GET YOUR GOVERNANCE ON
Using Governance Processes to Mature a Campus Information Security Program
NEbraskaCERT Cyber Security Forum, March 17, 2021

TODAY'S AGENDA

MAJOR COMPONENTS OF A CAMPUS INFOSEC PROGRAM
MEASURING DEPLOYMENT AND MATURITY
MOVING FORWARD USING GOVERNANCE PROCESSES
CAMPUS INFORMATION SECURITY PROGRAM ELEMENTS

Governance & Strategy
Management
Policy & Compliance
Awareness & Training
Services & Operations

GOVERNANCE & STRATEGY

LEADER WITH INSTITUTION-WIDE RESPONSIBILITY & AUTHORITY
WRITTEN STRATEGY
SUCCESS METRICS
SHARED RESPONSIBILITY
MANAGEMENT

RISK ANALYSIS & MANAGEMENT

ASSET PROTECTION

IDENTITY MANAGEMENT

INCIDENT RESPONSE

BUSINESS CONTINUITY

STAFFING

POLICY & COMPLIANCE

WRITTEN INFOSEC POLICIES

UNIFIED COMPLIANCE

FRAMEWORK BASED

VALIDATION

EXCEPTIONS
AWARENESS & TRAINING

STAFF & FACULTY
STUDENTS
THIRD PARTIES
PRIVILEGED ACCESS

SERVICES & OPERATIONS

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
DEPLOYMENT RUBRIC

Deployment measures stages of development for specific program elements.

- **0-5% deployed** (Not deployed)
- **6-35% deployed** (Slightly deployed)
- **36-65% deployed** (Partially deployed)
- **66-95% deployed** (Largely deployed)
- **96-100% deployed** (Fully deployed)

MEASURING DEPLOYMENT

- **Program Strategy**
- **Program Management**
- **Policy & Compliance**
- **Awareness & Training**
- **Services & Operations**

- Average Current Deployment State
- Average Desired Deployment State
MATURITY RUBRIC

Maturity measures capability to deliver program elements

MEASURING MATURITY

Domain
- Information Security Policies (ISO 5)
- Asset Management (ISO 8)
- Access Control (ISO 9)
- Physical Security (ISO 11)
- Operations Security (ISO 12)
- Communications Security (ISO 13)
- Incident Management (ISO 14)
- Business Continuity Management (ISO 17)
- Compliance (ISO 18)

Maturity level (low to high)
- Incomplete (0)
- Initial (1)
- Managed (2)
- Defined (3)
- Controlled (4)
- Optimized (5)

Current Score  Desired Score

11  12
GOVERNANCE PROCESSES

Understand
Prepare strategies, goals, and objectives

Ensure
Ensure institutional alignment

Meet
Meet stakeholder needs

Follow
Follow your mission

UNDERSTANDING CONTEXT

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependence on information technology systems and the Internet to conduct academic, research, and outreach programs and offer support services</td>
<td>Very high</td>
</tr>
<tr>
<td>Impact of major IT system downtime on operations</td>
<td>Very high</td>
</tr>
<tr>
<td>Dependency of multinational and multisite operations</td>
<td>Very high</td>
</tr>
<tr>
<td>Plans for multinational and multisite operations (outsourced business functions, multiple campus locations, new research collaborations, student enrollment overseas)</td>
<td>Very high</td>
</tr>
<tr>
<td>Impact to college from an Internet outage</td>
<td>Somewhat high</td>
</tr>
<tr>
<td>The sensitivity of stakeholders to privacy</td>
<td>Somewhat high</td>
</tr>
<tr>
<td>The sensitivity of stakeholders to security</td>
<td>Somewhat high</td>
</tr>
<tr>
<td>Value of college intellectual property stored or transmitted in electronic form</td>
<td>Moderate</td>
</tr>
<tr>
<td>Level of regulation regarding security</td>
<td>Moderate</td>
</tr>
<tr>
<td>Potential impact on reputation of a security incident</td>
<td>Moderate</td>
</tr>
<tr>
<td>Impact to national or critical infrastructure in case of outage or compromise to college systems</td>
<td>Very low</td>
</tr>
</tbody>
</table>
INSTITUTIONAL ALIGNMENT

• How do you include information security planning in your overall campus strategic planning process?
• How do your institution’s information security strategies support your campus strategic objectives?
• Do your campus leaders have roles and responsibilities with respect to campus information security?

STAKEHOLDERS

• Who are they?
• Understand their motivations
• Understand their concerns
• Understand what you can do to mitigate their concerns
STAKEHOLDERS—WHAT DO THEY...

Think & Feel?
• What really counts?
• Major preoccupation
• Worries and aspirations

See?
• Environment
• Peers

Hear?
• What peers say
• What the board says
• What influencers say

Say and Do?
• Attitude in public
• Appearance
• Behavior toward others

---

STAKEHOLDERS—WHAT DO THEY...

Think & Feel?
• Concerned about admissions, rankings
• Preoccupied with student well-being
• Worried about not meeting performance goals

See?
• Reduced funding from state
• Peers are implementing newer, faster systems

Hear?
• Classroom technology must be improved
• We don’t want to be in the news for a breach

Say and Do?
• Attends professional development conferences each year
• Fundraises for the institution
• Shadow IT systems for ease of use

---

STAKEHOLDERS—WHAT DO THEY...

Think & Feel?
• Concerned about admissions, rankings
• Preoccupied with student well-being
• Worried about not meeting performance goals

See?
• Reduced funding from state
• Peers are implementing newer, faster systems

Hear?
• Classroom technology must be improved
• We don’t want to be in the news for a breach

Say and Do?
• Attends professional development conferences each year
• Fundraises for the institution
• Shadow IT systems for ease of use
MISSION IMPOSSIBLE

Mission
Provides direction and purpose

Supported by core values
How you do the things you do

The IT department will strive to protect the confidentiality, integrity, and availability of institutional information, as well as reduce the risk of information exposure, to ensure that the College can meet its missions of educating tomorrow’s leaders, conducting global research and fostering community engagement.
The IT department enables the College to educate, research, and connect by protecting our most important institutional data.

**Objectives**

- Reduce risk due to lost and stolen devices
- Identify and implement in high risk areas
- All mobile devices secured by PIN or Password
- Institutional policy requiring PIN or Password

**Goals**

- 75% of institutional laptops have FDE
- Proof of concept
- Identify and implement in high risk areas

**Strategy**

- Institution policy requiring PIN or Password
THANK YOU!

Joanna Grama, JD, CISSP
Vantage Technology Consulting Group
www.VantageTCG.com
@runforserenity

VANTAGE
Technology Consulting Group