IT-28 Risk Mitigation Policy and Peer Review Process

Indiana University
University Information Security Office

September 12, 2017
Agenda For Today

• What is Policy IT-28?
• Policy Goals & Past Successes
• Leveraging Frameworks/Standards/Methods
• Implementing the Policy
• What is next for Policy IT-28?
• Q&A
Cyber Risk Mitigation Responsibilities, Policy IT-28; what is it?

Ongoing vigilance is maintained by a cycle of peer reviews of Unit risk mitigation strategies/efforts; a two-year cycle is expected. “Unit” describes any entity (IU and non-IU) that uses Indiana University technology resources.

Ensures that the [IU IT] community works to “vigilantly mitigate cyber security risks, maximize physical security for IT systems, and minimize unacceptable risks to IT systems and data from natural disasters (collectively, "Cyber Risks")”
So what drove IU to take on this risk assessment effort at such a large scale?

Initial efforts focused on balancing our mission and cyber risks.

Essential, distributed culture of the Academy

Growing institutional cyber risks
Small distributed risks grow into organizational risks

We think we only have about 4,000 servers. No one really knows.
So how does IU go about reducing our organizational Cyber Risks?

<table>
<thead>
<tr>
<th>Enterprise IT</th>
<th>Unit IT</th>
</tr>
</thead>
</table>
| • Operate facilities that:  
  • Maximize physical security  
  • Protect from natural disasters  
  • Minimize cyber security risks  
  • Provision an evolving set of IT infrastructure to meet common needs | • Deploy services that:  
  • Mitigate cyber security risks  
  • Maximize physical security  
  • Minimize unacceptable risks  
  • Reduce risk by adopting enterprise services |
Taking a look at a few milestones since implementing Policy IT-28

Policy
Adopted May 2013

Community Training Through April 2014

Initial Risk Mitigation Plans due May 2014

All Unit Risk Mitigation Plans Approved by June 2015

Planning for Second Round Started August 2016

Second Round Risk Mitigation Plans due March 2018

[Expected] Second Round Risk Mitigation Plans to be Accepted by June 2018

End of the first round of IT-28 peer review
What did/will IU actually accomplish with the first round of IT-28 risk assessment efforts?

2,330 Additional servers identified through IT-28 review process

33% Reduction in the number of servers outside of secure facilities

89.2% 4,614/5,171 servers will be in Secure Facilities after 1st Round
IT-28 is defined by Policy and guided by IU's Security & Privacy Program (ISPP)

- **Domain 1**: Risk Assessment and Treatment
- **Domain 2**: Policy Administration
- **Domain 3**: Organization
- **Domain 4**: Asset Management
- **Domain 5**: Human Resources
- **Domain 6**: Physical and Environmental
- **Domain 7**: Communications and Operations Management
- **Domain 8**: Identity and Access Control
- **Domain 9**: Information Systems Acquisition, Development, and Maintenance
- **Domain 10**: Incident Management
- **Domain 11**: Business Continuity Management
- **Domain 12**: Compliance

IU's Information Security and Privacy Program outlines a university-wide approach to implementing and managing information and information technology security and privacy. It describes the university's philosophies, values, and approach to safeguarding information and information technology.
Leveraging industry frameworks and standards to support local policy enables our success.

FRAMEWORKS

- Factor Analysis of Information Risk [FAIR]
  - Security states/goals influenced through **financial impact**
  - Provides a foundation to support robust risk assessment efforts

- NIST Cybersecurity Framework [CSF]
  - Managing and **prioritizing cybersecurity risks**
  - Controlling the scope of IT-28 efforts (and resources)
Functions and Categories in-scope of IT-28

**Identify**
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Protective Technology

**Protect**
- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance

**Detect**
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

**Respond**
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

**Recover**
- Recovery Planning
- Improvements
- Communications
Leveraging industry frameworks and *standards* to support local policy enables our success.

**STANDARDS**

- **NIST SP 800-53r4**, Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-171r1**, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- CIS Critical Security Controls v6.1
- Other standards/guidelines as required
Internal policy and standards have priority over external frameworks and standards

- IU Policy
  - IT-28
  - DM-02

- IU Standards
  - Information Security and Privacy Program (ISPP)
  - Protect.IU Resources

- Frameworks & Standards
  - Cybersecurity Framework
  - Factor Analysis of Information Risk
So we have a plan and some guidance, how do we actually implement IT-28?

- Plan
- Develop
- Train
- Execute
- Review
- Accept
- Improve

Timelines & Resources
- Peer Review Scope
- Documentation Tools
- Communications

Process Improvement Feedback
- Peer Review Teams Approved RM Plans
- IT Leaders Accept Recommendations
- Risk Mitigation Efforts Formalized

Peers Review Risk Mitigation Plans
- Peers Provide Strategy Recommendations

Assessment Goals
- Risk Assessment (Units)
- Risk Assessment (Review Teams)

Strategy Unit Goals
- Feedback
A new focus on operational security was introduced for the Second Round

- Supported by the NIST Cybersecurity Framework (CSF) and appropriate Special Publications (SP), a focus on Unit operational security (OS) will open discussion about five core topics of OS that peer review teams will assess:

- Highlighting operational security measures that **address common IT audit findings** is the primary reasoning behind this effort.

