Purpose
Arizona State University is committed to continually improving information technology in accordance with business needs, industry standards, best practices and legal requirements. The risk management program is designed to facilitate the achievement of ASU’s strategic objectives. We regularly review and rank our risks so we can mitigate risk proactively. This document outlines our approach for identifying and analyzing risk areas and taking corrective action in an effort to provide the most strategic, available and secure IT environment possible.

Applicability
This Standard applies to all Departments using ASU’s computing, internet, and communications resources, including its Component Units.

Standard
This document describes the process for conducting IT Risk Assessments at ASU. Both centralized and decentralized functions are reviewed periodically. ASU’s IT Risk Assessment cycle is a continuous improvement plan for assisting the business units with implementing University information security guidelines. The cycle is outlined as follows:

1. Identify areas of IT risk across ASU.
2. Identify corrective measures to be taken.
3. Follow-up review of corrective measure implementation.
4. Enforcement of corrective action measures where necessary.

ASU conducts IT risks assessments periodically, typically annually. The risk assessment process can include surveys filled out by each business unit, and/or reports generated from a set of identified data elements with results specific to each business unit. This document defines each key role in the assessment process along with procedural guidelines for:

- developing the Risk Assessment
- distributing the survey
- analyzing and distributing responses
- developing and conducting the corrective action plan

Roles
Information Security Office
ASU’s Information Security Office is responsible for the IT Risk Assessment process. Responsibilities include developing the IT Risk assessment, communicating plans, and conducting the IT Risk Assessments. This also includes analyzing information, disseminating the results and encouraging response activities within each department or unit.

Executive Leadership
ASU’s CISO and broader team work with the Information Security Task Force and other members of ASU leadership (https://www.asu.edu/about/leadership), as appropriate, to identify both the appropriate survey respondents and/or report reviewers for each department (business unit) and assemble corrective action working groups. These teams provide communication and endorsement of the IT Risk Assessment process to each department or units. Ultimately, each department or unit is responsible for managing and reducing their risk.

Corrective Action Workgroup
The Corrective Action Workgroup addresses the top risk areas across the University. This workgroup reviews those items requiring additional action; confirms University-wide or departmental accountability for specific risk areas, recommends specific corrective actions; and builds communication materials for areas to be addressed through consultation, documentation, presentations, or training materials. Participants of the Corrective Action Workgroup may vary depending on the risk areas identified in a given Risk Assessment.
IT Risk Assessment Survey Respondents/Report Reviewers

The IT Risk Assessment survey respondents or report reviewers are department liaisons designated by the appropriate Dean or Department Head (Accountable Administrator). A list of unit technical and business contacts is maintained and used for distributing the assessments.

Conducting the IT Risk Assessment via Survey

Survey mechanism

Self-reported survey questions are derived from industry standards including but not limited to ISO 27001, COBIT 5, COSO, CIS CSC, and the NIST Cybersecurity Framework. The questionnaire may include open-ended questions for respondent feedback on the survey mechanism and issues not covered in the multiple-choice questions.

Review of survey questions

Survey questions are reviewed before distribution to gauge their effectiveness and identify the range of possible responses to each question. The Information Security Office will assign appropriate ratings for each possible response.

The review process may include facilitated small group discussions, presentations with extended Q&A sessions, and/or requests for feedback by electronic mail. The survey typically emphasizes questions that were indicated as high risk areas University-wide in previous assessments. The survey may include benchmarks, as appropriate, with other universities undertaking similar efforts.

Distribution

The survey is distributed to all high level academic and administrative units of the University as identified by ASU’s Senior Leadership, modeling ASU’s leadership page. The senior IT and business administrators are the survey respondents for each high level department or unit. The survey is distributed electronically and includes the endorsement of ASU’s executive team.

Communication

Effective communication is important. Prior to distribution of the survey, the Risk Assessment is communicated to all units involved and to senior University management and should be forwarded from there to each of their respective department(s).

Conducting the IT Risk Assessment via Data Driven Reports

Report mechanism

As we have matured the IT Risk Assessment process, we frequently leverage data-driven IT Risk Assessment reports where the data elements included generally align with basic IT controls and identified corrective actions. Reports are unit-specific.

Communication

Report formats are communicated to all department/units and to senior University management.

Analysis and Dissemination of Results

The Risk Assessment is analyzed at the departmental level and University-wide. The analysis frequently includes elements such as Impact, Likelihood, Combined Risk Value, and Risk Rating for categorizing each response area. The final report provides an overview of IT risk areas of concern and can be compared to previous reports to measure improvements over time.

For each survey returned, the ISO summarizes the results and provides an overview of risk areas that may require attention.
Results are shared with department heads, University executive leadership, and shared with the Corrective Action Planning Workgroup as needed. The Chief Information Security Officer (CISO) or delegate meets with each Dean or Department Head periodically, generally annually, to discuss initial results and overall plans to reduce risk.

**Corrective Action**
The top risk areas identified in the Risk Assessment results are addressed through a University Corrective Action Plan developed in response to the aggregate Risk Assessment results. General guidelines are provided to allow adequate time for departmental implementation before the follow-up Risk Assessment.

**Convene Corrective Action Planning Workgroup**
On review of the Risk Assessment results, the Information Security Office presents the findings to the Corrective Action Workgroup. Depending on the findings, members may be added to the group to address specific knowledge or expertise.

**Develop Corrective Action Plan**
The Corrective Action Planning Workgroup reviews the top risk areas, confirms risk ranking, and develops or confirms the plan to address those areas University-wide. This recommended plan is sent to members of the ASU executive team up to and including the Provost and CFO for confirmation.

**Conduct Corrective Action Plan**
The Corrective Action Plan is made available and publicized to all appropriate business units for departmental implementation. The plan should be communicated and promoted in a variety of ways. Recommended communication mechanisms include:

- publication on the Information Security Office's Website, getprotected.asu.edu
- orientation sessions presented in person to business unit representatives
- electronic mail from senior management including endorsement of the process
- individual department meetings are scheduled with the Chief Information Security Officer (CISO) and each Dean or Department Head to review results and discuss the department's overall plans to reduce risk.

**Violations and Enforcement**
Each business unit is responsible for taking corrective action based on its Risk Assessment results and the Corrective Action Plan. The effectiveness of University and departmental corrective actions is measured in subsequent Risk Assessments. The Risk Assessment Team, including the University Technology Office, the Information Security Office and the Corrective Action Workgroup may escalate any issues or concerns through the appropriate management channels up to the executive level.

**Resources**
Executive IT Risk Review Dashboard: [https://analytics.asu.edu/group/executive-it-risk-review](https://analytics.asu.edu/group/executive-it-risk-review)
IT Risk Assessment Summaries: [https://getprotected.asu.edu/services/risk-assessment](https://getprotected.asu.edu/services/risk-assessment)

**Standard Revision**
This Standard is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at infosec@asu.edu.