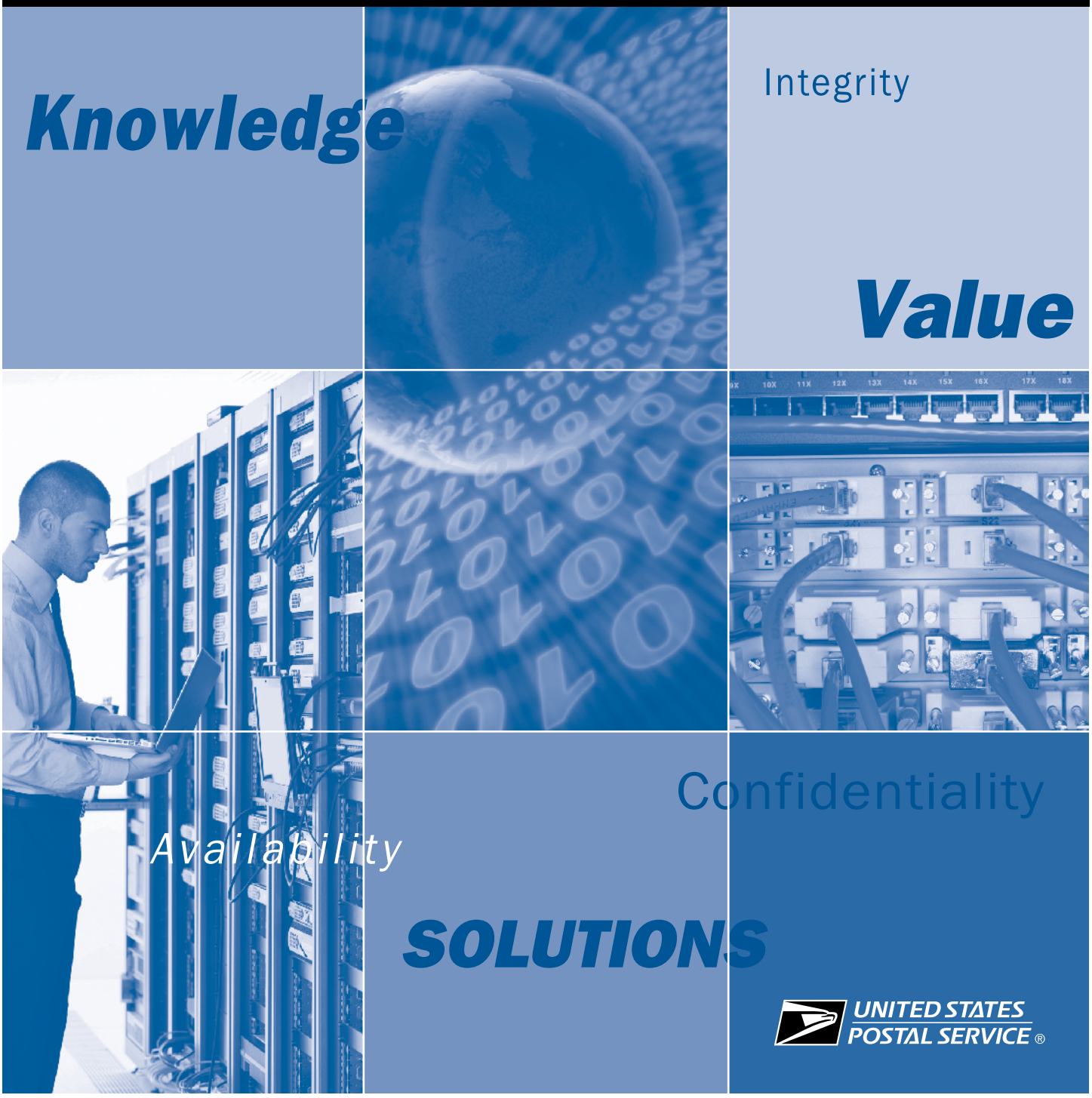
Certification and Accreditation

The Postal Service Process For
Protecting Its Information Resources



Certification and Accreditation (C&A) Requirements for Information Resources

Phase	C&A Deliverable	New and Major Information Resource Modifications[1]				Recertifications[2]		Service-Based Contracts (SBCs)	
		Nonsensitive and Noncritical		All Other Information Resources					
		Deliverables	Responsible	Deliverables	Responsible	Deliverables	Responsible	Deliverables	Responsible
1	Review Technical Solutions Life Cycle (TSLC) Documentation	Prepare Business Needs Statement (BNS) (if missing).	Project Mgr	Prepare BNS (if missing).	Project Mgr			Prepare BNS (if missing).	Project Mgr
2	Business Impact Assessment (BIA)	Yes	Project Mgr	Yes	Project Mgr	Yes	Project Mgr	Yes	Project Mgr
3	Arch Diagram	Yes	Project Mgr	Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
3	Security Specs	Yes	Project Mgr	Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
3	Security Plan	Yes[3]		Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
3	Risk Assessment	Yes	Project Mgr	Yes	Project Mgr	Yes	Project Mgr	Yes	Project Mgr
3	Site Security Review			Based on Policy Requirements	Information Systems Security Officer (ISSO) & U.S. Postal Inspection Service (USPIS)	If applicable	ISSO & USPIS	Based on Policy Requirements	ISSO & USPIS
4-5	Contingency Plans			Based on Policy Requirements	Project Mgr	If applicable	Project Mgr	Based on Policy Requirements	Project Mgr
