

Information Technology Services Division

Security Assessment Questionnaire <i>Policy Rescinded July 1, 2005</i>	Document Number: ITGS0013
	Effective Date: 3/25/04 <i>Rescinded July 1, 2005</i>
	Published By: Information Technology Services Division

1.0 Purpose

This questionnaire is to be used by Agency officials to measure the current status of their security programs and controls in order to make informed judgments and investments.

2.0 Scope

Missouri State Agencies should annually complete the security assessment questionnaire in the first quarter of the calendar year and submit a copy of it to the Information Technology Services Division.

Do not distribute the questionnaire based on public request. This assessment is exempt from public disclosure based on RSMo Chapter 610, Section 610.021 Sub-Paragraph (20) which states:

610.021 Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body.

3.0 Background

The National Institute of Standards and Technology (NIST) has issued a Vulnerability Self-Assessment Guide for Information Technology Systems. This assessment has been distilled into a few key questions in each of three areas: Management Controls, Operational Controls, and Technical Controls. This questionnaire is designed to provide a cost-effective technique for agency officials to determine the current status of their information security programs,

mitigate identified weaknesses and where necessary, establish a target for improvement.

4.0 References

- 4.1 Executive Orders
 - 03-26 Authorizes the OIT to coordinate information technology initiatives for the state
http://sos.mo.gov/library/reference/orders/2003/eo03_026.asp
 - 02-15 Establishes the Missouri Security Council
http://www.sos.mo.gov/library/reference/orders/2002/eo02_015.asp
 - 03-25 Designates OIT as principle forum to improve cyber security policies and procedures
http://sos.mo.gov/library/reference/orders/2003/eo03_025.asp
- 4.2 Cyber Security Committee Report
 - February 7, 2003
 - June 3, 2003
- 4.3 March 26, 2003 ITAB Meeting Minutes
http://oit.mo.gov/itab/minutes/ab_03_03.pdf
- 4.4 Security Assessment letter of Recommendation to CIO
<http://oit.mo.gov/SecurityPolicyRecommendation.pdf>

5.0 Revision History

Date	Description of Change
03/25/2004	Initial Standard Published
02/18/2005	Changed due date from the first quarter of the Fiscal Year to the first quarter of the calendar year.
06/08/2005	Policy Rescinded – Letter of recommendation from Tom Stokes and RD Porter to Dan Ross, CIO recommending Governance Standards ITGS0011 and ITGS0013 be rescinded. The Vulnerability Assessment Methodology and the Security Assessment Questionnaire will be replaced by a three step process outlined in the letter of recommendation. This letter may be accessed by clicking on the link in paragraph 4.4 above.

6.0 Definitions

Refer to ITAB Security Glossary and Acronyms:

<http://siipc.mo.gov/PortalVB/DesktopDefault.aspx?tabindex=7&tabid=8>

7.0 Distribution

This document will be distributed to the following:

Cabinet Members
Elected Officials
State Court Administrator
Senate Administrator
Chief Clerk

8.0 Inquiries

Direct inquiries about this document to:
Information Technology Services Division
Truman Building, Room 280
301 W. High Street
Jefferson City, MO 65102
Voice: 573-526-7741
FAX: 573-526-0132

Security Assessment Questionnaire

Agency Name: _____ Date of Evaluation: _____

System Name, Title, and Unique Identifier: _____

Check one: Major Application General Support System Entire Agency

Name(s) of Assessors: _____

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

Responses to this questionnaire are exempt from public disclosure based on RSMo Chapter 610, Section 610.021 Sub-Paragraph (20) which states:

610.021 Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body.

MANAGEMENT CONTROLS

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Risk Management								
1.1 Is risk periodically assessed?								
1.2. Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

2. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Review of Security Controls								
2.1. Have the security controls of the system and interconnected systems been reviewed?								
2.2. Does management ensure that corrective actions are effectively implemented?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

3. Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Life Cycle								
3.1. Has a system development life cycle methodology been developed?								
3.2. Are changes controlled as programs progress through testing to final approval?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

4. Authorize Processing (Certification & Accreditation)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Authorize Processing								
4.1. Has the system been certified/recertified and authorized to process (accredited)?								
4.2. Is the system operating on an interim authority to process in accordance with specified agency procedures?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

5. System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
System security plan								
5.1. Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.2. Is the plan kept current?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

OPERATIONAL CONTROLS

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Personnel Security								
6.1. Are duties separated to ensure least privilege and individual accountability?								
6.2. Is appropriate background screening for assigned positions completed prior to granting access?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

7. Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Is there user support?								
8.2. Are there media controls?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

8. Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
7.1. Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.2. Is data protected from interception?								
7.3. Are mobile and portable systems protected?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

9. Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization’s critical functions operating in the event of disruptions, large and small.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Contingency Planning								
9.1. Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.2. Has a comprehensive contingency plan been developed and documented?								
9.3. Are tested contingency/disaster recovery plans in place?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

10. Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance								
10.1. Is access limited to system software and hardware?								
10.2. Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.3. Are systems managed to reduce vulnerabilities?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

11. Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Data Integrity								
11.1. Is virus detection and elimination software installed and activated?								
11.2. Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

12. Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system document and formalize the system’s security controls. When answering whether there are procedures for each control objective, the question should be phrased “are there procedures for ensuring the documentation is obtained and maintained.”

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Documentation								
12.1. Is there sufficient documentation that explains how software/hardware is to be used?								
12.2. Are there formal security and operational procedures documented?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

13. Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education								
13.1. Have employees received adequate training to fulfill their security responsibilities?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

14. Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Incident Response Capability								
14.1. Is there a capability to provide help to users when a security incident occurs in the system?								
14.2. Is incident related information shared with appropriate organizations?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

TECHNICAL CONTROLS

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Identification and Authentication								
15.1. Are users individually authenticated via passwords, tokens, or other devices?								
15.2. Are access controls enforcing segregation of duties?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Logical Access Controls								
16.1. Do the logical access controls restrict users to authorized transactions and functions?								
16.2. Are there logical controls over network access?								
16.3. If the public accesses system, are controls implemented to protect the integrity of the application and the confidence of the public?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES:

17. Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.

Specific Control Objectives and Techniques	L.1	L.2	L.3	L.4	L.5	Risk Based Decision Made	Comments	Initials
Audit Trails								
17.1. Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								

Level 1 = Policy, L.2 = Procedures, L.3 = Implemented, L.4 = Tested, L.5 = Integrated

NOTES: