	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 1 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

Security Risk Management Standard

I. SCOPE

This standard applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This standard applies to all Tenet divisions, facilities, and related departments.

II. PURPOSE

Define responsibilities and steps required for implementing an Information Security Risk Management Process throughout Tenet facilities that provides a standard application of program principles while supporting flexibility of implementation at each facility. Risk Management is an important aspect of Tenet’s efforts to manage the security of information assets. It is a process in which risk is assessed and steps are taken to reduce and maintain risk at an acceptable level.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. STANDARD

Facility management is responsible for ensuring information risk management activities are performed at appropriate times for information assets under their control. Certain information security risk management decisions should be documented in the facility’s Information Security Control Exceptions Book.


The documents produced to support risk management activities are *CONFIDENTIAL* and shall be protected as such.

A. Information Risk Management Components

Information risk management is comprised of two major activities; risk assessment and risk mitigation. Documentation of risk decisions is very important to this process.

1. *Risk Assessment*

Facility and information asset managers shall perform risk assessments that include consideration of the following elements of risk management:

	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 2 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

- a) Information asset valuation;
- b) The magnitude of harm that may result from loss, misuse, unauthorized access, unavailability, or alteration of information assets;
- c) Threats and vulnerabilities;
- d) The likelihood of occurrence of threats; and
- e) The effectiveness of proposed or current safeguards.

2. *Risk Mitigation*

Risk mitigation controls shall be selected consistent with the risk assessment results and shall consider the potential cost of harm to the assets versus the cost of the control.

B. Information Risk Management Process


The Information Risk Management Process consists of the following steps:

1. Determine the risk assessment boundary, scope, and methodology.

The boundary defines the system or parts of a system or systems that will be considered in the assessment. Factors determining the boundary may include custodianship, management or control. The scope describes the depth to which analysis will be performed within the boundary. Factors that shall be considered in determining the scope of assessment include:

- a) The phase of the life cycle the system is in;
- b) The relative importance of the system under examination;
- c) The magnitude and types of changes the system has undergone since the last risk assessment; and
- d) The size of the system under consideration.

Facility Management shall utilize the boundary and scope information to select an appropriate methodology. Methodologies may be:

	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 3 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

- a) Formal or informal.
- b) Quantitative or qualitative.
- c) High or low level.
- d) Detailed or simplified.
- e) A combination depending on the system, Users, and environment.

2. Gather data.

- a) Identify and value the information assets.

Management shall determine asset value based on the impact and consequence to the organization (including replacement cost and the effect on the organization if the asset is disclosed, modified, destroyed or misused). The purpose of the valuation is to define assets in terms of their importance or criticality.

- b) Identify threats and vulnerabilities.


A threat is an entity or event that can harm the information asset under consideration. Vulnerabilities are weaknesses in existing safeguards or the absence of safeguards that allow threats to occur. Management shall assess threats not only in terms of their existence, but also in terms of the vulnerabilities of existing safeguards.

- c) Identify the likelihood of occurrence of particular threats and/or vulnerabilities.

As threats and/or vulnerabilities are identified and analyzed, the likelihood of their occurrence shall be estimated.

3. Perform Risk Analysis.

Management shall analyze the data obtained in the steps above. Risk analysis involves assignment of a risk factor based on the particular threat identified earlier, the value of the asset, and the likelihood of a threat occurring. The outcome of the

	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 4 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

analysis indicates the degree of risk associated with the specific assets and provides a basis for the selection of safeguards and risk mitigation decisions.

4. Select appropriate safeguards.

Selection of security services and mechanisms entails relating an appropriate security service to the threats/vulnerabilities defined and then selecting the most appropriate security mechanism. In selecting an appropriate security mechanism, management shall consider such factors as:

- a) Cost of the control service/mechanism;
- b) Organizational policy, legislation and regulation;
- c) Safety, reliability and quality requirements;
- d) System performance requirements;
- e) Life cycle costs of security measures;
- f) Technical requirements; and
- g) Cultural constraints.


5. Accept residual risk.

Management is responsible for reviewing the proposed security controls, determining that the operation of the information assets being assessed is/will be acceptable, and approving their implementation.

6. Implement safeguards/controls and monitor effectiveness.

Management is responsible for effectively implementing and then reviewing safeguards periodically in accordance with the evolution of the system throughout the system's life cycle.

Reviews of security controls and system assessments shall be performed when there are changes to the system and in accordance with the change control procedures described in Change Control Procedure No. 8.2.1.


	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 5 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

C. Risk Documentation

The information asset risk assessment and management process should be sufficiently documented and retained for review by the Corporate Privacy/Security Office and other parties as appropriate (template documentation book attached as Addendum A). Where risk decisions are made that involve the facility not complying with Tenet's Information Security Policies and Procedures, these control exceptions should be documented in the facility's Information Security Control Exceptions Book (see Addendum B).

1. The Information Security Control Exceptions Book should be used to document:
 - a) Requirements of the Information Security Policies and Procedures that the facility cannot meet, or for which a compensating control has been implemented; and
 - b) Instances where the alternative selected within the Information Security Policies and Procedures requires the facility to document that control. In such cases, the facility would typically be choosing a less restrictive option when given a number of alternatives, and is required to document this decision in accordance with that policy.

2. At a minimum, the Information Security Control Exceptions Book should contain the:
 - a) Date the control exception was documented;
 - b) Name of the individual documenting the control exception;
 - c) Effective date of the control exception;
 - d) Information Security Policy, Standard, or Procedure that required the control;
 - e) Description of the control as required in policy;
 - f) Description of how the control was fully/partially/not met, including a description of compensating controls that were implemented; and
 - g) Reason(s) why the control could not be implemented in accordance with the Information Security Policies and Procedures.

	Information Security Policies and Procedures	No. COMP-Sec 7.1.0
	Title: SECURITY RISK MANAGEMENT STANDARD	Page: 6 of 8
		Revised Date: 04/21/06
		Original Date: 03/09/01

3. The Information Security Control Exceptions Book should be retained for review by the Corporate Privacy/Security Office and other parties as appropriate.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Security Administration Policy No. 7.0.0.
- Change Control Procedure No. 8.2.1.
- Tenet Administrative Policies and Procedures No. 3.3 “Facility Risk Management Reporting Requirements”.

Additional information on risk assessment and risk management approaches can be found in the NIST Computer Security Handbook, the NIST Risk Management Framework, and the RCMP Computer Security Handbook.

