Innovations in Justice:

Information Sharing Strategies and Best Practices
BJA Regional Information Sharing Conference

Establishing Effective Security Policies and Procedures

Mr. James E. Cabral Jr., CISSP, CISA, GSEC
MTG Management Consultants, LLC

June 6, 2007

MTG Management Consultants

MTG Management Consultants, L.L.C.
1111 Third Avenue, Suite 3010
Seattle, Washington 98101-3292
206.442.5010   206.442.5011 *fax*
www.mtgmc.com

Albany Austin Denver Seattle Topeka Washington D.C.

Overview

- Justice IT Security Issues
- Security Policies
- Security Policy Development Life Cycle
- Example Policy Development
- Security Frameworks
- Security Guidance for Justice Systems
- Example Policies and Procedures
- Questions for You

Justice IT Security Issues

- Disaster Recovery
- File & Disk Level Encryption
- Enterprise & Personal Firewalls
- Ongoing Vulnerability Testing
- Multi-Tier Anti-Virus Solutions
- Intrusion Detection Systems
- Internal Modem Control
- Operating System File Integrity
- Web Site Security
- Patch Management
- Wireless Security
- E-Mail Filtering and Monitoring
- Spam & Spyware Controls
- Employee Web Monitoring & Filtering
- Instant Messenger Monitoring & Management
- Intrusion Prevention (Behavioral)

- Platform Security Compliance
- Remote Access Authentication/ Identity Management
- Remote Security Administration
- Enterprise-Wide Single Sign-On
- Self-Service Password Reset
- Secure Web-Based E-Mail
- Password Recovery
- Change Management Tracking
- Document Control & Classification
- Log Analysis & Consolidation
- Network Traffic Monitoring & Reconstruction
- Forensic Investigations & Media Analysis
- Agency & Staff Certification

Security Policies

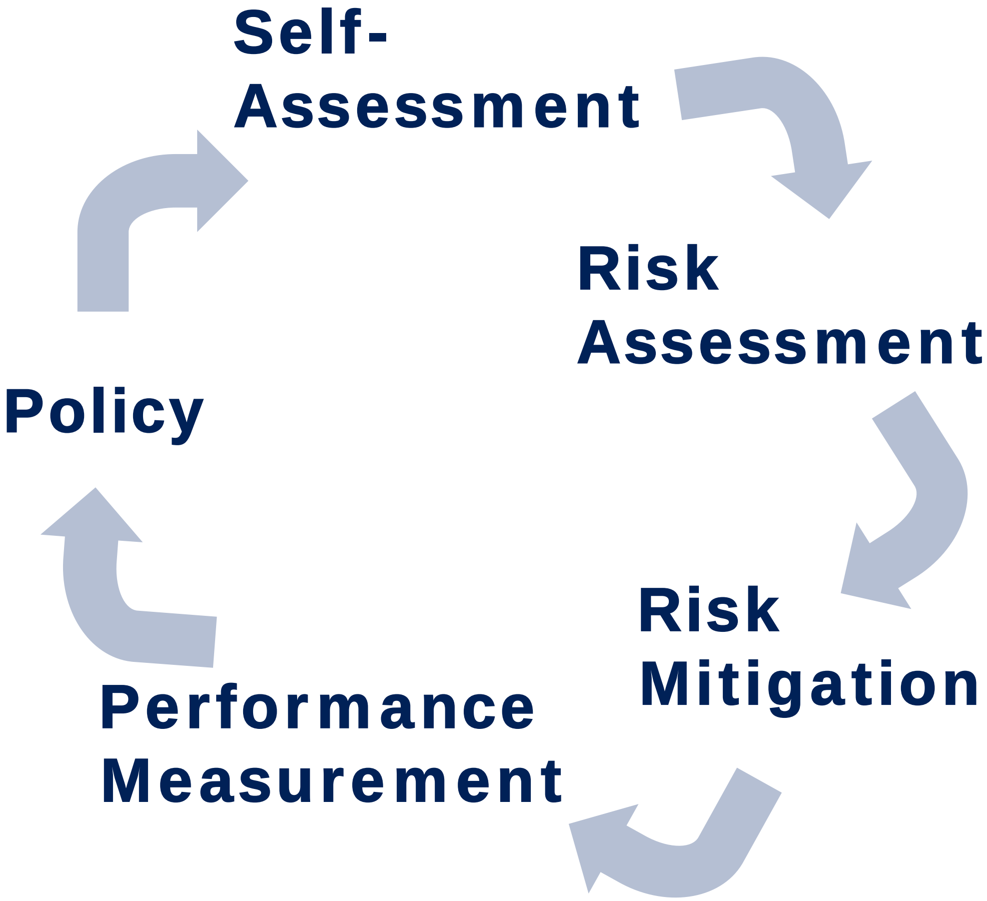
- Are administrative directives.
- Set goals and assign responsibilities.
- Reduce a specific set of security risks to a level acceptable to management.

