Navigating the FISMA Compliance Labyrinth

James D. Biggs, *JD Biggs & Associates, Inc.*
james@jdbiggs.com

Agu Ets, *Project Performance Corporation*

aets@PPC.com

www.jdbiggs.com

FEDERAL COMPUTER SECURITY REPORT CARD
FISMA - December 31, 2005

GOVERNMENTWIDE GRADE 2005: 🟡🟢

Treasury	🟡	State	🟡
Agency for International Develop	🟡	Defense	🟡
Transportation	🟡	SBA	🟢
Nuclear Regulatory Commission	🟡	NASA	🟢
SSA	🟡	Commerce	🟡
EPA	🟢	Veterans Affairs	🔴
Labor	🟢	Agriculture	🟡
Justice	🟡	HHS	🟡
GSA	🟡	Energy	🟡
National Science Foundation	🟢	HUD	🟢
Education	🟡	Homeland Security	🔴
OPM	🟡	Interior	🔴

PROJECT performance CORPORATION

Challenges in Navigating the FISMA Compliance Labyrinth

- Understanding compliance requirements
- Ensuring policies in place and enforced
- Defining security requirements
- Managing effective risk assessments
- Performing certification and accreditation
- Interfacing with other processes
- Implementing automation to support compliance

How To Address These Challenges?

Government Directives

Driving Legislation

- E-Government Act of 2002 - Public Law 107-347
  - "To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget."
- Title III - Federal Information Security Management Act
  - "Provide for development and maintenance of minimum controls required to protect Federal information and information systems."
  - Establish Agency Security Program
  - Establish annual reporting and assessment procedures
- Section 208 – Privacy Provisions
  - Ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.
  - Conduct Privacy Impact Assessment

Government Directives

Driving Legislation

- Office of Management and Budget (OMB) Circular A-130
- Appendix III - Security of Federal Automated Information Resources
- Supporting Memorandums
  - OMB Memorandum 03-19
  - OMB Memorandum 04-25
  - OMB Memorandum 05-15

Federal Information Security Management Act (FISMA) Methodology

Version 4.1 - October 2005

Organizational Requirements (3544)

- Provide protection commensurate with risk and magnitude of potential harm.
- Provide security that supports operations and assets.
- Delegate authority to CIO for FISMA compliance.
- Ensure sufficient trained personnel to support security requirements
- Ensure CIO reports annually on effectiveness of information security program.

Agency Program (3544 (b))

Develop, document and implement a security program to provide security for the information assets that support the operation of the agency.

Security Policies and Procedures

- Based on risk assessment results
- Cost effective controls designed to reducing in-place & planned risk
- Addressed throughout IT life-cycle
- Compliant with
  - FISMA Sec. 3544
  - NIST special publications
  - Acceptable system configurations
  - Other applicable requirements

Guidance Documents

- FIPS 199, 200, 201
- NIST SP 800-37
- NIST SP 800-14
- NIST SP 800-27
- NIST SP 800-41
- NIST SP 800-45
- NIST SP 800-48
- NIST SP 800-53
- NIST SP 800-59 & 60

Establish IT Environment

- Classify IT systems
- Define security policy
- Define baseline common & system specific security requirements
- Define baseline common & system specific security controls
- Define security life cycle
- Define interconnection agreements

Documents Produced

- System Descriptions Environment
- System Security Policy
- Interconnection Security Agreements
- Memorandums of Agreement
- Privacy Impact Assessment
- Configuration Management Plan
- System Development Plan
- Sensitive Data Encryption Policy & Plan
- Security Patch Policy
- Wireless Device Policy
- Email Use Policy

Subordinate Systems Plans

- Networks
- Facilities
- IT systems
- Groups of IT systems

Guidance Documents

- NIST SP 800-37
- NIST SP 800-18
- NIST SP 800-27
- NIST SP 800-33
- NIST SP 800-35
- NIST SP 800-36
- NIST SP 800-41
- NIST SP 800-44
- NIST SP 800-47

Create Security Plan

- Identify security plan policy
- Perform analysis with system owner
- Determine management controls
- Determine operational controls
- Determine technical controls
- Assemble system security plan
- Complete a Privacy Impact Assessment
- E-Authentication and risk assessment

Documents Produced

- System Descriptions Environment
- Boundary Definition
- System Security Requirements
- System Security Operating Procedures
- System Rules of Behavior
- System Security Plan

Continuity of Operations Plan

- Plans and procedures in place
- Mission critical systems
- Support required operations
- Protect assets

Guidance Documents

- NIST SP 800-37
- NIST SP 800-14
- NIST SP 800-34
- NIST SP 800-35

Perform Contingency Management Process

- Develop contingency planning policy statement
- Conduct the business impact analysis (BIA)
- Identify preventive controls
- Develop recovery strategies
- Develop an IT contingency plan
- Plan testing, training, and exercises
- Maintain Contingency Plan

Documents Produced

- Business Continuity Plan
- Business Recovery Plan
- Continuity of Operations Plan
- Continuity of Support Plan
- Crisis Communications Plan
- Cyber Incident Response Plan
- Disaster Recovery Plan
- Occupant Emergency Plan

Security Incident Reporting

- Security incident procedure for
  - Detecting
  - Reporting
  - Responding
- Mitigating damage risks
- Notify Federal CIRC
- Consult with
  - Law enforcement
  - Office of Inspector General
  - Other agencies as directed

Guidance Documents

- NIST SP 800-37
- NIST SP 800-14
- NIST SP 800-30
- NIST SP 800-31
- NIST SP 800-35
- NIST SP 800-61

Create Incident Response Plan

- Review incident response policy
- Assemble response team
- Define response procedures
- Define US-CERT coordination
- Agreements with other agencies
- Forensic analysis requirements
- Interface with law enforcement

Documents Produced

- Incident Response Plan
- US-CERT Coordination Plan
- Incident Logging Procedures`

Training Plans

- Inform staff and contractors
- Security risks of activities
- Responsibilities for compliance
- Reduce the risks

Guidance Documents

- NIST SP 800-37
- NIST SP 800-14
- NIST SP 800-16
- NIST SP 800-50

SP Create Security Training Program

- Design awareness & training program
- Develop material for training program
- Implement awareness & training program
- Evaluate and improve awareness & training program

Documents Produced

- Security Awareness & Training Plan
- Awareness & Training Metrics
- Needs Assessment Questionnaire
- Security Professional Development Syllabus

Testing and Evaluation Results

- Performed at least annually
- Management controls
- Operational controls
- Technical controls
- All systems in inventory
- Use independent evaluations

Guidance Documents

- NIST SP 800-37
- NIST SP 800-26
- NIST SP 800-42
- NIST SP 800-53A
- NIST SP 800-55
- NIST SP 800-64

Test & Evaluate Controls

- Perform system testing and evaluation
- Perform SP 800-26 evaluation and audit
- Examine C&A documentation
- Complete C&A security evaluation
- Update C&A documentation
- ST&E must include test cases, criteria, results using SP 800-53A and relevant STIG's

Documents Produced

- Security Test & Evaluation Plan
- System Self Assessment & Audit
- C&A Documentation Updates
- Recommendations for Enhanced Security Controls

Agency Risk Assessments

- Identify threats
- Identify vulnerabilities
- Analyze security controls
- Determine magnitude of harm

Guidance Documents

- NIST SP 800-37
- NIST SP 800-14
- NIST SP 800-30
- NIST SP 800-35
- NIST SP 800-64

Perform Risk Assessment

- Define operational environment
- Identify threats
- Identify vulnerabilities
- Analyze existing security controls
- Assess likelihood of threat
- Determine impact from loss
- Determine risk level
- Controls for mitigation of risk
- Reports and recommendations

Documents Produced

- Security Risk Assessment
- System Security Policy
- Management, Operational and Technical Controls
- Security Requirements
- Threat & Vulnerability Assessment

Remedial Action Process

- Remedial action process for
  - Planning
  - Implementing
  - Evaluating
  - Documenting
- Address deficiencies in
  - Policies
  - Procedures
  - Practices

Guidance Documents

- NIST SP 800-37
- OMB M-03-19
- OMB M-04-25
- OMB M-05-15
- POA&M
- NIST SP 800-55

Establish POA&M Process

- Identify weakness in systems
- Define remedial action needed
- Remedial costs as budget item
- Fill out POA&M matrix
- Separate PAO&M for each system
- Monitor progress
- Use previous POA&M reports
- Use C&A package data
- Submit to OMB upon request

Documents Produced

- Security Risk Assessment
- System Security Policy
- POA&M

Agency Reporting (3544 (c))

- The agency shall transmit a summary report of the annual IT security review including progress on correcting weakness and the results of the independent evaluation.
- IAW OMB M-05-15
- Tabular format - Tables A, B, C, & D
- Agency POA&M
- Previous IG report
- Previous FISMA compliance report
- Previous C&A package

Annual Independent Evaluation (3545)

- The agency shall perform an annual independent evaluation to determine the effectiveness of the security program and practices at the agency.
- Review security planning and the POA&M for resolving security weaknesses
- Review assigned security responsibilities and incident handling procedures

Review effectiveness of:

- Risk Assessments
- IT Security Program
- Capital Spending
- Security Training & Awareness

Create List of Conditions

- Identify issues
- Resolve & close issues
- Make recommendations for conditions
- Update POA&M

Incident Reporting (3546)

- The agency shall have a documented procedure for reporting security incidents and sharing information regarding common vulnerabilities.
- The agency shall have a documented procedure for coordinating with US-CERT.
- The agency shall have a documented procedure for patch management.

