NextGen IIA Services

October 2012
Agenda

• Current State
• NextGen IIA Service Descriptions
<table>
<thead>
<tr>
<th>Program Component</th>
<th>IT Security Program Office Responsibility</th>
<th>Your Unit Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>Oversight and coordination of serious IT security incident response. Incident analysis and metrics. University-wide incident profile.</td>
<td>Reporting serious incidents to IIA. Establishing unit procedures and tools. Responding to unit incidents per University and unit procedures. Tracking incidents locally.</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>Conducting agreed upon security activities with pre-assigned resources from the security office to supplement unit resources.</td>
<td>Collaborating with IIA resources to deliver security services to a given unit.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Establishing risk assessment methodology (RECON) and providing assistance and consulting in its use. Creating consolidated risk profiles.</td>
<td>Conducting periodic risk assessments and implementing appropriate mitigation plans.</td>
</tr>
<tr>
<td>Technical Security Services</td>
<td>Providing a wide range of technical and physical safeguards to mitigate security risks such as vulnerability scanning, virtual firewalls, network-based attack recognition, penetration testing.</td>
<td>Implementing unit-level technical and physical safeguards including internal vulnerability scanning, virtual firewalls, and network-based attack recognition.</td>
</tr>
<tr>
<td>Policy and Compliance</td>
<td>Developing University-wide security policies and procedures and unit-level templates. Establishing compliance metrics and monitoring unit compliance.</td>
<td>Establishing and implementing unit-level procedures. Ensuring unit is compliant with University policies and regulatory requirements.</td>
</tr>
<tr>
<td>Education and Awareness</td>
<td>Sponsoring training and education. Providing communication materials to units. Maintaining the safecomputing website.</td>
<td>Ensuring training of security professionals. Conducting unit education and awareness activities.</td>
</tr>
</tbody>
</table>
IT Security Unit Roles and Responsibilities

• Information Security Unit Liaison
  – Unit focal point for coordinating security activities and communicating with unit leadership and ITS/IIA
  – Coordinating/overseeing security planning, communication/awareness, and risk assessments

• Information Security Administrator
  – For unit unique systems only
  – Conducting daily security activities
Security Community

Examples:
- Academic Affairs (Provost)
- Financial Aid
- Registrar

Examples:
- UMHS
- LSA
- College of Engineering
- Business & Finance

Examples:
- Business School
- Nursing
- Music
Volume of Sensitive Information About People

Number of People (records)
High > 10,000
Medium 1,000 – 9,000
Low < 1,000
Information and Infrastructure Assurance (IIA) is transforming its services through the NextGen Michigan program. The NextGen Michigan Information Assurance Project has defined a three-tier service approach designed to support a unit's security needs regardless of whether a unit has adopted the new shared IT services (e.g. MiWorkspace).

The three service tiers are:

1. IT Security Essential Services
2. IT Security Services within Shared IT Services
3. Additional Services for Unit Unique Services/Systems
IT Security Essential Services

Fundamental, basic security services for the entire campus regardless whether a unit adopts shared IT services. In the common good.

- Compliance Guidance
- Development of Policies, Standards, and Guidelines
- Hardening Guides
- RECON as a Service
- Security Incident Response (24x7x365)
- Education and Awareness
- Basic Network Monitoring and Protection
- Vulnerability Scanning
Shared IT Security Services

When a unit adopts the MiWorkspace, MiServer, MiDatabase or other shared IT service, IIA transitions from an IT security partner to the unit's primary IT security service provider for those systems, services, and applications that ITS manages.

- Compliance (e.g., HIPAA, EAR/ITAR, FERPA) +
- Education and Awareness +
- Enhanced Network Monitoring and Protection
- Risk Management
- Hardening +
- Data Loss Prevention
- Vulnerability Management
- Information Asset Classification of Sensitive Systems
Additional IT Security Services

Units who do not adopt MiWorkspace or other shared IT services, or have infrastructure/systems outside of these services, can acquire for-fee support from IIA to meet their unique unit needs.

- IT Security Consulting
- IT Security Disaster Recovery/Business Continuity (DRBC) Planning
- IT Security Ethical Hacking
**IT Security Essential Services**

Scope: Foundation Services provided to all university units

---

**Shared IT Security Services**

Scope: MiWorkspace/MiServer/MiDatabase units

---

**Additional IT Security Services**

Scope: For-fee services to support units and infrastructure outside MiWorkspace

---

**Functional Dependencies**
QUESTIONS/COMMENTS?