Risk Assessment Briefing

University Information Security

Background

Risks vary across the University and over time, due to different activities, or changes in technology and regulation. The current Institutional Risk Profile illustrates risks from the Board of Regents' perspective.



Overview

The objective of the University Information Security Risk Management (ISRM) program is to support informed decisions about data privacy and data security risks across the University through iterative and practical risk analysis.

The program provides a continuous, common approach to:

- identify and safeguard private data as regulated (including FERPA, FISMA, HIPAA and PCI-DSS)
- prioritize realistic and actionable security efforts in the University environment
- remove barriers to innovation, while maintaining a responsible level of security for the University's assets.

Components of the ISRM include:

Component	Description
Gap analysis	a self-help process for units to compare current practices against security controls required by the University's information security standards (Appendices)
Private Data Inventory	periodic survey of the prevalence of private data which the University is obligated to protect
Risk assessments	detailed analysis of systems/processes/units that are considered Medium-to-High risk to identify potential risks and treatment options.

.

Risk Assessment process

Generally, risk assessments focus on processes that involve Private-Restricted and Private-Highly Restricted data, or are otherwise mission-critical for the enterprise. They typically do not include financial or governance controls.

The scope of each assessment is determined collaboratively with the unit. Phases of a risk assessment include:

Phase	1	2	3	4
	Context & Scope	Risk Assessment	Risk Treatment	Risk Acceptance
Outcome	determine scope and draft engagement letter	identify risks and assign Impact and Likelihood	determine options and draft a treatment plan outline	accept the risks/treatment decisions
Involving	IT director/equivalent and Executive (Dean/VP)	Point of Contact and Subject Matter Experts	Point of Contact and Subject Matter Experts	IT director/equivalent and Executive (Dean/VP)
Typical time commitment	1 to 2 meetings	a questionnaire followed by meetings*	1 to 2 meetings	1 meeting

** UIS recommends scheduling working meetings as a block if possible.*

Components of a risk assessment include:

Phase	Component	Description
Scope	**Process flow diagram**	also known as a swim lane diagram, to identify and prioritize processes
	Scope questionnaire	a brief set of questions to identify characteristics of systems/processes
	Planned initiatives	may include discussion of new processes/technology/services, e.g. cloud
Assessment	**Controls questionnaire**	a detailed set of process and technology questions based on ISO 27002/5, CSF or HIPAA/NIST 800-53 as appropriate
	Recent activity review	recent Audit findings, information security incidents or breach reports.

Schedule and preparation

Completion time for a risk assessment will depend on the scope and availability of key Subject Matter Experts (SMEs).

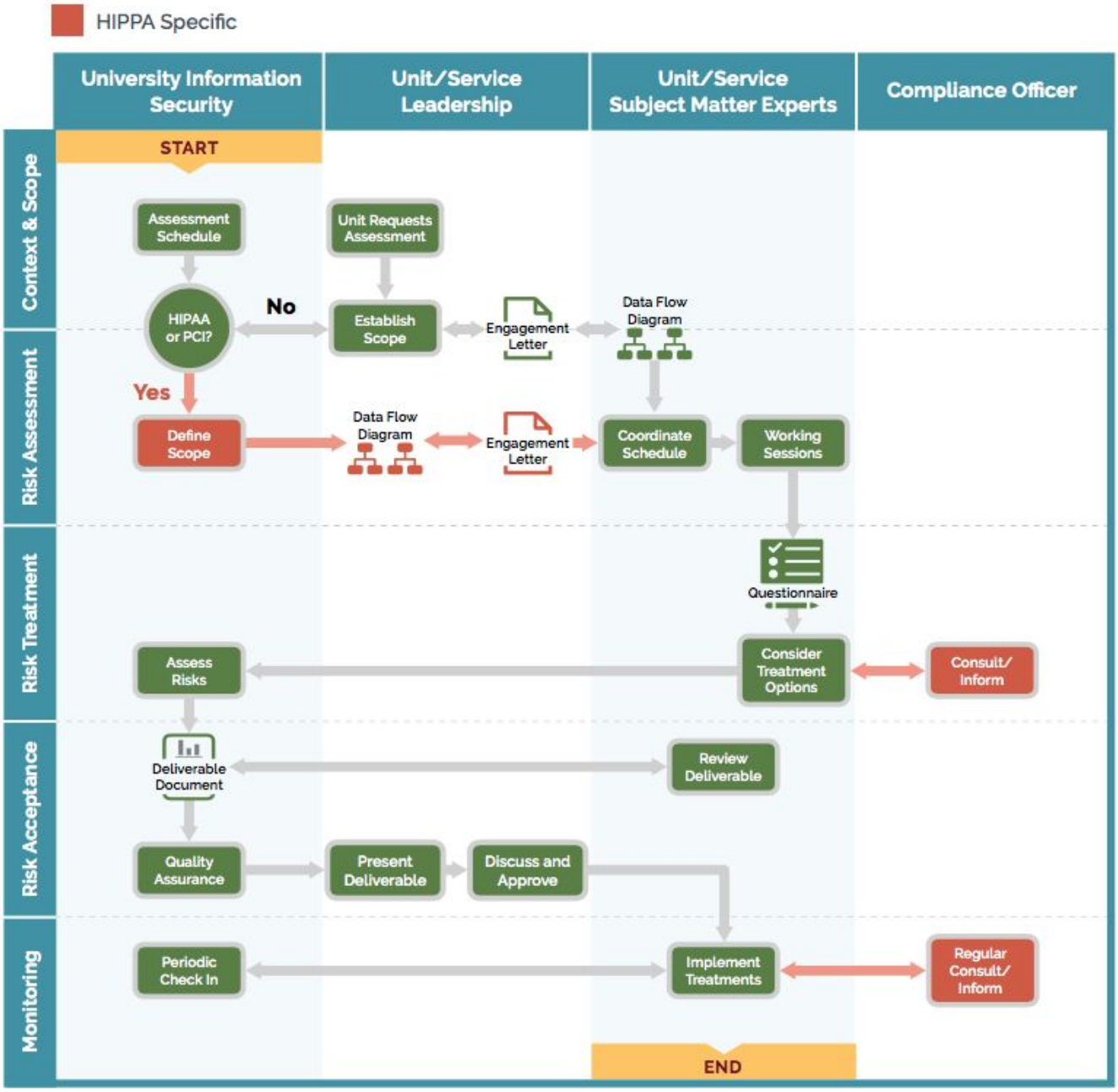
Units can prepare for a risk assessment by:

