Policy	Risk Management Policy
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	June 4, 2025
Reviewed	May 14, 2026; June 24, 2026
Approved by	Provost and Vice President of Academic Affairs
Version	26.1

RISK MANAGEMENT POLICY

PURPOSE

Shepherd University's Risk Management Policy is intended to establish a framework for identifying, evaluating, monitoring, and responding to risks to university systems and data, as well as support strategic decision-making.

Risk decisions are made all the time, sometimes without deep consideration and may even be based upon intuition. A formalized risk management process can uncover risks that were not anticipated, resolve funding conflicts, and help enhance executive buy-in to security improvements.

POLICY

Risk Identification

IT staff will conduct a yearly risk assessment using the CIS CSAT model. This assessment will provide the basis for the IT risk assessment. In some cases, additional risks may be identified through alternate means.

Risk Assessment

Risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation. It is a large part of the overall risk management process; many of the steps described in this framework focus on the assessment process.

Led by the CIO, IT staff will assess the identified risks based on likelihood and potential impact.

The formula that we will use is Risk = Likelihood x Impact. This means that the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event.

The components of the risk formula are:

Likelihood

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors.

The model that we use will have 3 values for Likelihood:

3 - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. (Being the highest)

2 - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

1 - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. (Being the lowest)

Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

The model that we use will have 3 values for Impact:

3 (High) - Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury. (Being the highest)

2 (Medium) - Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.

1 (Low) - Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest. (Being the lowest)

Risk

7 - 9 - If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

4 - 6 - If an observation is rated as medium risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.

1 - 3 - If an observation is described as low risk, it must be determined whether corrective actions are still required or decide to accept the risk.

Risk Prioritization and Mitigation

Risks will be prioritized, and mitigation strategies will be identified based on the risk assessment and resources available. In some cases, risk may be accepted due to the results of the assessment, limited resources, or both.

Results of the risk assessment and prioritization will be shared with upper management. This information will be used to inform decision-making relating to IT priorities for the coming year/s.

In order to assist with prioritization, 2 additional metrics are used – Cost to Remediate and Time to Remediate.

Cost to Remediate (CTR) -*Cost to Remediate* refers to the estimated financial expenditure required to fully mitigate, reduce, or eliminate a specific risk. This includes all direct and indirect costs associated with implementing controls, corrective actions, or recovery measures.

Components may include:

- Labor and personnel costs (e.g., consultants, internal teams)
- Technology or infrastructure investments (e.g., software, hardware)
- Legal or compliance costs

- Operational disruptions or downtime
- Training and change management

Time to Remediate (TTR)
Time to Remediate is the estimated duration required to implement effective mitigation or corrective actions for a given risk. This includes planning, execution, testing, and validation phases.

Factors influencing TTR:

- Complexity of the remediation effort
- Availability of resources and expertise
- Dependencies on third parties or systems
- Regulatory or procedural constraints

Mitigation Strategy
Once you identify risk, there are 4 things you can do with it.

Avoidance: To eliminate the conditions that allow the risk to be present at all, most frequently by dropping the project or the task.

Acceptance: To acknowledge the risk's existence, but to take no preemptive action to resolve it, except for the possible development of contingency plans should the risk event come to pass.

Mitigation: To minimize the probability of a risk's occurrence or the impact of the risk should it occur.

Deflection: To transfer the risk (in whole or part) to another organization, individual, or entity. (Outsource)

SCOPE OF AFFECTED PARTIES

This policy applies to all users such as students, faculty, and staff of Shepherd University accessing Shepherd University information assets.

ROLES & RESPONSIBILITIES

CIO/CISO – Information Privacy Officers

- Oversee and administer this policy.
- Provide authorization and directions to IT Services staff in accordance with this policy.
- Coordinate with IT staff to develop policies and procedures to address risks

IT Services Staff

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Participate in yearly risk assessment

RELATED

IT Information Security & Privacy Policy