	6	2.32%	0.1392	29
DS05	Ensure Systems Security	A	4.04	3.76	2.6	6.36	3.13%	0.1991	8
DS13	Manage Operations	E	4.6	4.8	2.1	6.9	3.56%	0.2456	3
AI07	Install and Accredit Solutions and Changes	C	3.91	3.79	2.12	5.91	3.03%	0.1791	16
DS09	Manage the Configuration	C	4.29	4.14	1	5.14	3.32%	0.1706	18
DS10	Manage Problems	E	4.32	4.47	2.95	7.42	3.34%	0.2478	2
ME04	Provide IT Governance	B	3.59	3.49	2.05	5.54	2.78%	0.154	24

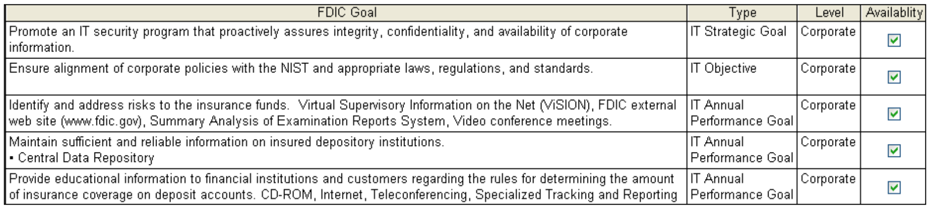
Source: DIT.

* DIT has not identified ownership of these processes.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

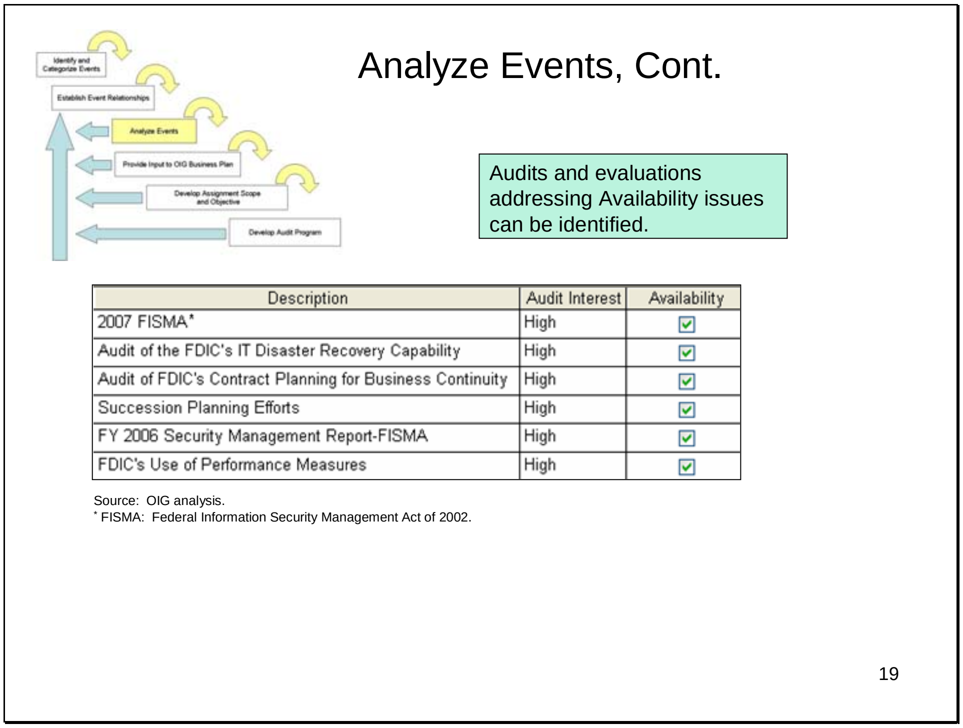
Analyze Events, Cont.

FDIC Goals relating to Availability can be identified.



FDIC Goal	Type	Level	Availablity
Promote an IT security program that proactively assures integrity, confidentiality, and availability of corporate information.	IT Strategic Goal	Corporate	☑
Ensure alignment of corporate policies with the NIST and appropriate laws, regulations, and standards.	IT Objective	Corporate	☑
Identify and address risks to the insurance funds. Virtual Supervisory Information on the Net (ViSION), FDIC external web site (www.fdic.gov), Summary Analysis of Examination Reports System, Video conference meetings.	IT Annual Performance Goal	Corporate	☑
Maintain sufficient and reliable information on insured depository institutions. • Central Data Repository	IT Annual Performance Goal	Corporate	☑
Provide educational information to financial institutions and customers regarding the rules for determining the amount of insurance coverage on deposit accounts. CD-ROM, Internet, Teleconferencing, Specialized Tracking and Reporting	IT Annual Performance Goal	Corporate	☑

Source: OIG analysis.