4	Network Connectivity Review Board (NCRB) Request	Yes	Project Mgr	Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
5	Security Test and Evaluation (ST&E) Plan	Yes[3]		Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
6	Security Code Review	Based on Requirements	Project Mgr	Based on Policy Requirements	Project Mgr	If applicable	Project Mgr	Based on Policy Requirements	Project Mgr
6	ST&E Testing & Report			Yes	Project Mgr	If applicable	Project Mgr	Yes	Project Mgr
6	Vulnerability Scan	Yes	Mgr CISO	Yes	Mgr CISO	Yes	Mgr CISO	Yes for Sensitive	Mgr CISO
6	Independent Reviews			If applicable	Project Mgr	If applicable	Project Mgr	If applicable	Project Mgr
6	Outstanding Items			If applicable	Project Mgr	If applicable	Project Mgr	If applicable	Project Mgr
6	Evaluation Report	YES	ISSO	Yes	ISSO	Yes	ISSO		
6	Certification Letter	YES	C & A Program Mgr	Yes	C & A Program Mgr	Yes	C & A Program Mgr		
6	Risk Mitigation Plan	Yes for High/ Mod Risk	Project Mgr	Yes for High/ Moderate Risk	Project Mgr	Yes for High/ Mod Risk	Project Mgr	Yes for High/ Mod Risk	ISSO
6	Accreditation Letter	YES	Mgr CISO	Yes	Mgr CISO	Yes	Mgr CISO		
7	Contingency Test Results			Yes	Portfolio Mgr & Executive Sponsor	Yes	Portfolio Mgr & Executive Sponsor	Yes	Portfolio Mgr & Executive Sponsor
7	Revised C&A Documents	As needed or every 5 years	ISSO & Project Mgr	As needed or every 3 years; yearly for payment card industry (PCI)	ISSO & Project Mgr	As needed or every 3 years; yearly for PCI	ISSO & Project Mgr	As needed or every 3 years	ISSO & Project Mgr

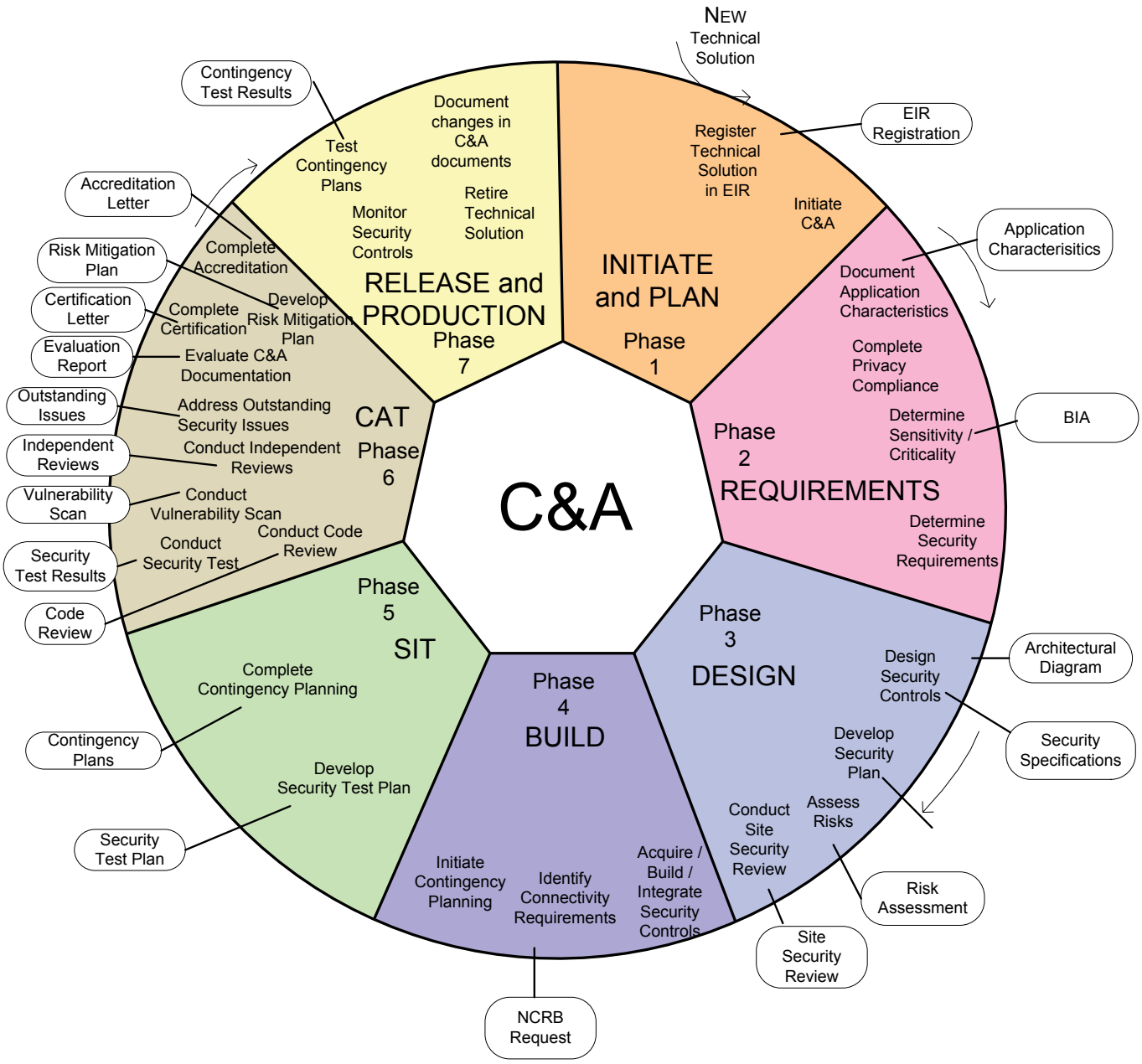
Footnotes

1 If part of an application includes an SBC, then the contract must be reviewed to ensure it contains clauses 1-1 and 4-19.

2 If either the BIA and/or Risk Assessment find that major changes have occurred, then follow the New and Major Information Resource Modification process.

3 If externally facing.

C&A Phases and Major Deliverables



The C&A process consists of seven interrelated phases that are conducted concurrently with the development and deployment of new information resources (technical solutions) and the recertification of existing information resources. Each phase in the C&A process corresponds to a phase in the Technical Solutions Life Cycle (TSLC).

The objectives of the C&A process are to assess threats and vulnerabilities, define security requirements, identify and implement security controls and processes, test security solutions, evaluate the effectiveness of security controls and processes chosen to protect the information resource, and obtain approval for deployment or continuing use.

Certification and Accreditation Phases

Phase 1, Initiate and Plan

In this phase:

- Register or update the proposed technical solution in Enterprise Information Repository.
- Initiate the C&A process.

Phase 2, Requirements

In this phase, conduct a Business Impact Assessment (BIA) to collect privacy-related information, to ensure compliance with privacy laws and regulations, to define sensitivity and criticality of the technical solution, and to determine information security requirements required to protect the technical solution.

Phase 3, Design

In this phase:

- Develop and document in an architecture diagram, the design for the technical solution.
- Define security specifications for contracts and acquisitions to protect the technical solution commensurate with its business value (if required).
- Identify information security controls and processes to satisfy the security requirements defined in the BIA and documented in a security plan.
- Conduct a risk assessment.
- Request a site security review (if required).

Phase 4, Build

In this phase:

- Build or acquire information security controls and processes and integrate the information resource.
- Define connectivity requirements.
- Submit a request to the Network Connectivity Review Board (if required).
- Initiate contingency planning (if required) to address unexpected interruptions to business activities supported by this information resource.

Phase 5, Security Integration Testing

In this phase:

- Develop a security test plan.
- Complete contingency plans.

Phase 6, Customer Acceptance Testing

In this phase:

- Conduct a security code review (if required).
- Conduct security testing to ensure the security controls and processes implemented in the build phase are effective.
- Document the results of the test in a report.

