

RIT Information Security Office

Information Security Plan

Draft updated January 14, 2009

This document provides an overview of the RIT Information Security Office strategy for providing information assurance at RIT. It is a living document and will be subject to updates.

RIT Information Security Mission

The Information Security Office provides leadership to the RIT community in safeguarding the confidentiality, integrity and availability of RIT information and computing assets. The Information Security Office provides strategy definition, risk assessment, standards development, communication & training, and investigation of threats & incidents.

Business Context:

Like other universities, RIT faces a number of challenges due to its heterogeneous and decentralized information technology services, the need to support three sometimes overlapping user groups (faculty, staff, and students), and the need to provide secure access to information at all times.

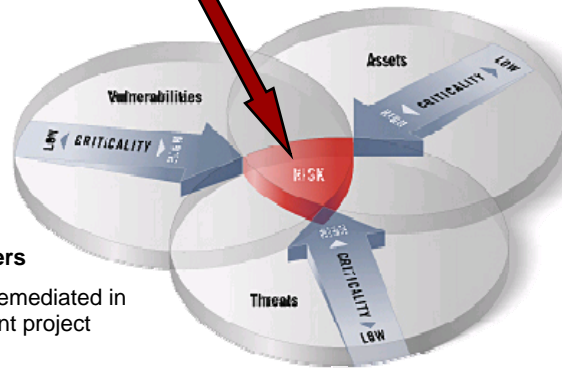
Key factors/drivers in managing information security at RIT include risk tolerance, asset protection, vulnerability management, and threat mitigation. The diagram below illustrates their interrelationships.

**What is our risk tolerance?
Compliance vs High Assurance**

- Numerous state breach, federal and international laws
- High assurance security

Asset Drivers

- Private information and increasing research
- Highly decentralized IT with proliferation of applications
- Diverse workforce and users including vendors and students



Vulnerability Drivers

- PI was not fully remediated in SSN Replacement project
- Open network
- Application vulnerabilities
- Varying levels of staff and user training