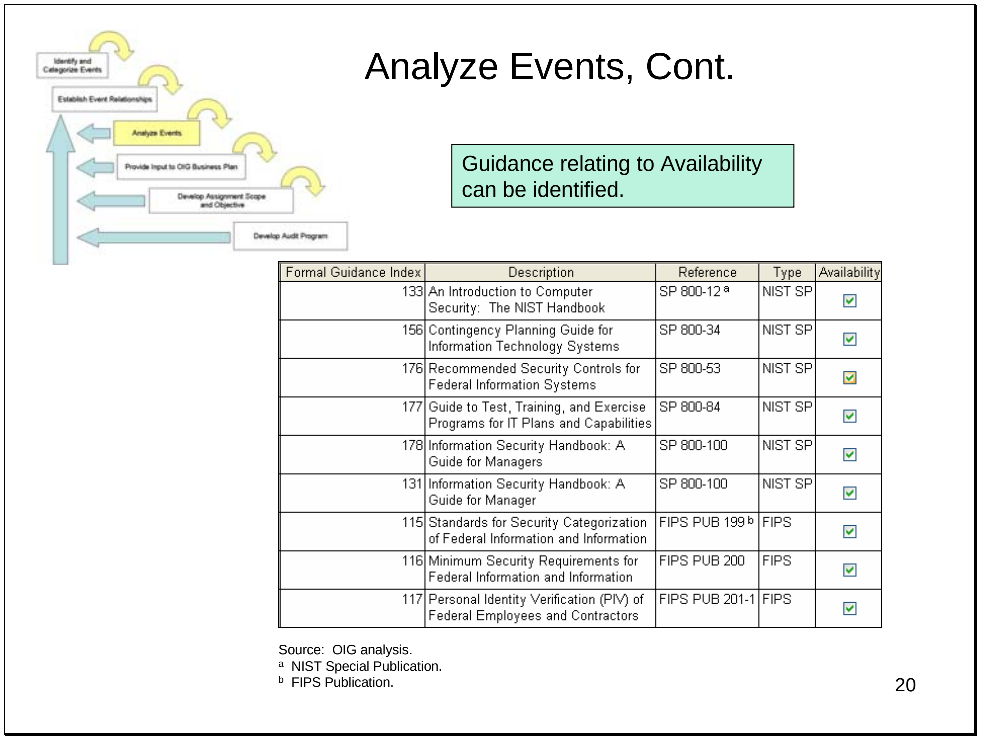
Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Analyze Events, Cont.

Audits and evaluations addressing Availability issues can be identified.

Description	Audit Interest	Availability
2007 FISMA*	High	☑
Audit of the FDIC's IT Disaster Recovery Capability	High	☑
Audit of FDIC's Contract Planning for Business Continuity	High	☑
Succession Planning Efforts	High	☑
FY 2006 Security Management Report-FISMA	High	☑
FDIC's Use of Performance Measures	High	☑

Source: OIG analysis.
* FISMA: Federal Information Security Management Act of 2002.



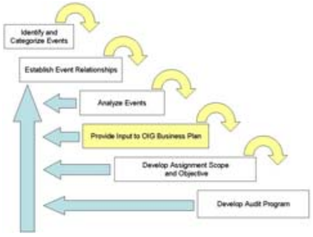
Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Analyze Events, Cont.

Guidance relating to Availability can be identified.

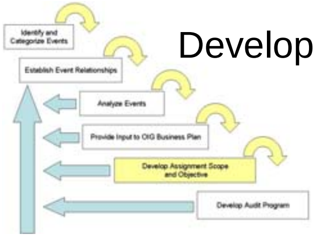
Formal Guidance Index	Description	Reference	Type	Availability
133	An Introduction to Computer Security: The NIST Handbook	SP 800-12 [a]	NIST SP	☑
156	Contingency Planning Guide for Information Technology Systems	SP 800-34	NIST SP	☑
176	Recommended Security Controls for Federal Information Systems	SP 800-53	NIST SP	☑
177	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	SP 800-84	NIST SP	☑
178	Information Security Handbook: A Guide for Managers	SP 800-100	NIST SP	☑
131	Information Security Handbook: A Guide for Manager	SP 800-100	NIST SP	☑
115	Standards for Security Categorization of Federal Information and Information	FIPS PUB 199 [b]	FIPS	☑
116	Minimum Security Requirements for Federal Information and Information	FIPS PUB 200	FIPS	☑
117	Personal Identity Verification (PIV) of Federal Employees and Contractors	FIPS PUB 201-1	FIPS	☑