FISMA

Overview

Organizational Requirements (3544)

- Delegate authority to CIO for FISMA compliance.
- Provide protection commensurate with risk and magnitude of potential harm.
- Provide security that supports operations and assets.

Ensure sufficient trained personnel to support security requirements

- Ensure CIO reports annually on effectiveness of information security program.

Agency Program (3544 (b))

Develop, document and implement a security program to provide security for the information assets that support the operation of the agency.

Agency Reporting (3544 (c))

- The agency shall transmit a summary report annually of IT security reviews, progress & results of independent evaluations
- Agency POA&M Previous IG report, FISMA compliance report Previous C&A package

IAW OMB M-05-15 Tabular format – Tables A, B, C, & D

Annual Independent Evaluation (3545)

- Agency shall perform annual independent evaluations.
- Review security planning and the POA&M for resolving security weaknesses.
- Review assigned security responsibilities and incident handling procedures
- Review effectiveness of Risk Assessments, IT Security Program, Capital Spending, & SETA

Incident Reporting (3546)

- The agency shall have a documented procedure for reporting security incidents and sharing information regarding common vulnerabilities.

- The agency shall have a documented procedure for coordinating with FedCIRC.
- The agency shall have a documented procedure for patch management.

FISMA

Agency Program (3544 (b))

- Security Policies and Procedures
  - Based on risk assessment results
  - Cost effective Controls
  - Addressed throughout lifecycle
- Guidance Documents (NIST -59, -60, -64; FIPS 199)
- Establish IT Environment
  - Classify IT systems
  - Define security policy
  - Define baseline common & system specific security controls
- Documents Produced
  - Systems Description Environment
  - System Security Policy
  - MOU, ISA documents
  - Supporting Policies

FISMA

Agency Program (3544 (b))

- Subordinate Systems Plans
  - Individual IT systems
  - Networks
  - Groups of IT systems
- Guidance Documents (NIST -18, -27; ISO/IEC 17799)
- Create Security Plan
  - Analysis with system owner
  - Determine management, operational and technical controls
  - Assemble security plan
- Documents Produced
  - Systems Description Environment
  - Boundary Definition
  - Rules of Behavior
  - Security Plan

FISMA

Agency Program (3544 (b))

- Continuity of Operations Plan
  - Identify mission critical systems
  - Put plans and procedures in place
  - Protect assets
- Guidance Documents (NIST -14, -34; ISO/IEC 17799)
- Perform Contingency Management Process
  - Develop contingency planning policy
  - Conduct business impact analysis
  - Develop recovery strategies and contingency plans
- Documents Produced
  - Continuity Plans (Business, Operations, Support)
  - Recovery Plans (Business, Disaster)
  - Incident Response Plan

FISMA

Agency Program (3544 (b))

- Security Incident Reporting
  - Install procedures for detecting, reporting and responding
  - Mitigate damage
  - Notify FedCIRC
  - Consult with law enforcement, IG and others
- Guidance Documents (NIST -14, -30, -61; ISO/IEC 17799)
- Create Incident Response Plan
  - Review incident response policy
  - Define response procedures and FedCIRC coordination
  - Interface with law enforcement
- Documents Produced
  - Incident Response Plan
  - FedCIRC Coordination Plan
  - Incident Logging Procedure

FISMA

Agency Program (3544 (b))

- Training Plans
  - Identify responsibility for compliance
  - Inform staff and contractors of security risks
- Guidance Documents (NIST -14, -16, -50)
- Create Security Training Program
  - Design awareness and training program
  - Develop instructional material for training program
  - Implement and evaluate awareness and training program
- Documents Produced
  - Security Awareness & Training Plan
  - Awareness & Training Metrics
  - Security Professional Development Syllabus

FISMA

Agency Program (3544 (b))

- Testing and Evaluation Results
  - Perform tests at least annually
  - Focus on management, operational and technical controls
  - Use independent evaluations
- Guidance Documents (NIST -26, -37, -42, -53A)
- Test and Evaluate Controls
  - Perform system testing and evaluation
  - Perform SP 800-26 Rev 1 evaluation and audit
  - Complete C&A security evaluation
- Documents Produced
  - Security Test & Evaluation Plan
  - System Self-Assessment and Audit
  - Recommendations for enhanced security controls

FISMA

Agency Program (3544 (b))

- Agency Risk Assessments
  - Identify threats and vulnerabilities
  - Analyze security controls
  - Determine magnitude of harm
- Guidance Documents (NIST-14, -30, -64; ISO/IEC 17799)
- Perform Risk Assessments
  - Define operational environment
  - Identify threats and vulnerabilities
  - Analyze security controls
  - Determine level of risk
- Documents Produced
  - Security Risk Assessment
  - System Security Policy
  - Management, Operational and Technical controls
  - Security Requirements

FISMA

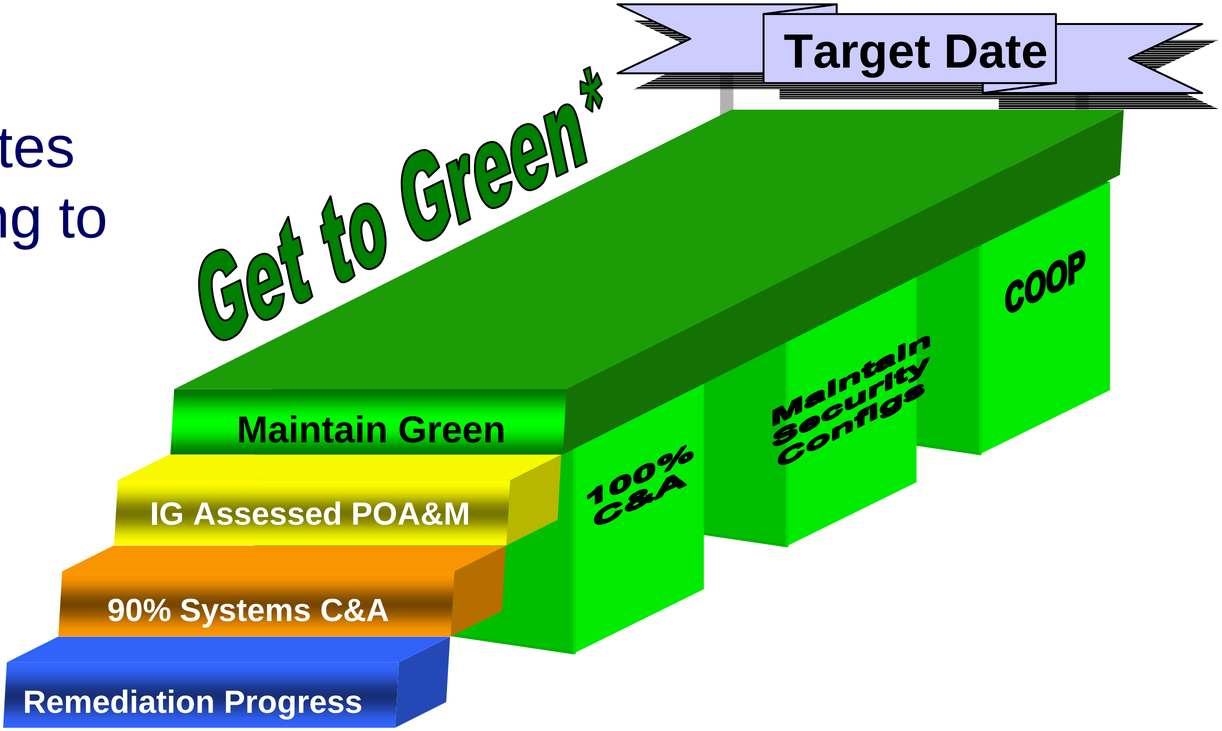
Agency Program (3544 (b))

- Remedial Action Process
  - Define process for planning, implementing, evaluating and documenting remedial action
  - Address deficiencies in policy, procedures and practice
- Guidance Documents (OMB M-04-25, POA&M, NIST -55)
- Establish POA&M Process
  - Identify weaknesses in systems
  - Define remedial action needed
  - Budget costs of remedial action
  - Monitor progress of remedial action
- Documents Produced
  - Security Risk Assessment
  - System Security Policy
  - POA&M

Government Directives

Driving Legislation

- FISMA also mandates compliance reporting to OMB
- FISMA reporting receives very high visibility!



