Information Security Risk Assessment

1. Purpose

The purpose of this policy is to establish requirements for reviewing Information Systems (IS) to identify risks and recommend appropriate security controls to mitigate identified risks to an acceptable and reasonable level.

Information Security Risk Management includes all of the activities that an organization carries out in order to manage and control risk. It is the process that includes evaluating risk, the impact to the University IS, risk decisions, risk treatment plans, monitoring of risk and the steps taken to mitigate risk to an acceptable level.

The risk assessment process should enable OUHSC Business Units to make well-informed decisions to protect the business unit and the University from unacceptable technology risks.

2. Policy

Information Security Risk Assessments –
Business Units must request an Information Security Risk Assessment from OUHSC Information Technology (IT) for all IS receiving, storing, processing, and/or transmitting University data, according to the following triggers:

1. Upon purchase of a new technology product.
2. Upon renewal of an existing technology product and according to the IS and Data Classification
    a. Category A – Every two (2) years
    b. Category B – Every three (3) years
    c. Category C – Every three (3) years
    d. Category D – As needed
3. Upon modification of the following:
    a. IS use-case
    b. IS interfaces with other systems and data
    c. IS method of interface
    d. IS and Data classification

All OUHSC technology purchases must undergo an Information Security Risk Assessment[1].

When submitting an Information Security Risk Assessment request, Business Units must provide, at a minimum, a complete description of the product, its functions and capabilities, interfaces with other systems and data, the method of interface, and all inputs and outputs.

If any of the above change, at any time, the Information Security Risk Assessment request must be updated to reflect these changes and be resubmitted to OUHSC IT.

The following requirements must be met as part of the IS Risk Assessment process:

4. All data and IS, Cloud Service Providers, and third-party web development efforts must have roles assigned by the Business Unit in accordance with the Information Security Roles and Responsibilities Policy.

[1] NOTE The Information Security Risk Assessment does not constitute an approval or authorization to purchase the reviewed product. State of Oklahoma and University purchasing rules still apply.

5. All data and IS, Cloud Service Providers, and third-party web development efforts must be classified in accordance with the IS and Data Classification Policy.
6. All new data and IS, Cloud Service Providers, and third-party web development efforts classified as Category A will undergo a solution architecture review by OUHSC IT.
7. All IS and data, Cloud Service Providers, and third-party web development efforts classified as Category A must have undergone an initial and will undergo a thorough assessment of security controls every two (2) years.
8. All IS and data, Cloud Service Providers, and third-party web development efforts, classified as Category B must undergo an assessment of security controls every three (3) years.

Risk Profiles

Upon completion of a Information Security Risk Assessment, where risks are identified, IT Security will supply the requesting Business Unit with a Risk Profile Summary. This document provides the following information:

- Name and Description of IS
- Vendor Details
- Business Unit Roles and Responsibilities
- Business Unit
- Classification
- Business Associate Agreement Requirement
- Next Scheduled Review Date
- Associated System of Record number
- Requestor Contact Details
- Identified Risks, Risk Level, and associated recommended Risk Actions

OUHSC IT's risk recommendation actions in response to the Risk Profile must be addressed in a timely manner, as evidenced by documentation supplied to Information Security. Recommendations are based upon policy or regulatory requirements or security best practices. In many cases the recommendations are designed to provide solutions that will sufficiently mitigate the identified risks to an acceptable level. However, some risks may not be entirely mitigated and will require a business decision and leadership acceptance of that risk OR a decision to avoid that risk by not using the Product.

Risk Decisions and Actions

IT Security recognizes the following risk decisions:

Risk Mitigation

Risk mitigation is a decision to systematically reduce the extent of exposure or the likelihood that a vulnerability could be exploited, by implementing administrative, operational or technical safeguards. Risk mitigation decisions are made by the IS Sponsor, IS Owner or IS Administrator.

Risk Acceptance

Risk acceptance is a decision where the cost of accepting the risk is acceptable because the risk level is insufficient to justify the cost of mitigating. High level risks that are accepted by the IS Sponsor should be reviewed by the college or Business Unit head and may be referred to the IT Risk Subcommittee of the Information Security Review Board.

Risk Avoidance

Risk avoidance is the decision to: (1) take steps to remove the risk, (2) engage in an alternate activity, or (3) otherwise end the specific exposure. Risk avoidance decisions can be made by the IS Sponsor or IS Owner.

Risk Transfer

Risk transfer is the decision to transfer responsibility of the risk to another entity. Risk Transfer decisions can be made by the IS Sponsor.

Risk Tracking

OUHSC maintains all identified risks in the OUHSC Risk Register. IS Owners and IS Administrators with assigned risk mitigation responsibilities, must provide IT Security with monthly updates regarding the status and current state of open risks.

Training
All Business Unit IS Owners, IS Administrators and Business Managers must undergo annual, and more frequently as needed, training to provide guidance on complying with the *Information Security Risk Assessment Policy.*

3. Definitions

Business Unit: As applied to the University, a Business Unit may be a department, a program or college, a support service or central administration function within the University. A business unit may extend across multiple locations.

Information System (IS): A system and/or service, which typically include: hardware, software, data, applications and communications that support an operational role or accomplish a specific objective. *Note – An IS can reside on premise or off-premise.

IS Sponsor: an individual responsible for providing the necessary funding and support for the IS Owner and Administrator to perform their roles and responsibilities. The IS Sponsor provides executive oversight of data and/or IS and assumes responsibility for policy compliance for the IS under his or her control. The IS Sponsor reviews high level risk items of the IS and makes risk treatment decisions for the Business Unit.

IS Owner: the individual responsible for maintaining a current inventory of all ISs within the business unit, classifying the data and IS, establishing rules for disclosing and authorizing access to IS data, conducting access control reviews, coordinating with campus IT to conduct risk assessments and serving as the escalation contact for the IS Administrator.

IS Owner Representative*:* An individual designated by the IS Owner to act on his or her behalf.

IS Administrator: An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device or system (e.g., system administrator or network administrator). At OUHSC the IS administrator role is typically performed by the business unit Tier One. The IS administrator role may be performed through an agreement between the business unit and Campus IT.

For additional Information Technology definitions, see Information Technology Policy Definitions Document at http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf

4. Scope

This policy is applicable to OU Health Sciences Center and OU Health Care Components.

5. Regulatory References

- HIPAA Standards for Safeguarding Customer Information
- Section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act")
- FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act]
- Payment Card Industry Data Security Standard

6. Authorization

This policy is authorized and approved by the OUHSC Dean's Council and Senior Vice President and Provost, and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University

may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

7. Review Frequency

This policy is scheduled to be reviewed, updated and modified as necessary, annually.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
03/20/2017	1.0	OUHSC IT	Baseline Version Changed title from Product Review to Information System Risk Assessment
07/07/2017	1.1	OUHSC IT	Rebranded as Information Security Risk Assessment

8.2 Approval History

Version	Date	Approved By
1.1	08/08/2017	Information Security Review Board (ISRB)
1.1	10/10/2017	OUHSC Dean's Council and Senior Vice President and Provost

8.3 Review History

Date	Reviewed By
08/08/2017	ISRB