<table>
<thead>
<tr>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
</tr>
<tr>
<td>Configuration Management</td>
</tr>
<tr>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Security Assessment</td>
</tr>
</tbody>
</table>
There are a few core elements of IT-28; each provides a critical function

- Roles and Responsibilities (Humans)
- Documentation Instruments (Data)
- Supporting Documentation
- Guiding Framework
- Peer Review
## Nine critical roles in implementing IT-28

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>UISO Analysts</td>
<td>PSIA</td>
<td>Manage the IT-28 implementation process</td>
</tr>
<tr>
<td>IT Community Partnerships (ITCP)</td>
<td>UITS</td>
<td>Communication geared towards the IT Professional’s community will go through ITCP.</td>
</tr>
<tr>
<td>Submitters - Unit</td>
<td>Varies</td>
<td>Submitters are the individuals responsible for submitting IT-28 related documentation on behalf of their Unit(s).</td>
</tr>
<tr>
<td>Director - Unit</td>
<td>Varies</td>
<td>Director level positions are expected to be involved at the strategic level of risk mitigation and ensure that the resources required for successful implementation of the risk mitigation plan are allotted to their IT department.</td>
</tr>
<tr>
<td>Dean/VP - Unit</td>
<td>Varies</td>
<td>The highest-level leader that a Unit’s IT department reports to is the expected person to fill this role.</td>
</tr>
<tr>
<td>Review Team Leader - Peer Review Team</td>
<td>Varies</td>
<td>Those review team members with the greatest expertise, skill sets, and/or availability may be asked to be a Review Team Leader (RTL).</td>
</tr>
<tr>
<td>Peer Review Team (PRT) Members</td>
<td>Varies</td>
<td>Participate in the review of Unit risk mitigation plans in accordance with outline procedures and RTL direction.</td>
</tr>
<tr>
<td>Joint Review Action Committee</td>
<td>Multiple</td>
<td>In the event that a Unit and their Peer Review Team cannot agree upon a satisfactory risk mitigation plan, the RTL will escalate the Unit’s peer review to the Joint Review Action Committee (JRAC).</td>
</tr>
<tr>
<td>Community Collaborators</td>
<td>Varies</td>
<td>Building trust with the IU IT community is crucial to the success of IT-28. There are a few IT professionals/leaders at IU whose input is highly valued by the UISO team.</td>
</tr>
</tbody>
</table>
There are two primary documentation instruments used in the IT-28 process:

**IT-28 Inventory Tool (IIT)**
- Developed on the ServiceNow Platform
- Inventory management for server assets only
- Collects all FAIR documentation elements
- Server-specific

**Comprehensive Evaluation**
- A narrative document to explain Unit business area and IT environment
- Describes any regulatory and/or use case specifics that affect IT strategies
- Unit-specific
The Comprehensive Evaluation is used to express the narrative of an IT Unit

<table>
<thead>
<tr>
<th>Executive Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Unit Mission</td>
</tr>
<tr>
<td>Overview of IT Services</td>
</tr>
<tr>
<td>Risk Assessment – Brief Narrative</td>
</tr>
<tr>
<td>Risk Mitigation Plan + Timeline</td>
</tr>
<tr>
<td>Risk Acceptance – Brief Narrative</td>
</tr>
<tr>
<td>Concluding Remarks</td>
</tr>
</tbody>
</table>
Supporting documentation is key to the success of Policy implementation

**IT-28 Handbook**

- Serves as the authoritative source for implementation details
- Can be modified for different audiences

UISO Handbook for Implementing IT-28

University Information Security Office
Public Safety and Institutional Assurance

Version 0.35
Last updated on: September 12, 2017
Supporting documentation is key to the success of Policy implementation

**IT-28 Placemat**

- Provides a brief overview of the IT-28 process
- Great for leadership meetings

---

**IT-28 Process Overview**

- Provides a brief overview of the IT-28 process
- Great for leadership meetings

---

**Documentation Instruments**

- There are two primary documentation instruments used in the IT-28 process: the IT-28 Inventory Tool (IT) and the Comprehensive Evaluation (CE). The IT is based on the ServicesNow Platform (PaaS), developed and maintained by UITTS. The CE remains the primary avenue for Unit's to describe their business operations and IT environment to the Peer Review Team responsible for assessing their submission. An exercise in operational security will provide a baseline for future strategy.