Security Policies
Considerations

- Pertinent legislation and regulations.
- Agreements with other parties.
- Higher level policies.
- Detailed knowledge of the target IT system.
- Anticipated threats.
- Implementation and operational costs.
- Management’s risk tolerance.

Security Policy Development Life Cycle

- Policy.
- Self-assessment.
- Risk assessment.
- Risk mitigation.
- Performance measurement.



Self-Assessment

Risk Assessment

Risk Mitigation

Performance Measurement

Policy

Security Policy Development Life Cycle
Organizing a Policy Program

1. Determine which system part or systems for which you would like to develop security policies.
2. Obtain leadership and involvement of senior management.
3. Identify and recruit internal and external stakeholders and obtain their input and support.
4. Assign a project manager to guide and oversee initiative.
5. Create a governance structure with defined roles and responsibilities.
6. Assemble appropriate stakeholders and hold a kickoff meeting to discuss process.

Security Policy Development Life Cycle
Step 1. Self Assessment

1. Gather relevant organizational data about the systems to be assessed.
2. Use available tools and frameworks to identify and describe each risk.
3. Identify current policies and controls that mitigate the risk.

Security Policy Development Life Cycle
Step 2. Risk Assessment

1. Categorize and quantify each identified risk:
   - Likelihood: remote, possible, or likely.
   - Severity: high, medium, or low.
   - Area of impact: human, financial, liability, etc.
2. Determine your tolerance level for each identified risk.
   - Is management willing to assume the risk?
3. Determine a numeric priority for action for each identified risk.

Security Policy Development Life Cycle
Step 3. Risk Mitigation

1. Determine risk-management strategies:
   - Avoid.
   - Mitigate.
   - Transfer.
2. Define security controls to mitigate risks.
   - Policies and procedures.
   - Technical controls.
   - Human controls.
3. Develop an implementation plan and assign responsibility for each control.

Security Policy Development Life Cycle
Step 4. Measure Implementation

1. Identify gaps in existing measurement methods.
2. Identify new measures to replace or complement existing measures.
3. Obtain management approval of new measures.
4. Collect measurements regularly.

Security Policy Development Life Cycle
Step 5. Policy Recommendation

1. Identify existing policy that addresses the identified risks.
2. Write proposed security policy that addresses these risks.
3. Recommend security policy for adoption by management.

Example Policy Development

Step		Action
1	Self-Assessment	Identify risks and existing policies and controls.
2	Risk Assessment	Identify the level of risk and priorities.
3	Risk Mitigation	List the control(s) your agency management will use to mitigate this risk.
4	Performance Measurement	List the measures your agency management will use to assess the effectiveness of this control.
5	Policy Recommendation	Make a recommendation to management regarding security policy to adopt.

Example Policy Development
Step 1. Self-Assessment

Identified risk:

“Personnel who have not undergone thorough background checks have access to information systems.”