Source: OIG analysis.
[a] NIST Special Publication.
[b] FIPS Publication.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

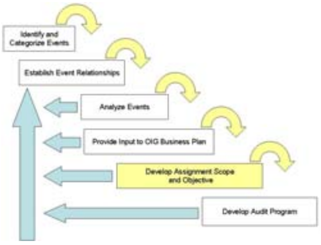
Provide Input to OIG Business Plan

- Develop audit assignment proposals based on the results of events analysis.
- Discuss audit assignment proposals and their priority with OIG and FDIC management.
- Prepare background information, resource requirements, and preliminary objective and milestones for approved assignments.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Develop Assignment Scope and Objective

- Relationships in the framework can be leveraged in developing audit assignment scope and objective(s).
- Survey internal controls using the results of DIT's annual COBIT© questionnaire that identifies IT process risks, maturities, activities, resources, and IT governance areas.


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Develop Assignment Scope and Objective, Cont.

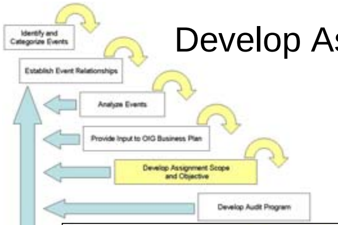
Using IT Disaster Recovery as an example audit assignment:

- Develop assignment scope considering a review of applicable COBIT© process documentation when developed by DIT.
  - COBIT© Management Guidelines
    - related process inputs and outputs
    - activities and functions (RACI chart*)
    - goals and metrics

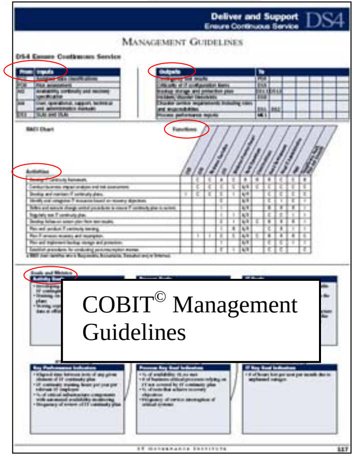
- Develop assignment objectives considering COBIT© high-level and detailed control objectives corresponding to the scope established.

*The RACI Chart defines who should be responsible (R), accountable (A), consulted (C), and informed (I) for specific control activities. The RACI model is a tool that can be used for identifying roles and responsibilities during an organizational change process.

23


Identify and Categorize Events
Establish Event Relationships
Analyze Events
Provide Input to OIG Business Plan
Develop Assignment Scope and Objective
Develop Audit Program

Develop Assignment Scope and Objective, Cont.


DS4 Deliver and Support
Ensure Continuous Service

MANAGEMENT GUIDELINES

DS4 Ensure Continuous Service

From | Inputs

Outputs | To

RACI Chart

Functions

Activities

Goals and Metrics

Key Performance Indicators

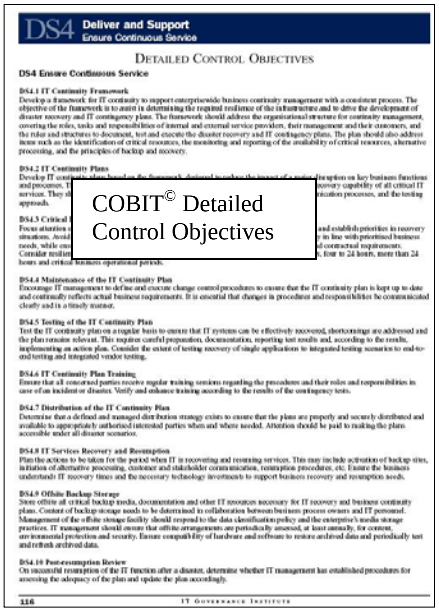
Process Key Goal Indicators

IT Key Goal Indicators

IT GOVERNANCE INSTITUTE 117

COBIT© Management Guidelines

Source: COBIT©.


DS4 Deliver and Support
Ensure Continuous Service

DETAILED CONTROL OBJECTIVES

DS4 Ensure Continuous Service

DS4.1 IT Continuity Framework
Develop a framework for IT continuity to support enterprisewide business continuity management with a consistent process. The objective of the framework is to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

DS4.2 IT Continuity Plans
Develop IT continuity plans based on the framework, designed to reduce the impact of a major disruption on key business functions and processes. T… recovery capability of all critical IT services. They sh… nication processes, and the testing approach.

DS4.3 Critical I…
Focus attention o… and establish priorities in recovery situations. Avoid… y in line with prioritised business needs, while ens… d contractual requirements. Consider resilien… , four to 24 hours, more than 24 hours and critical business operational periods.