---

**Process Actors**

- Unit: Entity that leverages IU technology infrastructure; internal & affiliate
- Maintains current IT-28 inventory documentation in the IT
- Submits CE via it28plan@iu.edu

- Peer Review Teams (PRT): Formed by business operation areas
- Responsible for Unit assessment
- Issues recommendations to Units

- PRT Members: Members of the IU IT community or respected KEN teams
- Volunteers, Community Collaborators

- VPT: Approves/Disapproves Unit transition plans and risk mitigation strategies
- Provides implementation guidance

- ISO: Manages IT-28 implementation efforts
- Provides training/consulting to Units
- Guides RT members during analysis

---

**A Phased Approach**

- **Plan**: Defining implementation priorities, second-round peer review goals, overall timelines, communication strategy, and peer review management are core efforts in the Plan phase.
- **Develop**: Documentation instrumentation improvement was the focus of the second-round implementation. The Protect.IU website and the IU KB are used as IT-28 core resources and will be refreshed before the second-round kickoff.
- **Train**: A robust communication strategy is prepared to guide the IT community in their IT-28 efforts. Additionally, InfoShares and tool documentation guides will be available to help the IT community understand second-round objectives.
- **Execute**: The IU IT community fulfills their documentation, risk mitigation, and transition planning responsibilities in preparation for [Peer] Review.
- **Review**: [Peer] Review phase covers all efforts during the peer review of a Unit's transition plans and risk mitigation strategy.
- **Accept**: Formal signing of the Acceptance report takes place after peer review analysis is complete.
- **Improve**: A debrief will be conducted after all second-round submissions have been approved.

---

**IT Units will participate in phases Train, Execute, Review, and Accept.**

**If you have any questions and/or concerns about the IT-28 process, please email**

**it28help@iu.edu**

---

**https://protect.iu.edu/online-safety/protect-data/cyber-risk-mitigation.html**
The implementation steps for the CSF align closely with the core of IT-28

<table>
<thead>
<tr>
<th>NIST CSF - Implementation Steps</th>
<th>IT-28 Function</th>
<th>IT-28 Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>: Prioritize and Scope</td>
<td>Comprehensive Evaluation (narrative)</td>
<td>Execution</td>
</tr>
<tr>
<td><strong>Step 2</strong>: Orient</td>
<td>IT-28 Inventory Tool (inventory/asset documentation)</td>
<td>Execution</td>
</tr>
<tr>
<td><strong>Step 3</strong>: Create a Current Profile</td>
<td>Operational Security Exercise</td>
<td>Execution</td>
</tr>
<tr>
<td><strong>Step 4</strong>: Conduct a Risk Assessment</td>
<td>Unit Risk Mitigation Plans, Review Team Evaluations</td>
<td>Review</td>
</tr>
<tr>
<td><strong>Step 5</strong>: Create a Target Profile</td>
<td>Peer Review Team / Unit Collaboration</td>
<td>Review</td>
</tr>
<tr>
<td><strong>Step 6</strong>: Determine, Analyze, and Prioritize Gaps</td>
<td>Peer Review Team Recommendations</td>
<td>Acceptance</td>
</tr>
<tr>
<td><strong>Step 7</strong>: Implement Action Plan</td>
<td>Unit implements Peer Review Team Priorities</td>
<td>Improvement</td>
</tr>
</tbody>
</table>
The review teams were as diverse and complex as the RAs themselves.

- ACADEMIC
- HEALTH
- REGIONALS
- RESEARCH
- SCIENCE-TECHNOLOGY
- SERVICES
- SPECIAL TEAM (UITS)
The peer review cycle is dynamic; Units and peer review teams must establish trust.
VPIT and Unit leadership formal acceptance of risk mitigation responsibilities

- Target Profile Created
- Peer Review Complete
- Unit Commits to Plan / Profile
- Acceptance Form Drafted
- Peer Review Complete
- Final Documents
- Review Team Leader
- IT Manager
- Unit Leadership
- Unit Acceptance
- VPIT Acceptance
- Review Team Notes
- Unit Plan
- UIISO / SME Input
- VPIT Signature
IT-28 Round Two Timeline

<table>
<thead>
<tr>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept</td>
<td>Jan</td>
</tr>
<tr>
<td>Oct</td>
<td>Feb</td>
</tr>
<tr>
<td>Nov</td>
<td>Mar</td>
</tr>
<tr>
<td>Dec</td>
<td>Apr</td>
</tr>
<tr>
<td></td>
<td>May</td>
</tr>
<tr>
<td></td>
<td>Jun</td>
</tr>
<tr>
<td></td>
<td>July</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
</tr>
</tbody>
</table>

- **Training**
  - 2017: Sept - Dec

- **Unit Submissions**
  - 2018: Jan - May

- **Peer Review**
  - 2018: June - July

- **VPIT Consulting**
  - 2018: June - July

- **Risk Mitigation Plan Acceptance**
  - 2018: June - July
Round 3 goals for IT-28

- Define the scope - IU Policy, ISPP and IT audit findings
- Identify CFS categories and control objectives
- Compare round 3 Current Profile to the round 2 Target Profile

Broad goals for IT-28

- Full CSF understanding at the Unit IT level.
- Further development of the IIT to include other IT assets
- Repeatable and standardized process that provides tangible metrics and roadmap for cyber risk mitigation.
Q&A

IT-28 Risk Mitigation Policy and Peer Review Process
Indiana University
University Information Security Office
Ian Washburn - ian@iu.edu
Charles Escue - cescue@iu.edu
October 17th, 2017