Example Policy Development
Step 2. Risk Assessment

- Likelihood.
  - » It is very likely that an individual with a criminal record has been or will be given access to protected information.
- Severity.
  - » It would have medium impact on the business if an individual with a criminal record gained access to protected information.
- Area of impact.
  - » The agency could be subject to liability.
- Level of tolerance.
  - » Management is not willing to assume this risk.

Example Policy Development
Step 3. Risk Mitigation

"Conduct background investigations internally using our own employees. Training will be provided by a neighboring agency that conducts its own investigations. Access to a public information database will be purchased and a policy will be written to ensure proper background investigations are conducted."

Example Policy Development
Step 4. Performance Measurement

"The personnel division commander will conduct an annual audit of the background investigations section to ensure it is complying with the agency policy."

Example Policy Development
Step 5. Policy Recommendation

- This policy will affect all new employees who have been given a conditional offer of hire.
- A thorough background check of the new hire will be completed prior to the person’s assignment to a position that will give them access to the agency’s system.
- Under the direction of the commander in charge of administration, the detectives assigned background investigations will conduct a thorough background check according to the procedures developed at the direction of the commander and approved by the chief of the agency.
- Due to the sensitive nature of the background check process, only the commander in charge of administration, the assistant chief of the agency, the agency chief, and the agency counsel will be allowed to review the completed background information.
- Any new hires failing to complete the background process will be promptly notified of their status and referred to the personnel section.

Security Frameworks

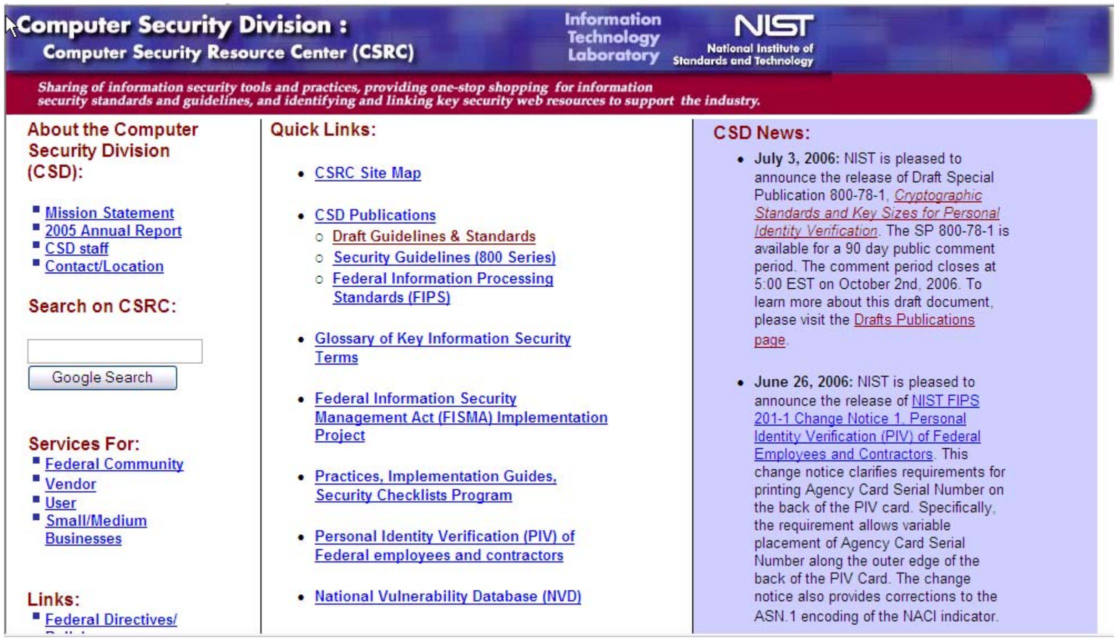
- NIST.
  - » U.S. standards.
  - » Security guidelines for federal systems.

- ISO 17799.
  - » Internationally recognized standard.
  - » Applicable to both public and private sector implementations.