DS4.4 Maintenance of the IT Continuity Plan
Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. It is essential that changes in procedures and responsibilities be communicated clearly and in a timely manner.

DS4.5 Testing of the IT Continuity Plan
Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

DS4.6 IT Continuity Plan Training
Ensure that all concerned parties receive regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.

DS4.7 Distribution of the IT Continuity Plan
Determine that a defined and managed distribution strategy exists to ensure that the plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

DS4.8 IT Services Recovery and Resumption
Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, resumption procedures, etc. Ensure the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.

DS4.9 Offsite Backup Storage
Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Content of backup storage needs to be determined in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data and periodically test and refresh archived data.

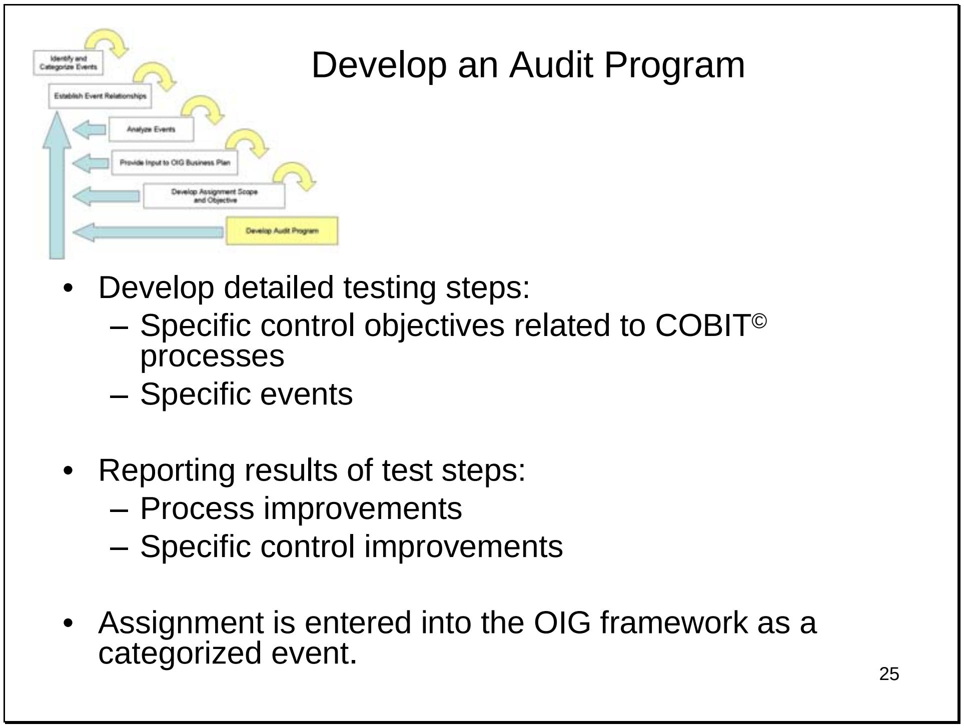
DS4.10 Post-resumption Review
On successful resumption of the IT function after a disaster, determine whether IT management has established procedures for assessing the adequacy of the plan and update the plan accordingly.

116 IT GOVERNANCE INSTITUTE

COBIT© Detailed Control Objectives

Source: COBIT©.

