A New Framework
A structured approach to managing **Information Asset** risk based on sound **Information Assurance** practices.

**Information Assurance**
- More strategy focused
- Concerned with governance, risk management, compliance
- Broader scope of information assets and safeguards
- Examples: Policies, metrics, assessments, BC/DR

**IT Security**
- More tools and tactics focused
- Stresses technology and operations
- Concerned with security apps and infrastructure
- Examples: Firewalls, AV, IDS

**Information Assets**
Data, documents, computers, or other devices that store, process, or transmit University data

Adapted from https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/
The Need for Change

- Program traditionally focused on policy & awareness
- Growing threats and regulatory requirements
- Technology and business processes changes
- Currently no viable way of assessing or managing risk

We must evolve to more effectively manage risk!
Objective

Improve the University’s overall InfoSec posture by:

- Taking the guesswork out of what should be protected, how, and to what degree
- Providing a unified method of assessing and managing information asset risk
- Fostering a culture of accountability
The Way Ahead
New Framework

Modeled after the National Institute of Standards and Technology (NIST) Cybersecurity Framework

- References globally recognized security standards
- Focuses on use of business drivers to guide security activities
- Provides a common taxonomy and mechanism to better manage information asset risk
Framework Functions

- Organize basic InfoSec activities at their highest level
- Provide a common taxonomy
Identify

Protect

Detect

Respond

Recover
Identify

- **Goal:** Develop organizational understanding to better manage information asset risk
- **Example Outcomes:** Governance, risk assessment, risk management, asset management
Identify Initatives

Governance

- Guidance Updates
- InfoSec Steering Committee
- IT Security Council
- University Compliance Council
Identify >> Initiatives (continued)

Risk Assessment & Management

- Units ID risks most critical *to them* and allocate/prioritize resources accordingly
- Units responsible for keeping focus areas current
- Maturity based; units will receive a “score” based on safeguard implementation
- ISO will develop/track campus metrics
Goal: Develop and implement appropriate safeguards to ensure delivery of services

Example Outcomes: Access controls, awareness and training, data security
Data Classification

- Risk level based on sensitivity of information handled & scope
- Safeguards based on “high water mark”

<table>
<thead>
<tr>
<th>Classification</th>
<th>Personal Devices</th>
<th>Servers &amp; Infrastructure Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desktop</td>
<td>Mobile</td>
</tr>
<tr>
<td>Regulated</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Confidential</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Public</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Internal</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Information Security
Protect ▶️ Initiatives (continued)

Safeguards

- Not a *mandate*—defines what “good” looks like
- Yes/No questions, each with a criticality rating
- Output used to calculate maturity scores
- Quantity and rigor driven by *risk level*
Awareness and Training

- SANS Securing the Human Training & Anti-Phishing
- THINK! Awareness Campaign
Detect
Detect

- **Goal:** Develop and implement appropriate activities to identify security events
- **Example Outcomes:** Anomaly and event detection, continuous monitoring
Detect Initiatives

Anomaly and Event Detection

- Bro Intrusion Detection System
- FireEye Threat Analytics Platform
- Qualys Vulnerability Scanning
Respond

- **Goal:** Develop and implement appropriate activities to take action regarding a security event

- **Example Outcomes:** Response planning, communications, mitigation, improvements
Respond ➔ Initiatives

- ISO Incident Response (IR) Analyst position funded
- Updated IR processes to be developed by ISO with input from key stakeholders, i.e., ISSC, ITSC
Identify
Protect
Detect
Respond

Recover
Recover

- **Goal:** Develop and maintain plans to restore any services impaired due to a InfoSec event
- **Example Outcomes:** Recovery planning, improvements, communications
Recover II Initiatives

- Business Continuity and Disaster Recovery (BC/DR) will be included in safeguard implementation.
- Formalized processes to be developed by ISO with input from key stakeholders, i.e., ISSC, ITSC.
Closing Comments

- Not a “one-size-fits-all” approach
- ITSC will serve as forum for discussion, training, etc.
- ISO will continue training and awareness efforts and make updates based on stakeholder feedback and lessons learned
Questions?