Threat Drivers

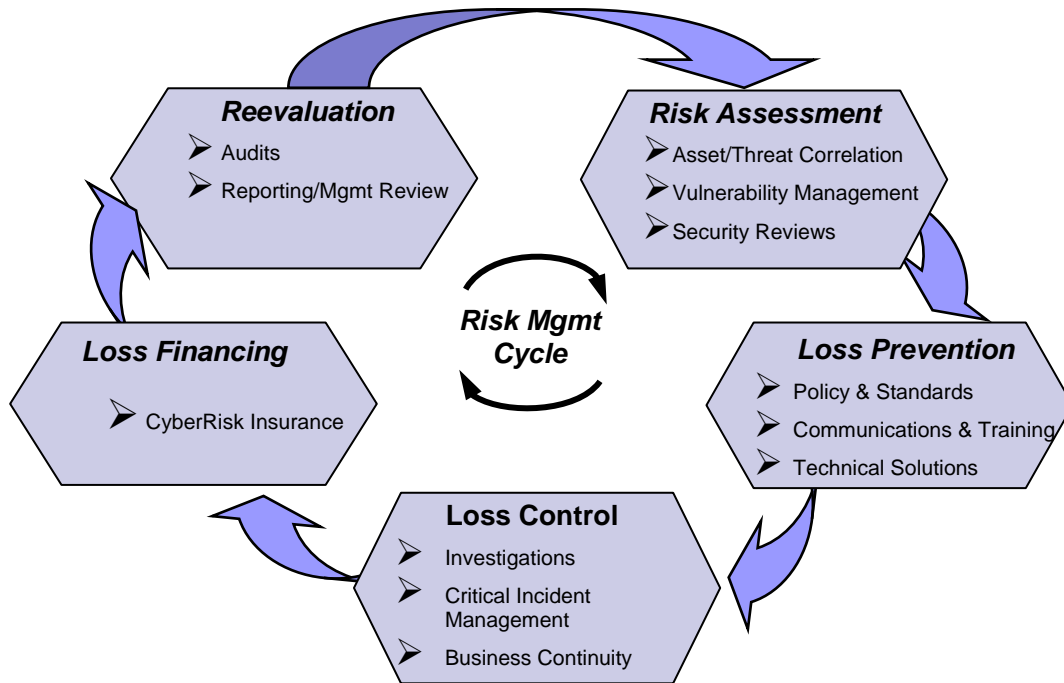
Profit Potential > Perceived Loss

- Compromises
- Stolen / lost devices
- Stolen / lost media
- Human error

Adapted from DHS/NYS CSIC

Risk Management Model

As part of RIT Global Risk Management Services, the RIT Information Security Office views its role through a risk management framework. Our focus areas are Risk Assessment, Loss Prevention, and Loss Control. We partner with Global Risk Management for Loss Financing, and Institute Audit, Compliance, and Advisement (IACA) conducts audits of RIT security controls implementation in the constituent organizations within RIT.



Risk Assessment

- Asset/Threat Correlation
- Vulnerability Management
- Security Reviews

Private Information Management @ RIT

Private Information Management @ RIT is a program where the RIT Information Security Office in cooperation with various campus support organizations scans computers and drives connected to the RIT network to determine if they contain private information. If private information is found, the computer owner is notified.

The goals of the program are to identify and reduce the amount of private information contained on computers that connect to the RIT network. This reduction will help

safeguard the RIT community against identity theft and will help RIT comply with relevant state and federal laws.

Vulnerability Management and Measurement

- ISO has access to enterprise results
 - Operating System and Applications
- Web: PHP issues, SQL Injection, Cross-Site Scripting
- Allow each IT organization to access their results

Security Reviews

Security reviews are conducted to manage potential info security exposures created in systems (hardware, applications, web).

Loss Prevention

Loss prevention at RIT includes Policy and Standards, Communications and Training, and Technical Solutions.

Policy and Standards

Policy describes the strategy and direction of RIT's approach to a particular issue; in this instance information security. All policies are grouped together in the Institute Policies and Procedures Manual.

Standards creation is led by the ISO. The standards are drafted by core teams of subject matter and business experts, and vetted through representatives of the RIT community. These standards help the RIT community implement the Information Security Policy.

The Information Security Policy (and standards) apply to the entire RIT community, including students, faculty, staff, external business associates, and volunteers.

Policies

The follow policies pertain to information security at RIT.

- [Information Security Policy \(C8.1\)](#)
- [Information Security Policy Plain English Guide](#)
- [Information Security Policy Cross Reference \(provides references to legislation and other information\)](#)
- [RIT Code of Conduct for Computer & Network Use \(C8.2\)](#)
- [RIT Code of Conduct for Computer & Network Use Plain English Guide](#)
- [RIT Privacy Policy \(C7\)](#)

Standards

Each standard has its own page that provides the standard, a corresponding Plain English Guide for the average computer user (where applicable), and additional resources to assist in compliance with the standard.

The following standards are now in effect at RIT:

- [Desktop & Portable Computer Security Standard](#)
- [Password Standard](#)
- [Computer Incident Handling Standard](#)
- [Server Security Standard](#)
- [Network Security Standard](#)
- [Information Access & Protection Standard](#)
- [Portable Media Security Standard](#)
- [Web Standard](#)

The following standards are currently in the standards creation process and not yet in effect:

- Services and Systems Development & Acquisitions Standard (sets requirements for acquisition and deployment of all systems, services, and applications at RIT)

Communications and Training

Communications

- Support Policies & Standards
 - Plain English Guides, Checklists, and Job aids help operationalize standards
- Provide additional communications through Website / Facebook page
- Issue Alerts & Advisories
- Host information security speakers

Training

Students

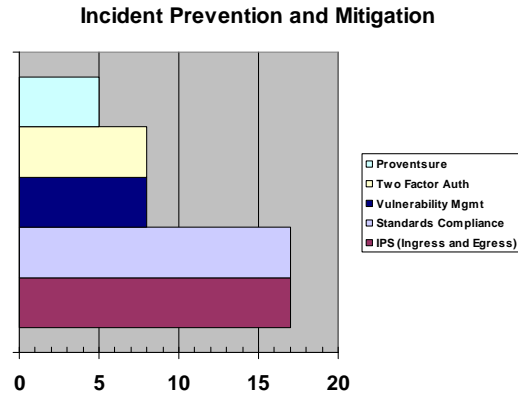
- Engage each entering class at orientation (extended to 90 minute sessions)
- Engage existing students through targeted ISO programming