24



Identify and Categorize Events

Establish Event Relationships

Analyze Events

Provide Input to OIG Business Plan

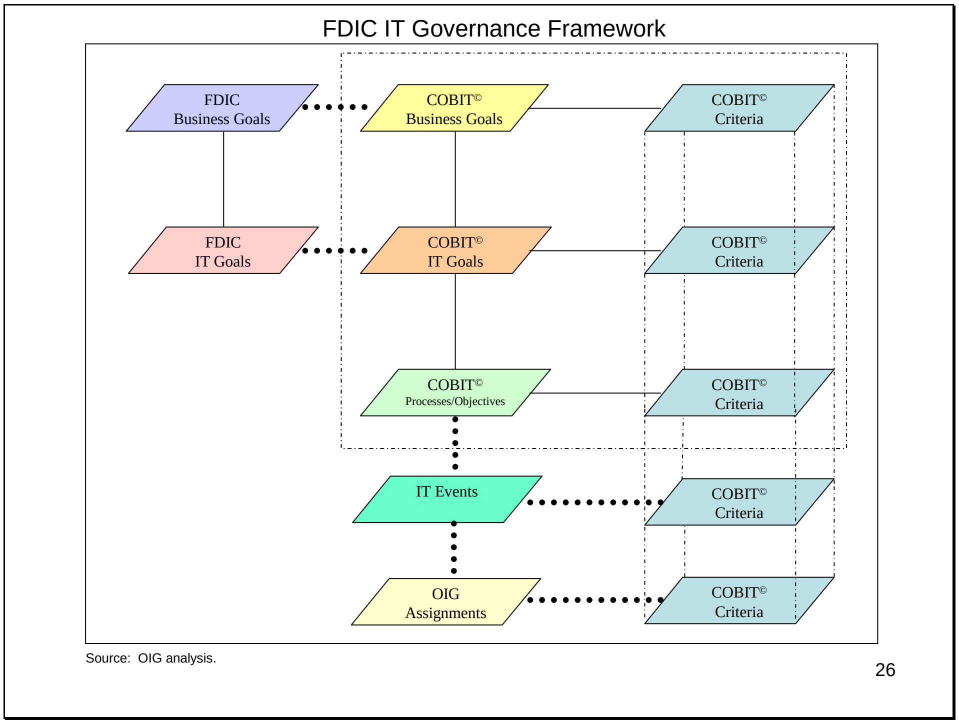
Develop Assignment Scope and Objective

Develop Audit Program

Develop an Audit Program

- Develop detailed testing steps:
  - Specific control objectives related to COBIT© processes
  - Specific events
- Reporting results of test steps:
  - Process improvements
  - Specific control improvements
- Assignment is entered into the OIG framework as a categorized event.

25



FDIC IT Governance Framework

FDIC Business Goals

COBIT© Business Goals

COBIT© Criteria

FDIC IT Goals

COBIT© IT Goals

COBIT© Criteria

COBIT© Processes/Objectives

COBIT© Criteria

IT Events

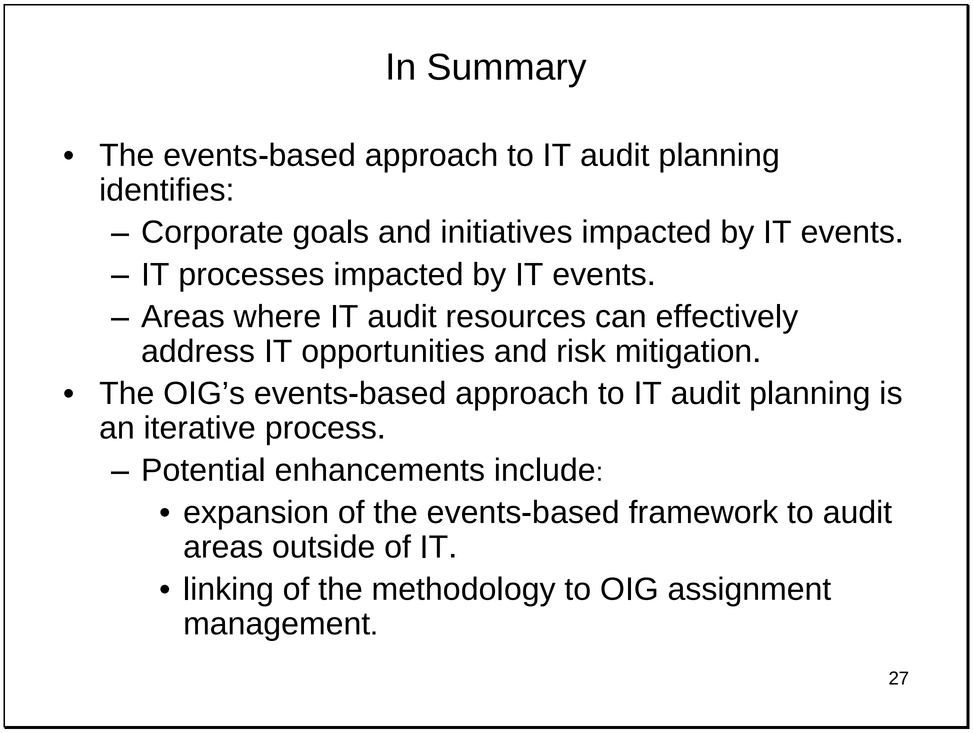
COBIT© Criteria

OIG Assignments

COBIT© Criteria

Source: OIG analysis.

26



In Summary

- The events-based approach to IT audit planning identifies:
  - Corporate goals and initiatives impacted by IT events.
  - IT processes impacted by IT events.
  - Areas where IT audit resources can effectively address IT opportunities and risk mitigation.
- The OIG’s events-based approach to IT audit planning is an iterative process.
  - Potential enhancements include:
    - expansion of the events-based framework to audit areas outside of IT.
    - linking of the methodology to OIG assignment management.