** Steps to "Get To Green" taken from a statement of the Honorable Karen Evans, Administrator for Electronic Government and IT, OMB, before the Committee on Government Reform, US House of Representatives, April 7, 2005*

Security Policies and Procedures

Where is my guiding light?

Policies Not Present or Enforced

- What are the problems?
  - Policies are not in place or are obsolete
  - Policy enforcement is lax
  - No process for reviewing and updating policies
  - Policies are ambiguous and loosely defined
- What may be the solution sets?
  - Establish policy taxonomy
  - Create policy review board and process
  - Assign a policy management team

Security Policies and Procedures

Management Controls	Security Planning Policy
	Risk Assessment Policy
	System and Services Acquisition Policy
	Certification, Accreditation, and Security Assessments Policy
Operational Controls	Security Awareness and Training Policy
	Configuration Management Policy
	Contingency Planning Policy
	Media Protection Policy
	Physical and Environmental Protection Policy
	System and Information Integrity Policy
	Incident Response Policy
	System Maintenance Policy
	Personnel Security Policy
Technical Controls	Access Control Policy
	Auditing and Accountability Policy
	Identification and Authentication Policy
	System and Communications Protection Policy

RA-1: Risk Assessment Policy and Procedures

Policy 2.1 Risk Management
Description:

[Define Department/Division/Group] must complete security categorization and classification of information and conduct a comprehensive risk assessment on systems in accordance with the Risk Management standards and practices.

CA-1: Certification, Accreditation, and Security Assessments Policy and Procedures

Policy 5.1 System Certification and Assessments

Description:

All [Define] systems must be certified and accredited by an officially designated accrediting authority (DAA) prior to operating in a production environment. [Define Department/Division/Group] must continuously monitor critical controls and establish and maintain Plan of Actions & Milestones (POA&M) in accordance with System Certification and Assessments standards and practices.

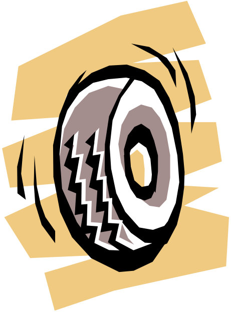
Security Requirements

What must I do to be secure??

Defining Requirements

- Baseline security requirements (BLSR) provide the foundation for the entire risk assessment process.
- BLSR are derived from Policies, Laws, Executive Orders, Directives, Regulations, Statutes
- Start with best practices (Don’t reinvent!)
- Project Management 101 – Establish Plan

Do Not Deviate



- Define and formalize management, operational, and technical Policies

Defining Requirements and Controls

- Define & formalize Clear / Concise Requirements
  - Incremental Approach – 1st Management, 2nd Operational, 3rd Technical
  - (Remember TMI = Information Overload / Short Circuit)
  - Distribute for Review / Acceptance / Buy-in
  - Signature Authority – C-Level
- Mapping Exercise
  - Management Requirement
  - Operational Requirement
  - Technical Requirement

In-Place Controls

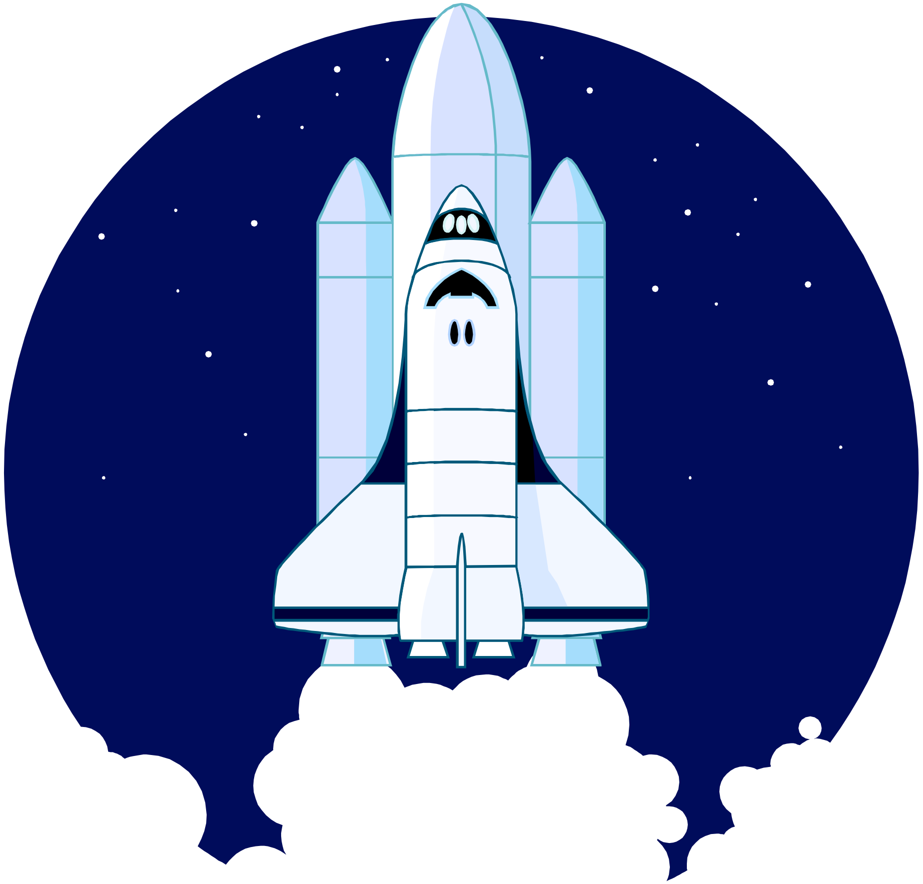
Creating a Value added RTM

Traditional Requirements Traceability Matrix (RTM)

1	2	3
Req #	**Requirement**	**Requirement Reference**
M-RA1	Perform security categorization in accordance with (IAW) FIPS – 199 and NIST Special Publications (SP) 800-59 & 60. This is documented and approved by an appropriate senior official.	800-53: RA-1 Based on Agency Policy or Directive.

RTM is developed for Management, Operational, & Technical security requirements. Each requirement is written in sufficient detail & references a source for that requirement.