- Conduct independent reviews for security code reviews, risk assessments, vulnerability scans, penetration testing, or security test validation (if required).
- Address outstanding issues.
- The ISSR or project manager completes the C&A deliverables and submits them to the ISSO.
- The ISSO evaluates the C&A deliverables and prepares an evaluation report highlighting the risks associated with placing the information resource in production, escalates security concerns or forwards the C&A evaluation report and supporting documentation to the certifier for review.
- The certifier reviews the C&A evaluation report and the supporting C&A documentation, escalates security concerns or prepares and signs a certification letter, and forwards the certification letter and C&A documentation to the accreditor.
- The project manager, executive sponsor, and ISSO prepare a risk mitigation plan for any residual risks rated as medium or high, recommending how the risk will be mitigated, the organization or individual responsible, and the time for resolution.
- The accreditor reviews the risk mitigation plan and the supporting C&A documentation, escalates security concerns or prepares and signs an accreditation letter, and forwards the accreditation letter and final C&A documentation package to the vice president functional business area (or executive sponsor if this responsibility is delegated) and vice president IT (or portfolio manager if this responsibility is delegated).

Phase 7, Release and Production

In this phase:

- The vice president functional business area (or executive sponsor if this responsibility is delegated) and vice president IT (or portfolio manager if this responsibility is delegated) review the accreditation letter and risk mitigation plan. They make a joint decision on whether to accept the residual risk and approve the information resource for deployment (with or without restrictions).
- Test contingency plans.
- Maintain security controls and processes in accordance with the security plan.
- Monitor security controls and review system and application logs.
- Update C&A documentation.
- Re-initiate the C&A.
- Retire the information resource.
- Dispose of the data.
- Sanitize the equipment and media (if required).

C&A Stakeholder Responsibilities

VP Functional Business Area

- Ensures resources are available for completing information security tasks throughout an information resource life cycle.
- Works jointly with the vice president IT (or the portfolio manager if this responsibility is delegated) to review accreditation letter and risk mitigation plan and, if acceptable, accept residual risk and approve deployment of the information resource. The vice presidents of functional business areas may delegate this responsibility to the applicable executive sponsor. If this responsibility is delegated, notice to that effect must be in writing.

Executive Sponsor

- Ensures completion of all security tasks throughout an information resource life cycle.
- (If the vice president functional business area delegated this responsibility) works jointly with the vice president IT (or the portfolio manager if this responsibility is delegated) to review accreditation letter and risk mitigation plan and, if acceptable, accept residual risk and approve deployment of the information resource.

VP IT

- Works jointly with the vice president functional business area (or the executive sponsor if this responsibility is delegated) to review accreditation letter and risk mitigation plan and, if acceptable, accept residual risks and approve deployment of the information resource. The vice president of IT may delegate this responsibility to the applicable portfolio manager. If this responsibility is delegated, notice to that effect must be in writing.

Portfolio Manager

- Serves as a liaison between the executive sponsor and IT providers.
- (If the vice president IT delegated this responsibility) works jointly with the vice president functional business area (or the executive sponsor if this responsibility is delegated) to review accreditation letter and risk mitigation plan and, if acceptable, accept residual risks and approve deployment of the information resource.

Information Systems Security Representative or Project Manager

- Ensures security controls are implemented.
- Notifies the executive sponsor, portfolio manager and ISSO of any risks that emerge during development or acquisition of the application.
- Works with the ISSO to prepare C&A documents.

Information Systems Security Officer

- Provides security guidance and expertise throughout the C&A process.
- Reviews the security testing and evaluates C&A documents.
- Prepares the C&A evaluation report and submits it to a certifier.

Certifier (Program Manager, C&A Process)

- Reviews the C&A evaluation report and supporting documents.
- If acceptable, prepares a certification letter and recommends accreditation.

Accreditor (Manager, CISO)

- Reviews the certification letter, risk mitigation plan, and C&A documents.
- If acceptable, prepares accreditation letter and recommends deployment.

For more information and help

Information security policies and processes
Go to the PolicyNet website at: *http://blue.usps.gov/cpim/hbkid.htm.*

C&A deliverable templates
TSLC Waterfall templates:
http://itwebshare.usps.gov/sites/itweb/SitePages/TSLC%20Waterfall%20Templates.aspx

TSLC Agile templates:
http://itwebshare.usps.gov/sites/itweb/SitePages/TSLC%20Agile%20Templates.aspx

Corporate Information Security Office

Headquarters Location.....202-268-5713

Raleigh Location.....919-501-9245

Information Security Hotline.....919-501-9350

E-mail comments to: *information_security@usps.gov.*

Pub 805-A
PSN 7610-07-000-8289
January 2013