Security Frameworks
NIST

The Federal Information Security Management Act (FISMA) of 2002 requires the National Institute of Standards and Technology (NIST) to ensure that they are:

> "…developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards…"



Computer Security Division :
Computer Security Resource Center (CSRC)
Information Technology Laboratory
NIST
National Institute of Standards and Technology

Sharing of information security tools and practices, providing one-stop shopping for information security standards and guidelines, and identifying and linking key security web resources to support the industry.

About the Computer Security Division (CSD):

- Mission Statement
- 2005 Annual Report
- CSD staff
- Contact/Location

Search on CSRC:

Services For:

- Federal Community
- Vendor
- User
- Small/Medium Businesses

Links:

- Federal Directives/

Quick Links:

- CSRC Site Map
- CSD Publications
  - Draft Guidelines & Standards
  - Security Guidelines (800 Series)
  - Federal Information Processing Standards (FIPS)
- Glossary of Key Information Security Terms
- Federal Information Security Management Act (FISMA) Implementation Project
- Practices, Implementation Guides, Security Checklists Program
- Personal Identity Verification (PIV) of Federal employees and contractors
- National Vulnerability Database (NVD)

CSD News:

- **July 3, 2006:** NIST is pleased to announce the release of Draft Special Publication 800-78-1, *Cryptographic Standards and Key Sizes for Personal Identity Verification*. The SP 800-78-1 is available for a 90 day public comment period. The comment period closes at 5:00 EST on October 2nd, 2006. To learn more about this draft document, please visit the Drafts Publications page.
- **June 26, 2006:** NIST is pleased to announce the release of NIST FIPS 201-1 Change Notice 1, Personal Identity Verification (PIV) of Federal Employees and Contractors. This change notice clarifies requirements for printing Agency Card Serial Number on the back of the PIV card. Specifically, the requirement allows variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card. The change notice also provides corrections to the ASN.1 encoding of the NACI indicator.

FIPS-Federal Information Processing Standards

Security Frameworks
ISO 17799

- Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

Security Guidance for Justice Systems

- CJIS Security Policy
  - » Mandatory for systems that connect to NCIC.
- SEARCH – Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies, *A Guide for Executives, Managers, and Technologists*
  - » Guidance for state and local law enforcement.
- Applying Security Practices to Justice Information Sharing (JIS)
  - » Guidance for state and local JIS.
  - » Includes both wired and wireless versions.

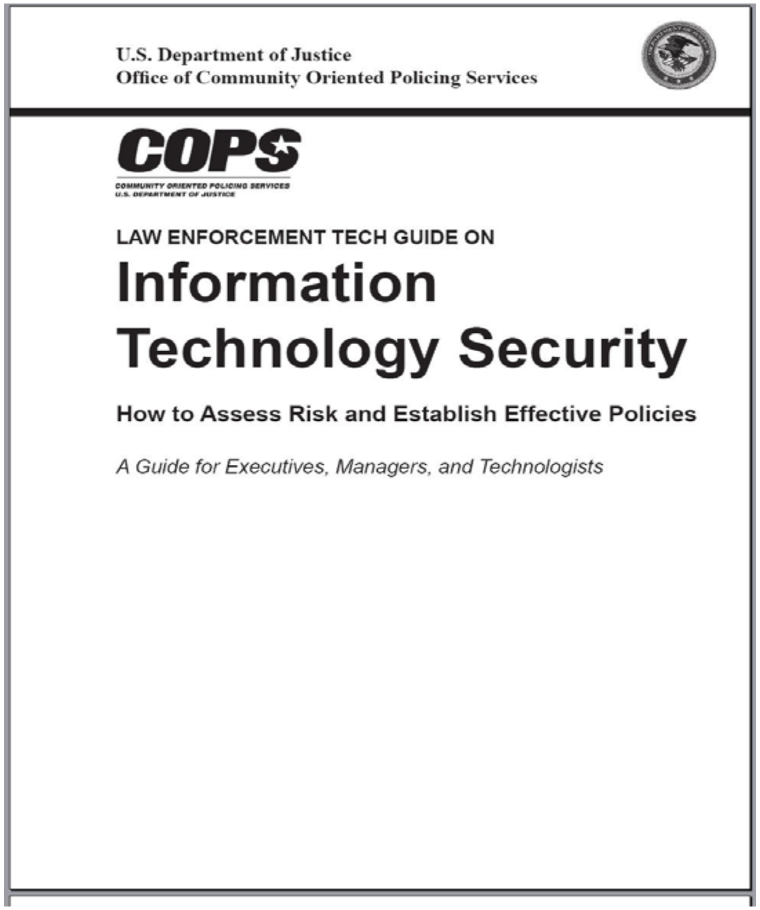
Security Guidance for Justice Systems
CJIS Security Policy