- identifying a Point-of-Contact and Subject Matter Experts
- confirming the availability of the Subject Matter Experts and communicating expectations
- identifying current or planned initiatives that may be relevant and should be considered
- reviewing the Data Security Classification and Information Security Risk Management policies
- conducting a gap analysis of current practices against University information security standards can expedite a risk assessment, but is not a requirement of the risk assessment.

Questions
please contact:
infosecurity@umn.edu

or directly:
conor@umn.edu
mandy@umn.edu
nshawver@umn.edu
phillips@umn.edu
laube004@umn.edu

Process flow for risk assessments



Risk Impact and Likelihood Criteria

UIS' risk evaluation is aligned with the current University Compliance Reporting Standards (9/10/14) so that risks are compared and assigned the correct decision-making level for risk treatment consistently across the enterprise.

Once risks have been evaluated (scored), they should be managed appropriately based on business need:

- similar risks may have different Impacts or Likelihood for different departments or units and therefore different treatment plans decided at the unit level
- a risk that is common to many areas may require a collaborative treatment plan decided at a higher level.

Impact

The following criteria are defined by the Compliance Reporting Standards with additions defined by UIS (in italics):

Impact	Criteria
High impact	• Death or serious bodily injury due to unsafe University activity • More than $1,000,000 likely at issue • Likely disqualification or major penalty from program (e.g. NCAA, research sponsor, etc.) • Potential widespread and serious legal problem • President, Chancellor, Vice President, Vice Chancellor, Dean, Head Coach, Athletic Director credibly accused of misconduct • Requirement to report incident to an outside regulatory body with a reasonable likelihood of substantial financial or programmatic penalty • Incidents highly likely to be accompanied by substantial negative publicity • Circumstance is reasonably likely to result in a serious criminal charge against a University employee for University-related conduct • Matters of significance requiring immediate escalation to the General Counsel • Any other circumstance that meets compliance area-specific criteria for "high impact" • *University mission (research, instruction) prevented for more than 72 hours.*
Medium impact	• "Near miss" death or serious injury due to unsafe U activities • Between $250,000 and $1,000,000 likely at issue • University manager or supervisor credibly accused of misconduct • Reasonable likelihood of a penalty from an outside body (i.e. research sponsor, NCAA, MPCA, etc.) that is not substantial and is not anticipated to interfere with University programs in the judgment of the responsible reporting party and responsible Vice President • Potential for substantial negative publicity • Otherwise in the judgment of responsible reporting party and Vice President is of significance to be reported to the Executive Oversight Compliance Committee as

	part of a periodic report ● Meets customized area-specific criteria for "medium" impact ● *University mission (research, instruction) prevented for 24 to 72 hours.*
Low impact	● Minor safety concern or accident ● Less than $250,000 likely at issue ● Isolated minor legal or policy violations (violation of work rules, general HR violations, financial policies, HR policies, petty theft, etc.) or a series of minor violations that may reflect a problematic trend ● *University mission (research, instruction) prevented for less than 24 hours.*

Likelihood

The following criteria are defined by UIS. In some circumstances, other factors may need to be considered.

Likelihood	**Criteria**
High likelihood	● A related incident has occurred within the last 2 years ● An incident is highly likely (>50%) to occur within the next 2 years.
Medium likelihood	● A related incident has occurred within the last 2 - 5 years ● An incident is moderately likely (>25%) to occur within the next 5 years.
Low likelihood	● A related incident has NOT occurred at the department or unit within the last 5 years ● An incident may occur within the next 5 years.
Other factors	*If past experience or statistical information is not available at the dept/unit/University, consider breach/vulnerability reports and best practices for:* ● *peer institutions* ● *industry* ● *community/public/media security awareness.*