**Risk Assessment (RA) Standard**

Figure - Indiana University Seal—only approved university-wide policies may use the seal

# T-12

**About This Standard**

**Effective Date:**

*In review*

**Date of Last Review/Update:**

*4/7/23 draft*

**Responsible University Office:**

*University Information Policy Office*

**Responsible University Administrator:**

***Office of the Vice President for Information Technology and Chief Information Officer***

**Policy Contact:**

***University Information Security Office -*** *uiso@iu.edu*

## Scope

This standard supports [Policy IT-12 (Security of Information Technology Resources)](https://policies.iu.edu/policies/it-12-security-it-resources/index.html) and applies to all Indiana University information technology resources, regardless of whether those resources are managed by the university or provisioned from third parties on behalf of the university, and to all users of those resources regardless of affiliation.

## Objectives

The key objective of this standard is to ensure that institutional information technology risk is assessed, prioritized, and managed on an ongoing basis. The operation of information systems and the processing, transmission, and storage of institutional information can significantly affect the financial, operational, reputational, regulatory, and/or safety risks to the institution, to institutional assets, and to individuals.

## Standard

The following tables detail baseline security controls for risk assessment that are to be applied to a particular information technology resource based on its [security categorization](https://informationsecurity.iu.edu/policies/standards/it12-security-categorization-procedure.docx). Select controls as applicable. For example, all controls may not apply to every system component or technology, or to situations governed by specific regulations.

|  |  |
| --- | --- |
| **Control:** | **Security Categorization** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Units must: 1. Categorize their information technology resources using the [IT-12 Security Categorization Procedure](https://informationsecurity.iu.edu/policies/standards/it12-security-categorization-procedure.docx).2. Update documentation of security categorizations at least annually and as needed to reflect changes. |
| **Notes**   | See:* [Policy DM-01 (Management of Institutional Data)](https://policies.iu.edu/policies/dm-01-management-institutional-data/index.html)
* <https://datamanagement.iu.edu/types-of-data/classifications.php>
 |
| **NIST Cross Reference**   | RA-2 |

|  |  |
| --- | --- |
| **Control:** | **Risk Assessment** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Units must assess IT risk every two years or upon major changes or updates to systems. Units must:1. Identify systems to assess.
2. Select standard controls to assess.
3. Collect and analyze system information (documentation, system purpose, and importance to IU's mission).
4. Identify and document risks and gaps.
5. Plan, propose, and prioritize mitigations.
6. The senior executive officer of a department or school must accept mitigation plans, and/or accept those risks for which mitigation is not planned.
7. Make a risk assessment report with documented plan and acceptance available to the UISO.
8. Implement planned mitigations.
 |
| **Notes**   | Units can substantially satisfy this control by: 1. Engaging quarterly with their UISO assigned security analyst, and
2. Implementing security controls that align with the IT-12 standards, and as recommended by the UISO.

Although security risk assessment must be performed every two years, it need not be done all at once; it may be done in small, iterative, priority-based cycles. |
| **NIST Cross Reference**   | RA-3 |

|  |  |
| --- | --- |
| **Control:** | **Vulnerability Scanning** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | * Units must enroll IT resources outside the IU Data Center in the university vulnerability scanner for regularly scheduled scans. Scans must occur at least monthly, and after significant changes to the IT resource.
* Scan reports must be reviewed, and vulnerability mitigations must be prioritized by vulnerability criticality. Critical vulnerabilities must be mitigated within five business days, either by applying compensating controls or by patching.
* A record of vulnerability dispositions must be created and maintained. This record and the scan reports should be made available to unit staff responsible for risk assessment. It must include:
	+ Vulnerabilities identified;
	+ Disposition: “patched”, “compensating control(s) applied”, “not mitigated”, or “false positive”;
	+ If applicable: a.) What compensating controls were applied, or b.) reason for not mitigating; and
	+ Date.
* Notify: Units must notify uiso@iu.edu if they elect not to mitigate a vulnerability.
 |
| **Notes**   | * In Qualys, the university vulnerability scanning tool, level 4 and 5 vulnerabilities are to be considered “critical” vulnerabilities in terms of prioritization.
* See [About vulnerability scanners](https://kb.iu.edu/d/bgzt).
* Systems running in the data center are scanned weekly.
* Report update frequency is set by units.
 |
| **NIST Cross Reference**   | RA-5 |

## Definitions

**Standard** - Standards (like procedures) support policy by further describing specific implementation details (i.e., the "how"). A standard can be thought of as an extension of policy that articulates the rules, mechanisms, technical or procedural requirements, or specifications to be used in carrying out/complying with policy. Standards, along with procedures, promote a consistent approach to following policy. Standards make policies more practically meaningful and effective. Standards are definitional and clarifying in nature, specifying the minimums necessary to meet policy objectives. Because standards directly support policies, compliance with standards is nonoptional and failure to follow standards may result in sanctions imposed by the appropriate university office.

## Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved, this could include the Office of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the Vice President and General Counsel, and/or appropriate law enforcement agencies. See [Policy IT-02 (Misuse and Abuse of Information Technology Resources)](http://policies.iu.edu/policies/categories/information-it/it/IT-02.shtml) for more details.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

## Additional Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| ***Subject*** | **Contact** | **Phone** | **Email** |
| Questions about the standard | University Information Security Office | 812-855-UISO (8476) | uiso@iu.edu  |
| Vulnerability scanning | USIO’s scanner admin | NA | scanner-admin@iu.edu |

## History

April 7, 2023 revised after stakeholder feedback

February 12, 2022 draft for review

## Related Information