Managing Effective Risk Assessments

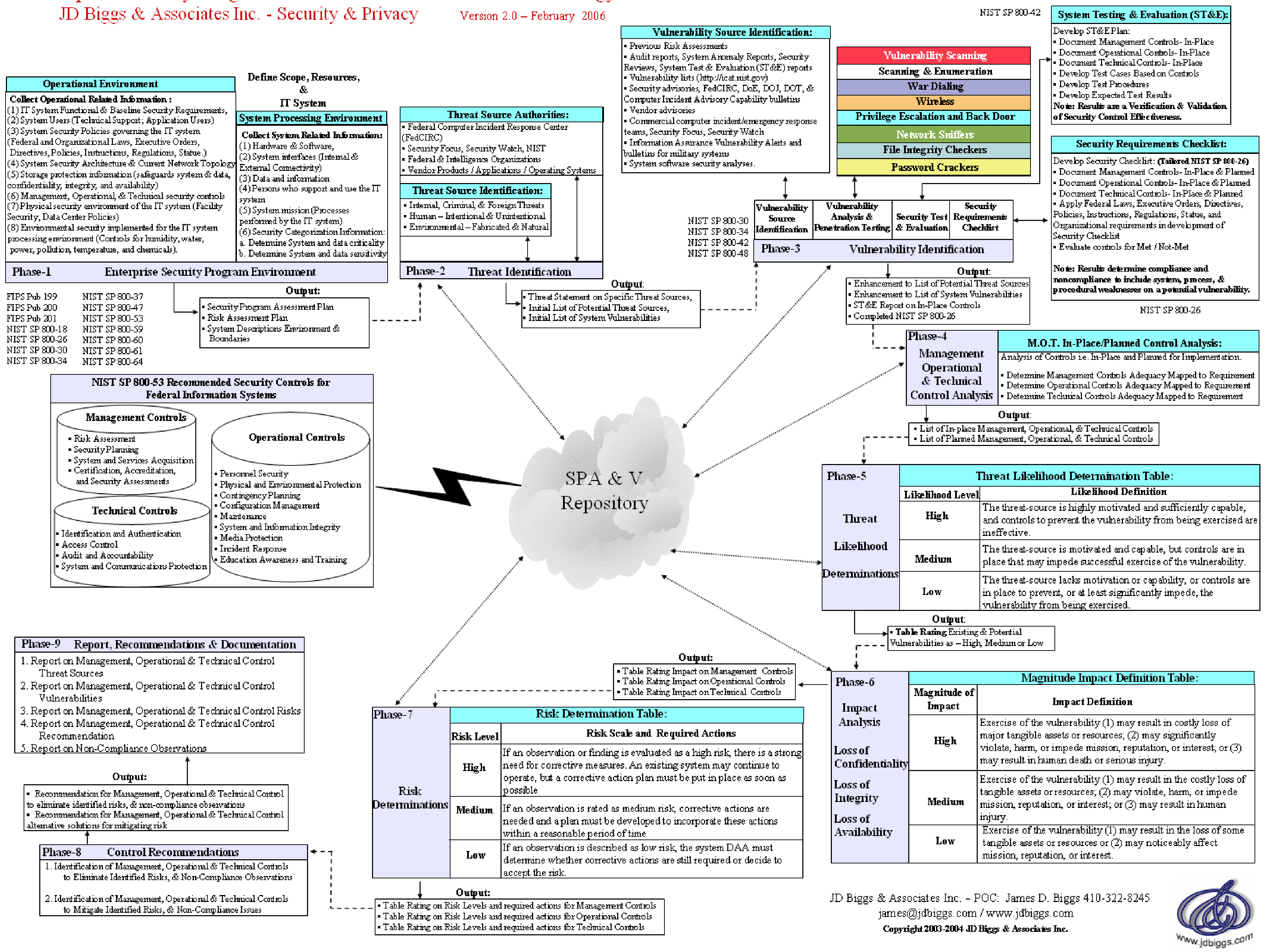


Are you sure we have looked at all risks?

Enterprise Security Program Assessment & Validation Methodology

JD Biggs & Associates Inc. - Security & Privacy

Version 2.0 – February 2006



Define Scope, Resources, & IT System

Operational Environment

Collect Operational Related Information :
(1) IT System Functional & Baseline Security Requirements,
(2) System Users (Technical Support; Application Users)
(3) System Security Policies governing the IT system (Federal and Organizational Laws, Executive Orders, Directives, Policies, Instructions, Regulations, Statue.)
(4) System Security Architecture & Current Network Topology
(5) Storage protection information (safeguards system & data, confidentiality, integrity, and availability)
(6) Management, Operational, & Technical security controls
(7) Physical security environment of the IT system (Facility Security, Data Center Policies)
(8) Environmental security implemented for the IT system processing environment (Controls for humidity, water, power, pollution, temperature, and chemicals).

System Processing Environment

Collect System Related Information:
(1) Hardware & Software,
(2) System interfaces (Internal & External Connectivity)
(3) Data and information
(4) Persons who support and use the IT system
(5) System mission (Processes performed by the IT system)
(6) Security Categorization Information:
a. Determine System and data criticality
b. Determine System and data sensitivity

Phase-1 Enterprise Security Program Environment

FIPS Pub 199
FIPS Pub 200
FIPS Pub 201
NIST SP 800-18
NIST SP 800-26
NIST SP 800-30
NIST SP 800-34
NIST SP 800-37
NIST SP 800-47
NIST SP 800-53
NIST SP 800-59
NIST SP 800-60
NIST SP 800-61
NIST SP 800-64

Output:
- Security Program Assessment Plan
- Risk Assessment Plan
- System Descriptions Environment & Boundaries

NIST SP 800-53 Recommended Security Controls for Federal Information Systems

Management Controls
- Risk Assessment
- Security Planning
- System and Services Acquisition
- Certification, Accreditation, and Security Assessments

Technical Controls
- Identification and Authentication
- Access Control
- Audit and Accountability
- System and Communications Protection

Operational Controls
- Personnel Security
- Physical and Environmental Protection
- Contingency Planning
- Configuration Management
- Maintenance
- System and Information Integrity
- Media Protection
- Incident Response
- Education Awareness and Training

Threat Source Authorities:
- Federal Computer Incident Response Center (FedCIRC)
- Security Focus, Security Watch, NIST
- Federal & Intelligence Organizations
- Vendor Products / Applications / Operating Systems

Threat Source Identification:
- Internal, Criminal, & Foreign Threats
- Human – Intentional & Unintentional
- Environmental – Fabricated & Natural

Phase-2 Threat Identification

Output:
- Threat Statement on Specific Threat Sources,
- Initial List of Potential Threat Sources,
- Initial List of System Vulnerabilities

Vulnerability Source Identification:
- Previous Risk Assessments
- Audit reports, System Anomaly Reports, Security Reviews, System Test & Evaluation (ST&E) reports
- Vulnerability lists (http://icat.nist.gov)
- Security advisories, FedCIRC, DoE, DOJ, DOT, & Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams, Security Focus, Security Watch
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

Vulnerability Scanning
Scanning & Enumeration
War Dialing
Wireless
Privilege Escalation and Back Door
Network Sniffers
File Integrity Checkers
Password Crackers

NIST SP 800-42

System Testing & Evaluation (ST&E):
Develop ST&E Plan:
- Document Management Controls- In-Place
- Document Operational Controls- In-Place
- Document Technical Controls- In-Place
- Develop Test Cases Based on Controls
- Develop Test Procedures
- Develop Expected Test Results

Note: Results are a Verification & Validation of Security Control Effectiveness.

Security Requirements Checklist:
Develop Security Checklist: **(Tailored NIST SP 800-26)**
- Document Management Controls- In-Place & Planned
- Document Operational Controls- In-Place & Planned
- Document Technical Controls- In-Place & Planned
- Apply Federal Laws, Executive Orders, Directives, Policies, Instructions, Regulations, Statue, and Organizational requirements in development of Security Checklist
- Evaluate controls for Met / Not-Met

Note: Results determine compliance and noncompliance to include system, process, & procedural weaknesses on a potential vulnerability.

NIST SP 800-26

NIST SP 800-30
NIST SP 800-34
NIST SP 800-42
NIST SP 800-48

Vulnerability Source Identification	Vulnerability Analysis & Penetration Testing	Security Test & Evaluation	Security Requirements Checklist

Phase-3 Vulnerability Identification

Output:
- Enhancement to List of Potential Threat Sources
- Enhancement to List of System Vulnerabilities
- ST&E Report on In-Place Controls
- Completed NIST SP 800-26

Phase-4 Management Operational & Technical Control Analysis

M.O.T. In-Place/Planned Control Analysis:
Analysis of Controls i.e. In-Place and Planned for Implementation.
- Determine Management Controls Adequacy Mapped to Requirement
- Determine Operational Controls Adequacy Mapped to Requirement
- Determine Technical Controls Adequacy Mapped to Requirement

Output:
- List of In-place Management, Operational, & Technical Controls
- List of Planned Management, Operational, & Technical Controls

SPA & V Repository

Phase-5 Threat Likelihood Determinations

Threat Likelihood Determination Table:

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Output:
- Table Rating Existing & Potential Vulnerabilities as – High, Medium or Low

Phase-6 Impact Analysis
Loss of Confidentiality
Loss of Integrity
Loss of Availability

Magnitude Impact Definition Table:

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect mission, reputation, or interest.

Output:
- Table Rating Impact on Management Controls
- Table Rating Impact on Operational Controls
- Table Rating Impact on Technical Controls

Phase-7 Risk Determinations

Risk Determination Table:

Risk Level	Risk Scale and Required Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
Low	If an observation is described as low risk, the system DAA must determine whether corrective actions are still required or decide to accept the risk.

Output:
- Table Rating on Risk Levels and required actions for Management Controls
- Table Rating on Risk Levels and required actions for Operational Controls
- Table Rating on Risk Levels and required actions for Technical Controls

Phase-8 Control Recommendations
1. Identification of Management, Operational & Technical Controls to Eliminate Identified Risks, & Non-Compliance Observations
2. Identification of Management, Operational & Technical Controls to Mitigate Identified Risks, & Non-Compliance Issues

Output:
- Recommendation for Management, Operational & Technical Control to eliminate identified risks, & non-compliance observations
- Recommendation for Management, Operational & Technical Control alternative solutions for mitigating risk

Phase-9 Report, Recommendations & Documentation
1. Report on Management, Operational & Technical Control Threat Sources
2. Report on Management, Operational & Technical Control Vulnerabilities
3. Report on Management, Operational & Technical Control Risks
4. Report on Management, Operational & Technical Control Recommendation
5. Report on Non-Compliance Observations

JD Biggs & Associates Inc. - POC: James D. Biggs 410-322-8245
james@jdbiggs.com / www.jdbiggs.com

Agency Risk Assessments

- What are the problems?
  - Rushed effort with inadequate planning
  - Critical skills not in labor mix
  - Coordinating access to facilities and systems
  - Resource availability
- What may be the solution sets?
  - Include risk assessment in SDLC
  - Project planning 101, 102 and 103
  - Senior management involvement