- Roles and Responsibilities
- Security Enforcement
- Computer Security Incident Response Capability
- ORI Authorizations and User Agreements
- Technical Security
- Use and Dissemination of Criminal History Record Information and NCIC Hot File Information
- Audits of CJIS Information Systems
- APPENDICES
  - » A – Forms
  - » B – Web Sites
  - » C – Guideline Documents
  - » D – Other Resources

Security Guidance for Justice Systems

Law Enforcement Tech Guide and Tool (continued)

- Designed to give decision makers a better understanding of the importance of the self and risk-assessment process.
- Distill established guidance from NIST.
- Give decision makers an IT security and risk-assessment tool that can help them through a complicated process.



U.S. Department of Justice
Office of Community Oriented Policing Services

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

LAW ENFORCEMENT TECH GUIDE ON

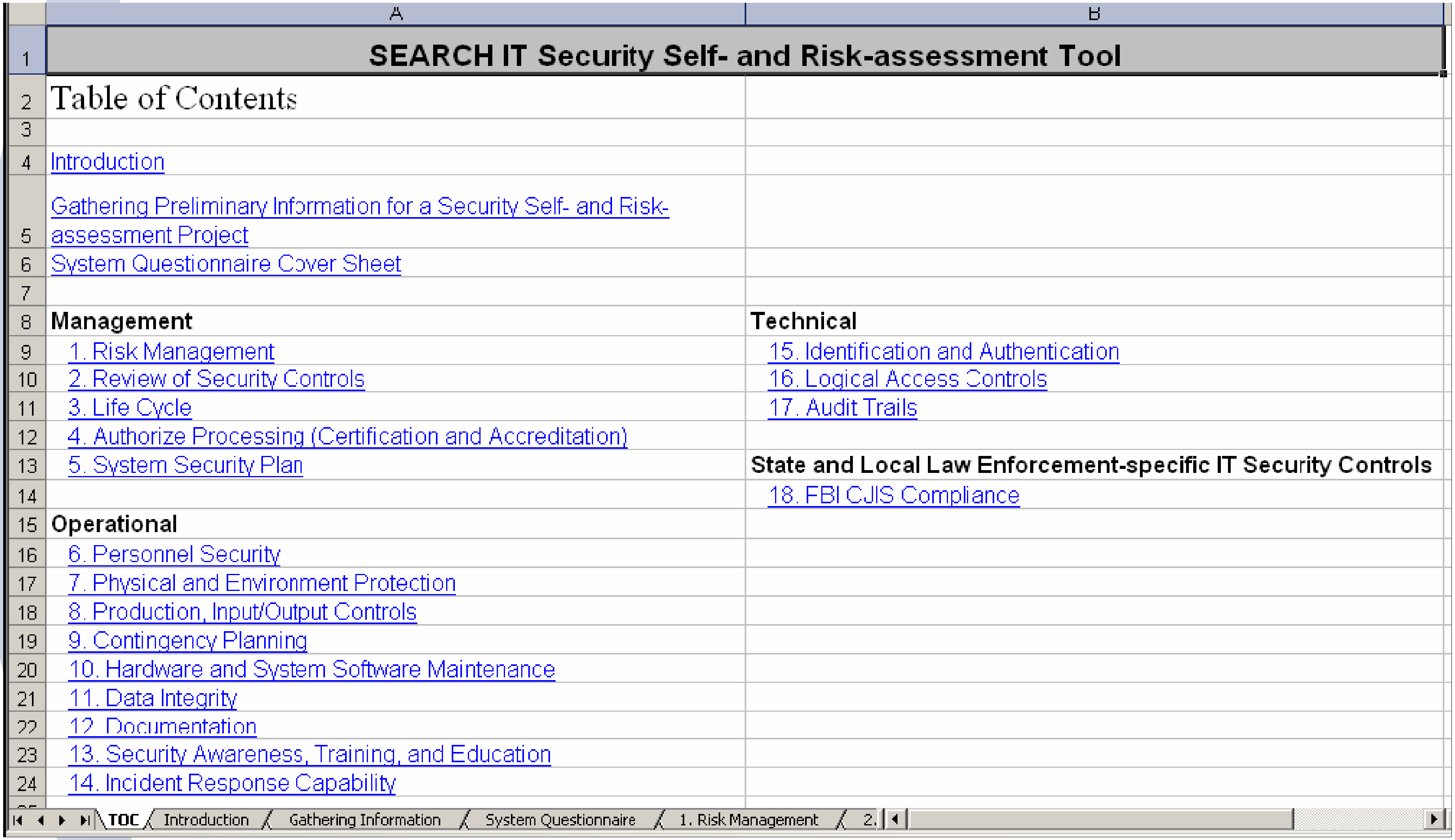
Information Technology Security

How to Assess Risk and Establish Effective Policies

A Guide for Executives, Managers, and Technologists

Security Guidance for Justice Systems

Law Enforcement Tech Guide and Tool (continued)

