Classification Levels Workshop

Michelle Luttrell
mjluttre@uci.edu

OIT Security - Risk & Compliance
Securityreviews@uci.edu

Agenda

- Background Information
- Classification Levels
- Classifying Items – Things to Think About
- Available Resources
- Q&A

UC Irvine

Terminology

Institutional Information = Data

- A term that broadly describes all data and information created, received and/or collected by UC.

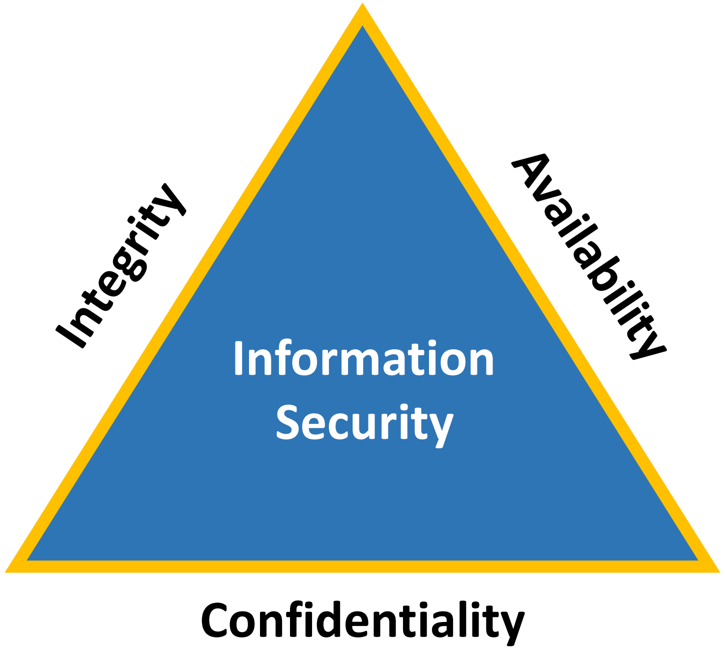
IT Resource = Assets, Systems, etc.

- A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability.

UC Classification Types

- **Protection Levels**
  - P1 – P4 (most significant)
  - Designed around confidentiality and integrity
  - Driven by security needs

- **Availability Levels**
  - A1 – A4 (most significant)
  - Designed around availability
  - Driven by Unit



Availability Levels

- A-Levels are driven by the Unit

Availability Level 1 **Minimal**	**Availability Level 2** **Low**	**Availability Level 3** **Moderate**	**Availability Level 4** **High**
Loss of availability poses **minimal** impact or financial losses.	Loss of availability may cause **minor** losses or inefficiencies	Loss of availability would result in **moderate** financial losses and/or reduced customer service	Loss of availability would result in **major** impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level

Protection Levels

Protection Level
P1 - Minimal

- Public Information
- Integrity still important
- Unauthorized modification is the primary concern
- Minimum security requirements sufficient

Protection Level
P2 - Low

- Internal use, not generally intended for public use.
- Small financial or reputational risk to UC
- Minor privacy impacts to individuals or groups

Protection Level
P3 - Moderate

- Proprietary
- Moderate fines, penalties, civil actions
- Moderate financial loss, reputational damage
- Moderate harm to the privacy of individuals or groups

Protection Level
P4 - High

- Statutory
- Significant fines, penalties, civil, criminal, regulatory action, financial loss, reputational damage
- Significant harm to individuals, groups

Classification – Things to Think About

What Do I Have?

?

How Toxic is it?

?

How Much Do I Have?

?

What Do I Have

Institutional Information

- Identify the Proprietor and ask about the classification level
- Any special data handling requirements?
- Is the data the master source of record?

IT Resource

- What type of data does it process, transmits, or stores?
- What other assets does it communicate with?
- Any special security control requirements?
- Is it considered Critical Infrastructure?

How Toxic Is It?

Things to Think About:

- What would be the impact if the data or resource was ever compromised or exposed?
- Would it cause any harm?
- How comprehensive is the data?
- What can someone do with the data elements?

How Much Do I Have?

The number of records can impact the risk level

Large Data Sets

Vs.

Small Data Sets

Critical Infrastructure

- CISO works with UCI leadership and Units to identify CI Resources

- Unique requirements are needed beyond standard Protection Level and Availability Level Controls to properly protect the IT Resource due to:
  - A high degree of risk
  - Complexity of the Resource
  - Specialized nature of the resource
  - Shared IT Resources, that if compromised it would impact the security of other systems.

- Unique requirements need to be CISO approved.

- Special risk assessment will be needed

Critical Infrastructure - Examples

- Authentication and Authorization Services (Active Directory, Kerberos, KSAMS, etc.)
- Domain Name System (DNS)
- Network and Security Hardware (routers, switches, firewalls, etc.)
- Management Tools
    - Backup, patch, or software management consoles
    - Network and firewall management tools
    - VMware vCenter and disk array management consoles
    - Encryption key management systems
- Specialized Systems (FacNet, etc.)

Classification Resources

- UCI Classifying Institutional Information and IT Resources
- UC Protection Level Classification Guide
- UC Availability Level Classification Guide
- Classification Decision Tree
- securityreviews@uci.edu