Vulnerability Identification

Vulnerability Scanning

Scanning & Enumeration

War Dialing

Wireless

Privilege Escalation and Back Door

Network Sniffers

File Integrity Checkers

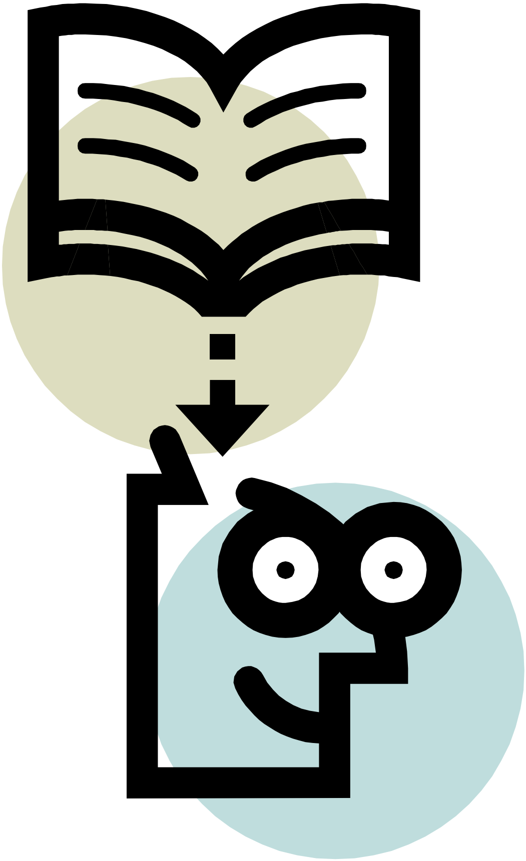
Password Crackers

- **Vulnerability Assessment** – Network topology review; workstation & server security testing, 3rd party access review, regulation & policy compliance review, inbound/outbound traffic control, firewall & router ACLs to include log files, IDS setup & implementation and phone lines.
- **Penetration Testing** – Establish rules of engagement, Indemnification. Pen Testing is actively evaluating security control effectiveness.

Vulnerability Scanning Tools

Tool	Capabilities	Website	Linux	Win32	Cost
CyberCop Scanner	Vulnerability scanner	http://www.pgp.com/products/	✕	✕	$
Description	CyberCop Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.				
ISS Internet Scanner	Vulnerability scanner	http://www.iss.net/	✕		$
Description	*ISS Internet Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.*				
Nessus	Vulnerability scanner	http://www.nessus.org/	✕	# (client only)	Free
Description	A freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.				
SAINT	Vulnerability scanner	http://www.wwdsi.com/saint/	✕		$
Description	SAINT is an updated and enhanced version of SATAN, is designed to assess the security of computer networks.				
SARA	Vulnerability scanner	http://www-arc.com/sara/	✕		Free
Description	Sara is a freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.				

Certification and Accreditation

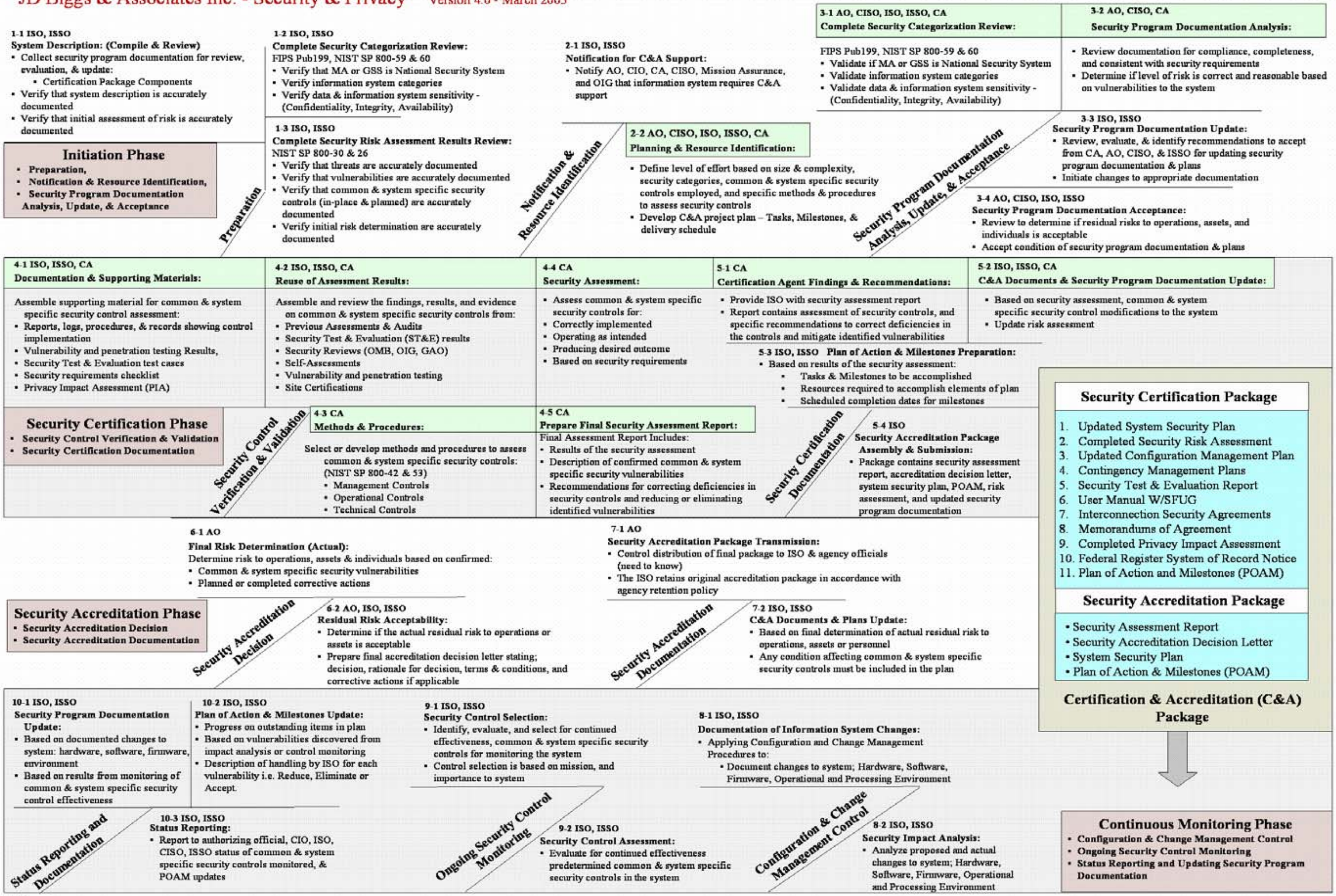


How can I manage all these tasks and documents?

Enterprise Security Certification & Accreditation Methodology

JD Biggs & Associates Inc. - Security & Privacy

Version 4.0 - March 2005



1-1 ISO, ISSO
System Description: (Compile & Review)
- Collect security program documentation for review, evaluation, & update:
  - Certification Package Components
- Verify that system description is accurately documented
- Verify that initial assessment of risk is accurately documented

1-2 ISO, ISSO
Complete Security Categorization Review:
FIPS Pub199, NIST SP 800-59 & 60
- Verify that MA or GSS is National Security System
- Verify information system categories
- Verify data & information system sensitivity - (Confidentiality, Integrity, Availability)

1-3 ISO, ISSO
Complete Security Risk Assessment Results Review:
NIST SP 800-30 & 26
- Verify that threats are accurately documented
- Verify that vulnerabilities are accurately documented
- Verify that common & system specific security controls (in-place & planned) are accurately documented
- Verify initial risk determination are accurately documented

Initiation Phase
- **Preparation,**
- **Notification & Resource Identification,**
- **Security Program Documentation Analysis, Update, & Acceptance**

Preparation
Notification & Resource Identification
Security Program Documentation Analysis, Update, & Acceptance

2-1 ISO, ISSO
Notification for C&A Support:
- Notify AO, CIO, CA, CISO, Mission Assurance, and OIG that information system requires C&A support

2-2 AO, CISO, ISO, ISSO, CA
Planning & Resource Identification:
- Define level of effort based on size & complexity, security categories, common & system specific security controls employed, and specific methods & procedures to assess security controls
- Develop C&A project plan – Tasks, Milestones, & delivery schedule

3-1 AO, CISO, ISO, ISSO, CA
Complete Security Categorization Review:
FIPS Pub199, NIST SP 800-59 & 60
- Validate if MA or GSS is National Security System
- Validate information system categories
- Validate data & information system sensitivity - (Confidentiality, Integrity, Availability)

3-2 AO, CISO, CA
Security Program Documentation Analysis:
- Review documentation for compliance, completeness, and consistent with security requirements
- Determine if level of risk is correct and reasonable based on vulnerabilities to the system

3-3 ISO, ISSO
Security Program Documentation Update:
- Review, evaluate, & identify recommendations to accept from CA, AO, CISO, & ISSO for updating security program documentation & plans
- Initiate changes to appropriate documentation

3-4 AO, CISO, ISO, ISSO
Security Program Documentation Acceptance:
- Review to determine if residual risks to operations, assets, and individuals is acceptable
- Accept condition of security program documentation & plans

4-1 ISO, ISSO, CA
Documentation & Supporting Materials:
Assemble supporting material for common & system specific security control assessment:
- Reports, logs, procedures, & records showing control implementation
- Vulnerability and penetration testing Results,
- Security Test & Evaluation test cases
- Security requirements checklist
- Privacy Impact Assessment (PIA)

4-2 ISO, ISSO, CA
Reuse of Assessment Results:
Assemble and review the findings, results, and evidence on common & system specific security controls from:
- Previous Assessments & Audits
- Security Test & Evaluation (ST&E) results
- Security Reviews (OMB, OIG, GAO)
- Self-Assessments
- Vulnerability and penetration testing
- Site Certifications

4-4 CA
Security Assessment:
- Assess common & system specific security controls for:
- Correctly implemented
- Operating as intended
- Producing desired outcome
- Based on security requirements

5-1 CA
Certification Agent Findings & Recommendations:
- Provide ISO with security assessment report
- Report contains assessment of security controls, and specific recommendations to correct deficiencies in the controls and mitigate identified vulnerabilities

5-2 ISO, ISSO, CA
C&A Documents & Security Program Documentation Update:
- Based on security assessment, common & system specific security control modifications to the system
- Update risk assessment

5-3 ISO, ISSO Plan of Action & Milestones Preparation:
- Based on results of the security assessment:
  - Tasks & Milestones to be accomplished
  - Resources required to accomplish elements of plan
  - Scheduled completion dates for milestones

Security Certification Phase
- **Security Control Verification & Validation**
- **Security Certification Documentation**

Security Control Verification & Validation
Security Certification Documentation

4-3 CA
Methods & Procedures:
Select or develop methods and procedures to assess common & system specific security controls: (NIST SP 800-42 & 53)
- Management Controls
- Operational Controls
- Technical Controls

4-5 CA
Prepare Final Security Assessment Report:
Final Assessment Report Includes:
- Results of the security assessment
- Description of confirmed common & system specific security vulnerabilities
- Recommendations for correcting deficiencies in security controls and reducing or eliminating identified vulnerabilities

5-4 ISO
Security Accreditation Package Assembly & Submission:
- Package contains security assessment report, accreditation decision letter, system security plan, POAM, risk assessment, and updated security program documentation

Security Certification Package
1. Updated System Security Plan
2. Completed Security Risk Assessment
3. Updated Configuration Management Plan
4. Contingency Management Plans
5. Security Test & Evaluation Report
6. User Manual W/SFUG
7. Interconnection Security Agreements
8. Memorandums of Agreement
9. Completed Privacy Impact Assessment
10. Federal Register System of Record Notice
11. Plan of Action and Milestones (POAM)

Security Accreditation Package
- Security Assessment Report
- Security Accreditation Decision Letter
- System Security Plan
- Plan of Action & Milestones (POAM)

Certification & Accreditation (C&A) Package

6-1 AO
Final Risk Determination (Actual):
Determine risk to operations, assets & individuals based on confirmed:
- Common & system specific security vulnerabilities
- Planned or completed corrective actions

7-1 AO
Security Accreditation Package Transmission:
- Control distribution of final package to ISO & agency officials (need to know)
- The ISO retains original accreditation package in accordance with agency retention policy

Security Accreditation Phase
- **Security Accreditation Decision**
- **Security Accreditation Documentation**

Security Accreditation Decision
Security Accreditation Documentation

6-2 AO, ISO, ISSO
Residual Risk Acceptability:
- Determine if the actual residual risk to operations or assets is acceptable
- Prepare final accreditation decision letter stating; decision, rationale for decision, terms & conditions, and corrective actions if applicable

7-2 ISO, ISSO
C&A Documents & Plans Update:
- Based on final determination of actual residual risk to operations, assets or personnel
- Any condition affecting common & system specific security controls must be included in the plan

10-1 ISO, ISSO
Security Program Documentation Update:
- Based on documented changes to system: hardware, software, firmware, environment
- Based on results from monitoring of common & system specific security control effectiveness

10-2 ISO, ISSO
Plan of Action & Milestones Update:
- Progress on outstanding items in plan
- Based on vulnerabilities discovered from impact analysis or control monitoring
- Description of handling by ISO for each vulnerability i.e. Reduce, Eliminate or Accept

9-1 ISO, ISSO
Security Control Selection:
- Identify, evaluate, and select for continued effectiveness, common & system specific security controls for monitoring the system
- Control selection is based on mission, and importance to system

8-1 ISO, ISSO
Documentation of Information System Changes:
- Applying Configuration and Change Management Procedures to:
  - Document changes to system; Hardware, Software, Firmware, Operational and Processing Environment

Status Reporting and Documentation
Ongoing Security Control Monitoring
Configuration & Change Management Control

10-3 ISO, ISSO
Status Reporting:
- Report to authorizing official, CIO, ISO, CISO, ISSO status of common & system specific security controls monitored, & POAM updates

9-2 ISO, ISSO
Security Control Assessment:
- Evaluate for continued effectiveness predetermined common & system specific security controls in the system

8-2 ISO, ISSO
Security Impact Analysis:
- Analyze proposed and actual changes to system; Hardware, Software, Firmware, Operational and Processing Environment

Continuous Monitoring Phase
- **Configuration & Change Management Control**
- **Ongoing Security Control Monitoring**
- **Status Reporting and Updating Security Program Documentation**

Legend
Authorizing Official = AO
Chief Information Officer = CIO
Chief Information Security Officer = CISO
Information System Owner = ISO
Information System Security Officer = ISSO
Certification Agent = CA

PROJECT performance CORPORATION

JD Biggs & Associates Inc. POC: James D. Biggs 410-322-8245
james@jdbiggs.com / www.jdbiggs.com

www.jdbiggs.com

Accreditation Decision

- I have determined that the risk to **Agency Operations**, **Agency Assets**, or **Individuals** resulting from the operation of the information system is acceptable.
- Accordingly, I am issuing an ***Authorization to Operate*** the information system in its existing operating environment.
- This security accreditation is my formal declaration that **Adequate Security Controls** have been implemented in the information system and that a satisfactory level of security is present in the system.

C&A Process Overview

- C&A Process Phases
  - Initiation Phase
  - Security Certification Phase
  - Security Accreditation Phase
  - Continuous Monitoring Phase
- C&A Roles and Responsibilities
  - Authorizing Official (AO)
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Information System Owner (ISO)
  - Information System Security Officer (ISSO)
  - Certification Agent (CA)

Security Certification Package

Updated System Security Plan
Completed Security Risk Assessment
Updated Configuration Management Plan
Contingency Management Plans
Security Test & Evaluation Report
User Manual W/SFUG
Interconnection Security Agreements
Memorandums of Agreement
Completed Privacy Impact Assessment
Federal Register System of Record Notice
Plan of Action and Milestones (POAM)

Security Accreditation Package

- Security Assessment Report
- Security Accreditation Decision Letter
- System Security Plan
- Plan of Action & Milestones (POAM)