Faculty/Staff

- Provide Digital Self Defense courses (Online and Instructor-led)
- Engage new faculty/staff at orientations
- Promote technical training for systems/network administrators

Technical Security Solutions

- Priority technical solutions identified by ISO team
 - Degausser & CD Shredders
 - Laptop encryption
 - Proventsure (PI) Scanner
 - Vulnerability Scanning Software
 - Two factor authentication
 - Intrusion Prevention System (IPS) – not yet approved
- Note: ISO strongly supported Desk Configuration Management for ITS



- ISO met with reps from FAST and ITS (TSS/CSS)
 - Each organization had different priorities based on:
 - existing infrastructure
 - computing environment managed (homogeneous vs. heterogeneous)
 - available resources

Technical Security Solutions (Resources)

Capital Budgeting

- ISO leads in identifying and advancing funding request for capital to purchase enterprise technical security solutions

Evaluation

- In partnership with key technical support organizations leads in a cross-enterprise evaluation of technical solutions

Implementation

- Key technical support organizations purchase and implement software as enterprise, scaleable services.

May take several years for delivery of enterprise, scaleable delivery

- Some departments are permitted to pursue independent solutions as guided by standards.

Loss Control

Incident Handling & Investigations

- Investigations have increased to consume nearly 1 FTE.
- Critical Incident Management/Business Continuity
- Managers remain accountable for development of Business Continuity Planning for their areas.
- ISO will leverage processes developed by Business Continuity Office for:
 - Technical inventory (servers, other hardware)
 - Understanding dependencies of business processes to specific technology to develop DR plans

Loss Financing

- AIG Policy

Reevaluation

- In order to assess standards implementation, ISO and IACA are cooperating in:
 - Developing an audit methodology
 - Hiring external audit capability
 - Serving as a technical resource
- Reporting/Management Review
 - Board Audit Committee briefings
 - Annual report

Roles and Responsibilities

Process	Information Security Office will: (and other risk mgmt functions)	ISO views IT organizations will:
Threat Monitoring	<i>Information Security Officer identifies and notifies IT staff about high priority threats</i>	<i>IT staff review ISO threat notices and interpret these for their specific environment</i>
Vulnerability Scanning	<i>Information Security Officer conducts vulnerability scanning ISO will follow up to assure high risk gaps are eliminated</i>	<i>IT staff fix vulnerabilities and conduct independent scans of their own environments</i>
Security Reviews	<i>ISO engaged in system reviews of major systems upon request</i>	<i>IT staff conduct their own security reviews or request ISO assistance</i>
Standards Process	<i>Leads standards process</i>	<i>IT staff participate in standards process as required and implement standards in their environments</i>
Communications & Training	<i>Communications Specialist implements communication strategy action items (communications, training and awareness)</i>	<i>Management and IT staff interpret communications for application in their environment (adoption of new standards, alerts/advisories)</i>

Process	Information Security Office will: (and other risk mgmt functions)	ISO views IT organizations will:
Technical Solution Evaluation & Implementation	<i>Coordinates capital budgeting requests and lead cross divisional evaluation process</i>	<i>IT staff participate in evaluation and are responsible for implementation in their environments. Enterprise scale installation/delivery through ITS project management</i>
Forensics Investigations	<i>ISO investigator leads investigations process</i>	<i>IT staff follow incident handling standard and provide necessary support</i>
Critical Incident (CI) Management & Business Continuity	<i>BC Director leads crisis management of CI's and coordinates development of business continuity and disaster recovery plans</i>	<i>IT staff develop disaster recovery and BC plans for their area</i>
Insurance	<i>Risk Management assesses risk and procures insurance coverage</i>	<i>IT staff provide information required by insurance carrier</i>
Audits	<i>IACA incorporates information security into their audits</i>	<i>IT staff respond to audit findings as required</i>
Reporting & Mgmt Review	<i>Develop reporting</i>	<i>Management review as deemed necessary</i>

Defense in Depth

Security requires a multilayered approach including standards, technical controls, and human factors.