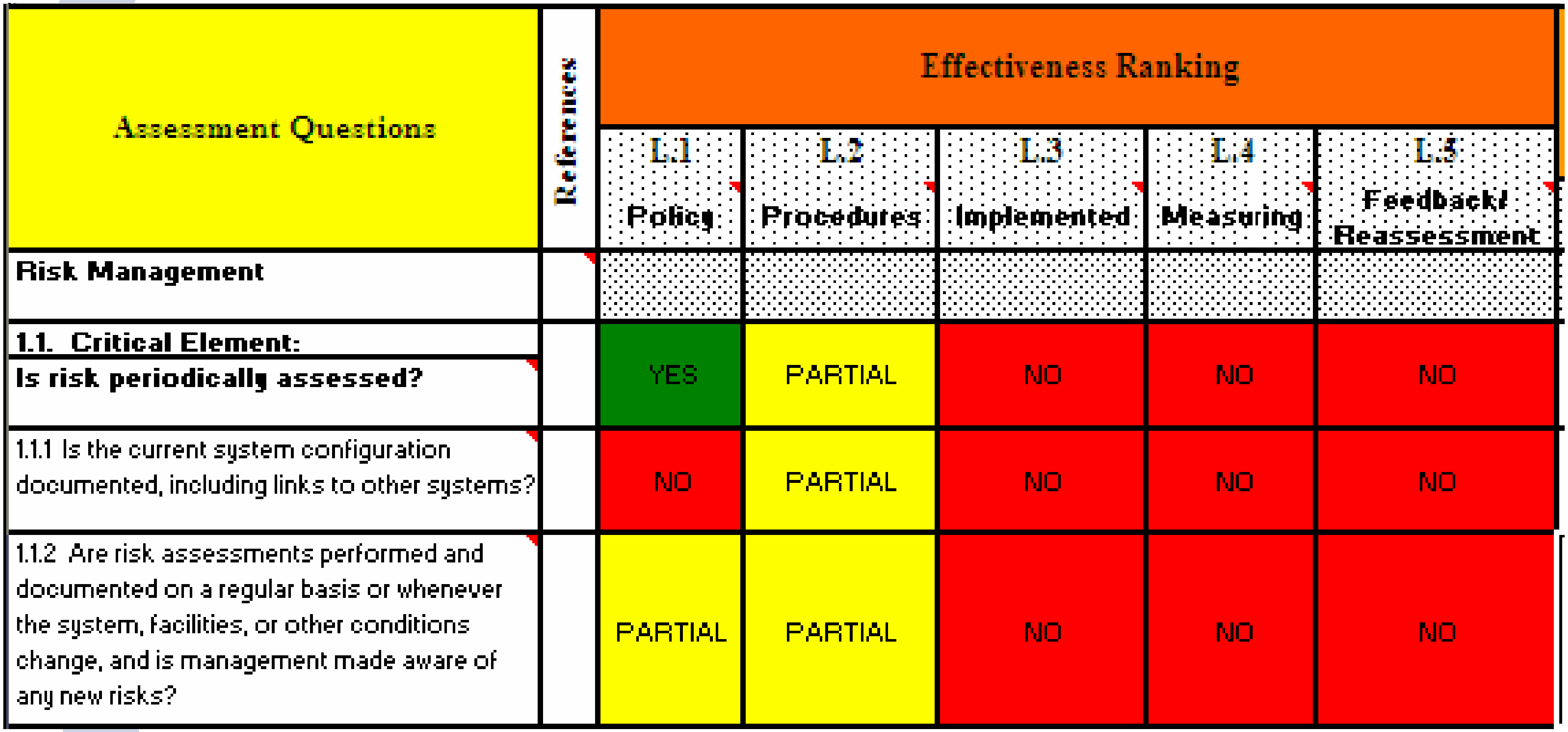


	A	B
1	**SEARCH IT Security Self- and Risk-assessment Tool**	
2	Table of Contents	
3		
4	Introduction	
5	Gathering Preliminary Information for a Security Self- and Risk-assessment Project	
6	System Questionnaire Cover Sheet	
7		
8	**Management**	**Technical**
9	1. Risk Management	15. Identification and Authentication
10	2. Review of Security Controls	16. Logical Access Controls
11	3. Life Cycle	17. Audit Trails
12	4. Authorize Processing (Certification and Accreditation)	
13	5. System Security Plan	**State and Local Law Enforcement-specific IT Security Controls**
14		18. FBI CJIS Compliance
15	**Operational**	
16	6. Personnel Security	
17	7. Physical and Environment Protection	
18	8. Production, Input/Output Controls	
19	9. Contingency Planning	
20	10. Hardware and System Software Maintenance	
21	11. Data Integrity	
22	12. Documentation	
23	13. Security Awareness, Training, and Education	
24	14. Incident Response Capability	

Security Guidance for Justice Systems

Law Enforcement Tech Guide and Tool (continued)