Certification & Accreditation (C&A) Package

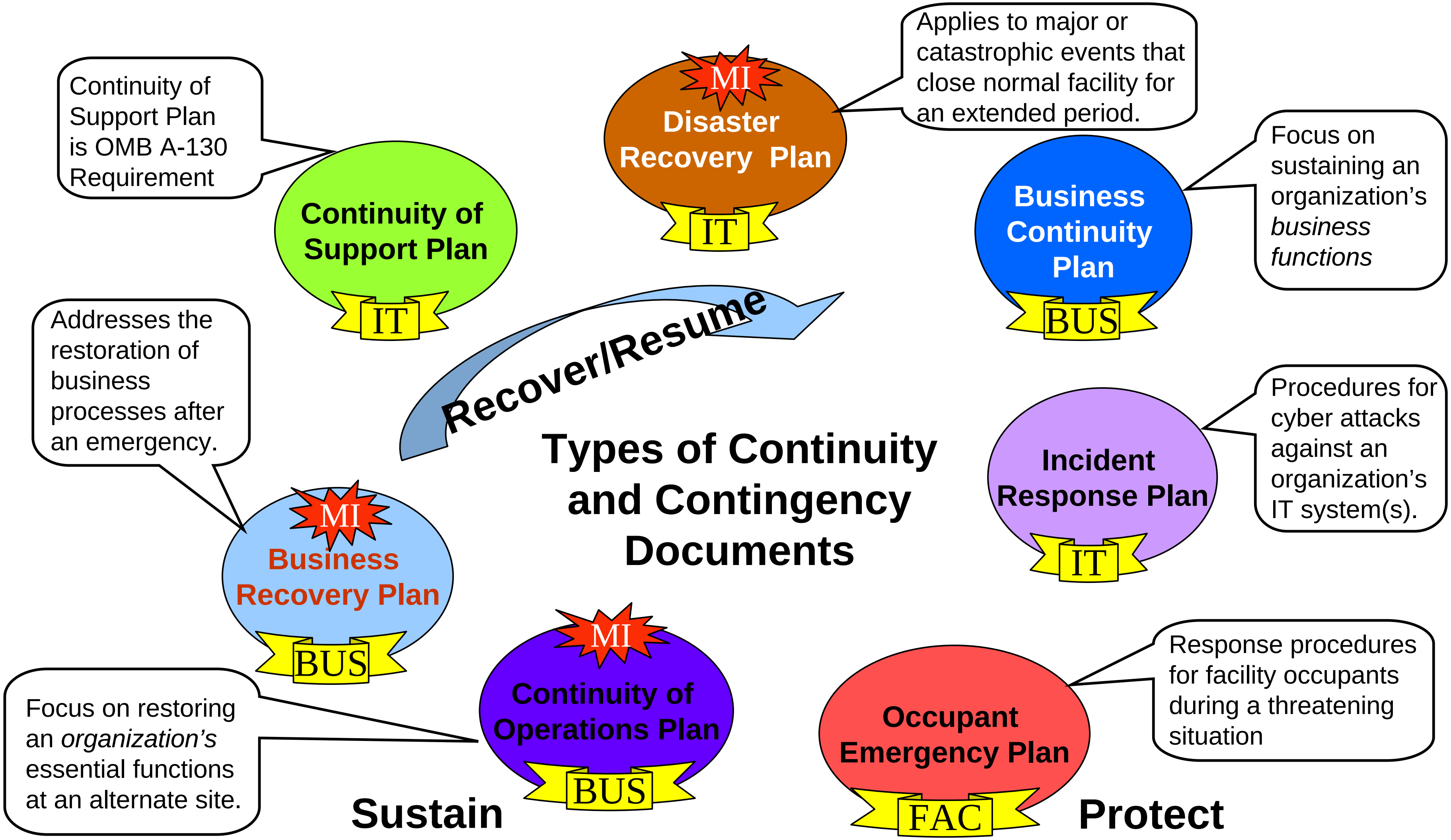
C&A Process Tasks

- Required for major applications and general support systems
  - Evaluation of management, operational and technical security controls
  - Triggered by time (3 years) or significant changes
- Define accreditation boundaries, interfaces and subsystems and operating environment
- Assess risk for the environment within accreditation boundary
  - Threats and vulnerabilities
  - System test and evaluation
- Develop the Accreditation Package
  - Result of C&A activities by certifier.
  - Details all the activities from first three phases
- Make risk-based accreditation decision
  - Accept residual risk for that environment
  - Authorization to operate in that environment

Interface with Other Processes

Now how does this piece fit?

Contingency Planning



Types of Continuity and Contingency Documents

Recover/Resume

Continuity of Support Plan (IT)

Continuity of Support Plan is OMB A-130 Requirement

Disaster Recovery Plan (MI, IT)

Applies to major or catastrophic events that close normal facility for an extended period.

Business Continuity Plan (BUS)

Focus on sustaining an organization's *business functions*

Incident Response Plan (IT)

Procedures for cyber attacks against an organization's IT system(s).

Business Recovery Plan (MI, BUS)

Addresses the restoration of business processes after an emergency.

Continuity of Operations Plan (MI, BUS)

Focus on restoring an *organization's* essential functions at an alternate site.

Occupant Emergency Plan (FAC)

Response procedures for facility occupants during a threatening situation

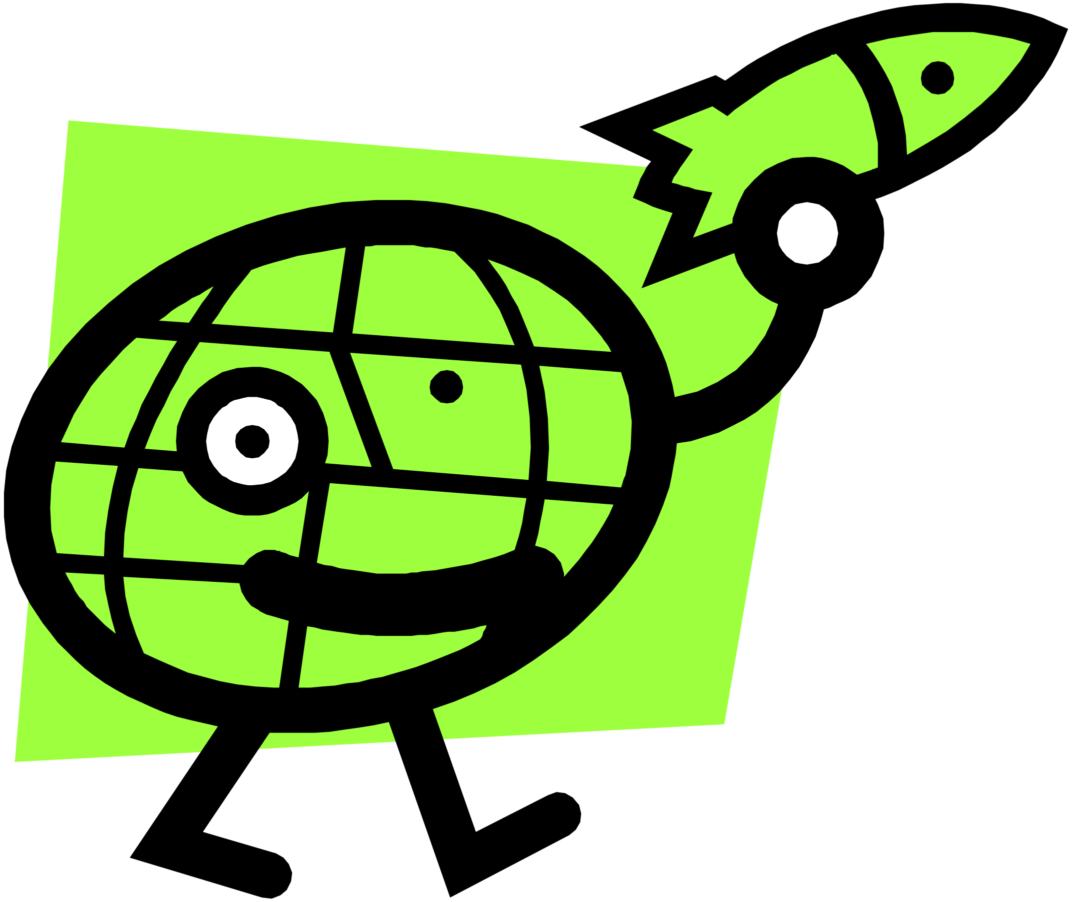
Sustain

Protect

Remedial Processes

- POA&M
  - Manage all known weaknesses in the POA&M
  - Verify and validate completed corrective actions
- Maintain Security Requirements
  - Maintain BLSR & BLPR under configuration control
  - Leverage existing and cost effective controls
- Self Assessments
  - Supports the C&A Continuous Monitoring process
- OIG or GAO audits

Using Automation Support for FISMA



How can I make this process fly?

Benefits of Automation Support

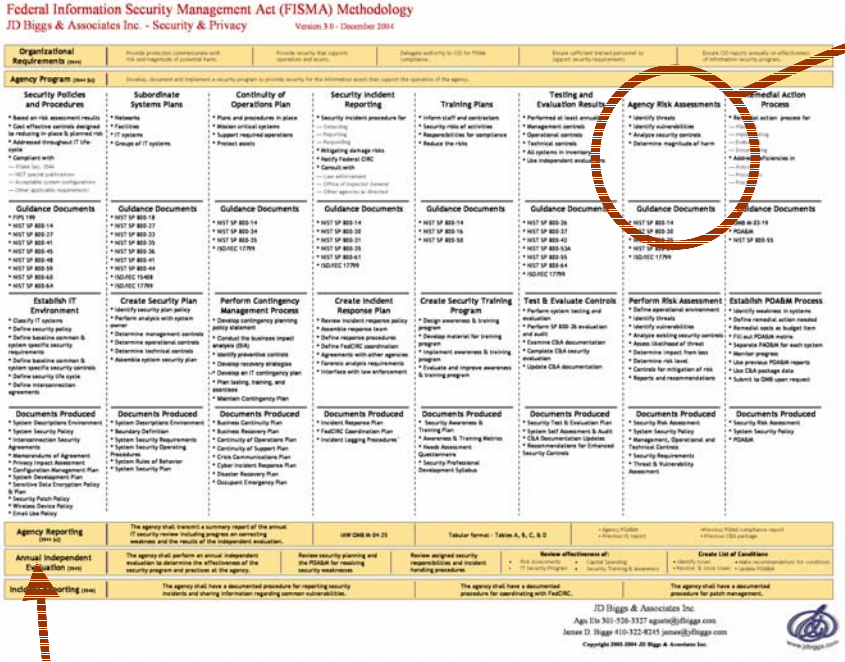
- Reduced Personnel Costs for Compliance
- Consistency in Assessments and Evaluations
- Documents Formatted Correctly
- System Inventory Management Automated
- Auditable Compliance Process

