

Information Technology (IT) Risk Assessment Standard

Issue Date: June 1, 2004

Effective Date: June 1, 2004

Number: HHSS-2004-002-B

1.0 Purpose

This standard defines guidelines used to perform Information Technology (IT) Risk Assessments (RA) on HHSS IT hardware, software, or business processes using IT resources. RA is an audit of HHSS IT resources to determine potential security risks and vulnerabilities and to initiate an appropriate remediation plan for unacceptable risks identified.

The RA is intended to evaluate the security risks for HHSS resources to safeguard the information collected and used by HHSS and to protect HHSS's ability to access IT resources in order to carryout it's mission to the citizens of the State of Nebraska.

2.0 Scope

RA may be conducted on any IT resource, to include applications, servers, networks, and any process or procedure by which these systems are used, administered, and/or maintained.

This standard covers all:

- computer hardware, software applications, and communication devices owned or supported by HHSS
- business processes employing IT resources
- outside entities that have signed a *Third Party Agreement* with HHSS

This standard sets guidelines for conducting a RA and includes:

- when a RA will be performed
- what IT resources will be audited as part of the RA
- how the RA will be performed
- who will be involved in the RA

3.0 Standard

This standard provides guidelines for compliance to the IT Security Policy No. HHSS-2004-002.

The HHSS IT Security Administrator or designated team using the guidelines defined in this document will be responsible for conducting RA audits.

RA audits will be conducted on a predefined schedule and will focus on specific vulnerabilities, safeguards, and remediation action.

The RA audit will be a coordinated effort between the IT Security Administrator and the HHSS entity responsible for the IT resource under review. It will be the joint responsibility of the HHSS entity and HHSS Information Systems & Technology (IS&T) to take appropriate action to address security risks and vulnerabilities and to insure they meet all HHSS Policies.

3.1 RA Schedule.

- 3.1.1 Scheduled RA audit(s) for large IT resources will be completed in the first quarter of each year as part of the HHSS IT Plan update process.

Large IT resources include:

HHSS Network Infrastructure (LAN/WAN)
HHSS Server Operations and Desktops
N-FOCUS Application
CHARTS Application
MMIS Application
AVITAR Application

- 3.1.2 RA audits will be completed for large IT resources when any significant change is made to that resource.

- 3.1.3 Medium and small IT resources not listed in section 4.1.1 will have a RA audit conducted at least once every three years or when any significant change is made to the resource.

3.2 IT Resources to be audited.

- 3.2.1 For each RA audit, the HHSS IT Security Administrator will provide worksheets listing the assets to be audited. RA may cover physical and/or electronic risks and safeguards.

3.3 RA Procedure

- 3.3.1 The IT Security Administrator will provide RA worksheets to collect information pertaining to the resource(s) being audited.

- 3.3.2 Instructions on completing the RA worksheets will be provided to each participant at the time the RA worksheets are distributed.

- 3.3.3 The IT Security Administrator will compile a Risk Assessment Summary Report using the information collected from the RA Worksheets. The RA Summary report will provide the following:

- A summary of the security safeguards and an evaluation of their effectiveness.
- A description of any security deficiencies that were uncovered and their potential risk to the asset reviewed.
- A description of any violation of HHSS security policies and required actions for compliance.
- A recommendation for improving safeguards.

Due to the sensitive security issues included in the report, the RA Summary Report and its contents will be considered confidential. The information contained in the report is intended for the use of the IT Security Administrator and the program area participating in the review. No information from the report may be released to any other party without written authorization of the IT Security Administrator.

- 3.3.4 Any unacceptable security risks or violations of HHSS IT Security Policies identified by the RA will require the immediate initiation of an appropriate remediation plan. This plan will be developed through the collaborative effort of the HHSS entity responsible for the IT resource, IS&T, and the IT Security Administrator. Once the remediation plan has been implemented, a follow up RA will be initiated to assess the effectiveness of the remediation plan.

3.4 RA Participants

- 3.4.1 The RA will be a joint effort between the IT Security Administrator, IS&T, and the HHSS entity responsible for the resource(s) being audited. HHSS staff, contractors and contracted

business partners are expected to cooperate fully with the RA and provide all requested information.

4.0 Enforcement

Should a violation of this IT Security Standard occur, the individual(s) who committed the violation will be personally liable for their actions or the actions taken by others due to their violation of this standard. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability. Any employee found to have violated this policy may be subject to disciplinary action, as defined in the governing policy HHSS 2004-002.

5.0 Revision History

HR Legal – 03/12/2004

CCT Approval – 05/27/2004