Self-Assessment

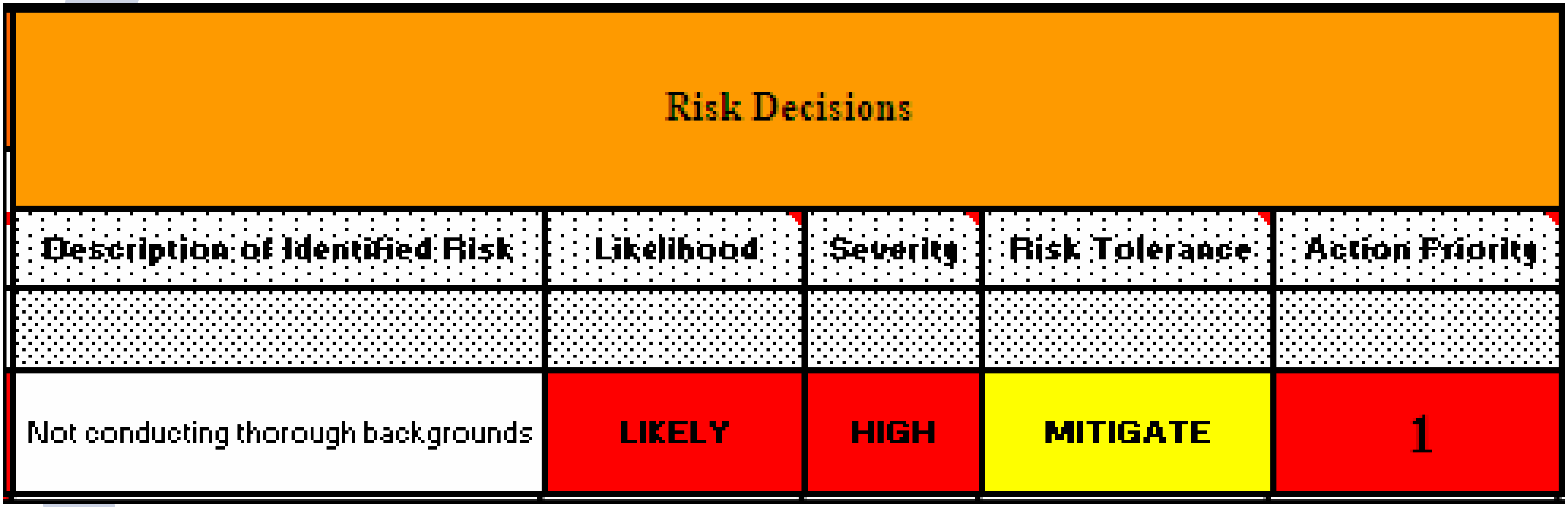


Assessment Questions	References	Effectiveness Ranking				
		L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Measuring	L.5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**		YES	PARTIAL	NO	NO	NO
1.1.1 Is the current system configuration documented, including links to other systems?		NO	PARTIAL	NO	NO	NO
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?		PARTIAL	PARTIAL	NO	NO	NO

Security Guidance for Justice Systems

Law Enforcement Tech Guide and Tool (continued)

Risk Assessment



Risk Decisions				
Description of Identified Risk	Likelihood	Severity	Risk Tolerance	Action Priority
Not conducting thorough backgrounds	LIKELY	HIGH	MITIGATE	1

Security Guidance for Justice Systems
Applying Security Practices to JIS

- Support.
  - Governance.
  - Physical security.
  - Personnel security screening.
  - Separation of duties.
- Prevention.
  - Identification and authentication.
  - Authorization and access control.
  - Data integrity.
  - Data classification.
  - Change management.
  - Public access, privacy, and confidentiality.
  - Firewalls, VPNs, and other network safeguards.
- Detection and recovery.
  - Intrusion detection systems.
  - Critical incident response.
  - Attack detection and prevention.
  - Security auditing.
  - Risk management.
  - Disaster recovery and business continuity.

Example Policies and Procedures

- State of Minnesota Office of Enterprise Technology

  www.state.mn.us/portal/mn/jsp/home.do?agency=OETweb

- SANS

- GLOBAL Privacy and Information Quality

References

- SANS Security Policy Project and Primer.
  - » http://www.sans.org/resources/policies/.
- NIST Computer Security Special Publications.
  - » http://csrc.nist.gov/publications/nistpubs/.
- ISO 17799.
  - » http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441.
- CJIS Security Policy.
  - » Contact your state CJIS systems officer.
- Law Enforcement Tech Guide for IT Security Policies.
  - » http://www.cops.usdoj.gov/mime/open.pdf?item=512.
- Applying Security Practices to JIS.
  - » http://it.ojp.gov/topic.jsp?topic_id=58.
- Privacy Policy Development Guide and Implementation Templates.
  - » http://it.ojp.gov/topic.jsp?topic_id=55.

Questions for You

- What are your key security issues?
- What policies are you creating now?
- What frameworks, guidance documents, or tools are you using?
- What additional guidance or tools do you need?

Questions & Answers