Criteria for Tool Selection

- Integration Potential with Existing Infrastructure
- User Interface Intuitive and Effective
- Capability for Audit Trail
- Output Formats for Documents and Reports
- Adaptability to Specific Agency Requirements
- Interface to POA&M Process

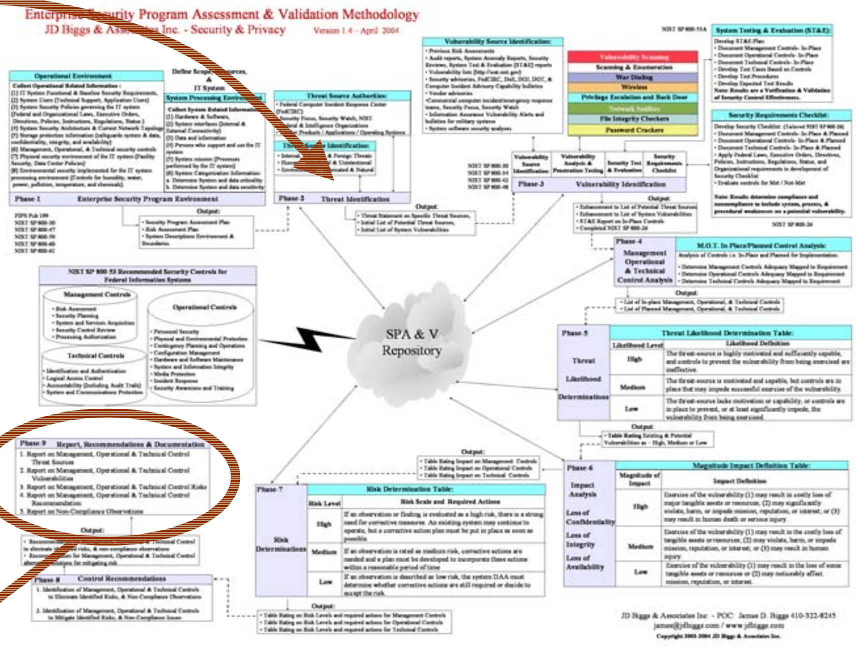
Sample of Vendor Products

- Automated Security Self-Assessment Tool (ASSET)
- Xacta Web C&A
- Xacta Commerce Trust
- Risk Management System (RMS)
- Risk Watch
- Trusted Agent FISMA
- Other Proprietary Support Tools



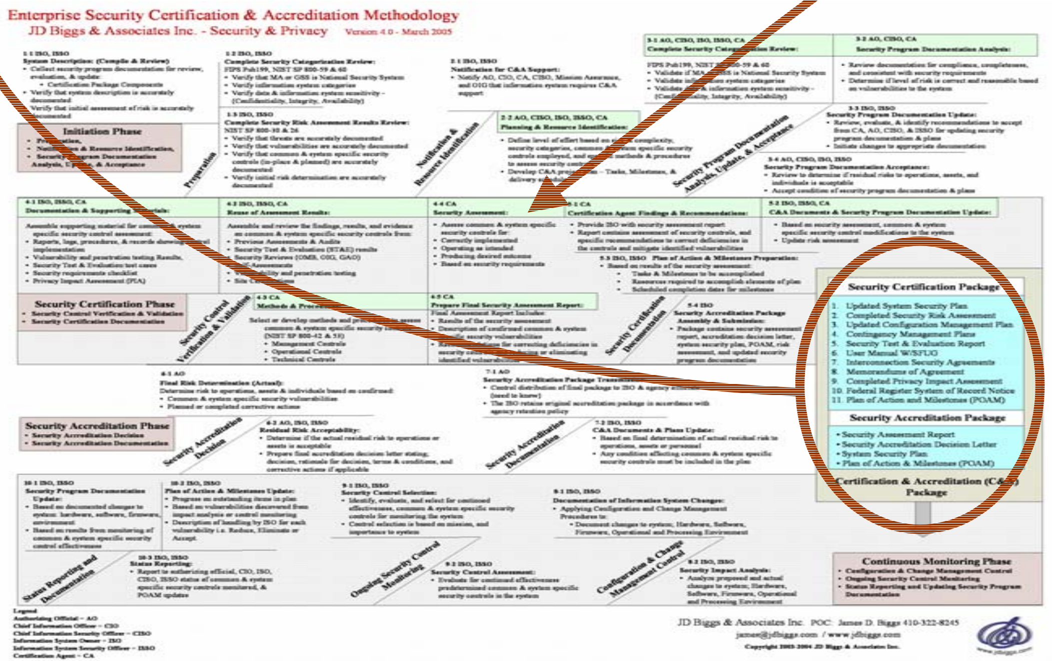
Federal Information Security Management Act (FISMA) Methodology
JD Biggs & Associates Inc. - Security & Privacy Version 3.0 - December 2004

Organizational Requirements
Agency Program
Security Policies and Procedures
Subordinate Systems Plans
Continuity of Operations Plan
Security Incident Reporting
Training Plans
Testing and Evaluation Results
Agency Risk Assessments
Remedial Action Process
Guidance Documents
Establish IT Environment
Create Security Plan
Perform Contingency Management Process
Create Incident Response Plan
Create Security Training Program
Test & Evaluate Controls
Perform Risk Assessment
Establish POA&M Process
Documents Produced
Agency Reporting
Annual Independent Evaluation
Incident Reporting
JD Biggs & Associates Inc



Enterprise Security Program Assessment & Validation Methodology
JD Biggs & Associates Inc. - Security & Privacy Version 1.4 - April 2004

Operational Environment
Define Scope, Resources, & IT System
System Processing Environment
Threat Source Authorities
Threat Source Identification
Vulnerability Source Identification
Vulnerability Scanning
Scanning & Enumeration
War Dialing
Wireless
Privilege Escalation and Back Door
Network Sniffers
File Integrity Checkers
Password Crackers
System Testing & Evaluation (ST&E)
Security Requirements Checklist
Phase 1 Enterprise Security Program Environment
Phase 2 Threat Identification
Phase 3 Vulnerability Identification
Phase 4 M.O.T. In Place/Planned Control Analysis
Phase 5 Threat Likelihood Determination Table
Phase 6 Magnitude Impact Definition Table
Phase 7 Risk Determination Table
Phase 8 Control Recommendations
Phase 9 Report, Recommendations & Documentation
NIST SP 800-53 Recommended Security Controls for Federal Information Systems
Management Controls
Operational Controls
Technical Controls
SPA & V Repository
High
Medium
Low



Enterprise Security Certification & Accreditation Methodology
JD Biggs & Associates Inc. - Security & Privacy Version 4.0 - March 2005

Initiation Phase
Preparation
Notification & Resource Identification
Security Program Documentation Analysis, Update, & Acceptance
Security Certification Phase
Security Control Verification & Validation
Security Certification Documentation
Security Accreditation Phase
Security Accreditation Decision
Security Accreditation Documentation
Continuous Monitoring Phase
Configuration & Change Management Control
Ongoing Security Control Monitoring
Status Reporting and Documentation
Security Certification Package
Security Accreditation Package
Certification & Accreditation (C&A) Package

Security Certification Package
1. Updated System Security Plan
2. Completed Security Risk Assessment
3. Updated Configuration Management Plan
4. Contingency Management Plans
5. Security Test & Evaluation Report
6. User Manual W/SFUG
7. Interconnection Security Agreements
8. Memorandums of Agreement
9. Completed Privacy Impact Assessment
10. Federal Register System of Record Notice
11. Plan of Action and Milestones (POAM)

Security Accreditation Package
- Security Assessment Report
- Security Accreditation Decision Letter
- System Security Plan
- Plan of Action & Milestones (POAM)

How everything fits together.

FISMA Compliance Avoids Red

Are you ready for an IG Inspection?

Had Enough?

Any Questions?

Navigating the FISMA Compliance Labyrinth

Thank you

James D. Biggs, 410-322-8245 james@jdbiggs.com
JD Biggs & Associates, Inc. http://www.jdbiggs.com

Agu Ets, 301-526-3327 aets@ppc.com
Project Performance Corporation **http://www.ppc.com**