Implementation Frequently Asked Questions

Implementation questions:

1. Does IS-3 address the need for risk assessment review and follow up?

Yes. IS-3, Part III, Section 6.1 requires Locations to "[respond] to risk once determined and [prioritize] investments/budgets to address identified risks." It also requires Locations to "[monitor] risk on an ongoing basis" and to "[provide] a feedback system for continuous improvement."

Additionally, section 7.1 states that Workforce Managers must "ensure that IT Workforce Members have appropriate security skills and qualifications, and are educated on a regular basis, or receive training related to the security job requirements, policies, procedures and best practices to maintain minimum standards of information security."

Workforce Members whose role requires monitoring or managing risk must respond to information security incidents and determine the effectiveness of their response. It is an important job duty to review risk assessments after major changes, information security incidents, the identification of new vulnerabilities, and the identification of new threat actors. Workforce Members with the training and experienced needed to understand the risks UC faces must make these evaluations. If there are questions, please contact your CISO.

2. Does the policy require off-line backups?

No. IS-3 is a systemwide policy that sets a basic standard while also providing Location-specific flexibility. The policy avoids requiring specific methods for cyber risk management when multiple methods are possible and equally effective.

While backups are required, having at least one set of backups that is not connected to the network is only one way to manage cyber risk. Units should have a method to ensure that at least one backup copy of Institutional Information is protected from network threats like wipers, credentialed intrusions, and ransomware. Many threats enumerate network resources. An off-line backup is highly recommended for many recovery situations. See also Business and Finance Bulletin IS-12.

3. IS-3 Section 13.1 requires administrator access to IT Resources Classified at Protection Level 3 or higher to take place through a "managed access control point." What are some examples of a managed access control point?

The policy authors selected this language to allow for a range of approaches to secure access. This requirement can be met with the correct implementation of:

- A Jump Box (Microsoft also calls these secure administrative hosts, others use bastion host);
- A Secure Admin Workstation (SAW);
- A Privilege Access Manager (PAM);
- Multifactor-protected VPN access to an administrator vlan (or security zone) or software defined network (SDN);
- User Based Analytics (UBA) with appropriate rule sets and autonomous actions.

This is an area of rapid innovation and Cloud Suppliers and Hypervisor Suppliers are working to offer additional technological solutions to protect administrative access.

4. IS-3 Section 14.1 requires pen tests every three years. Is it possible that a pen test might be required more frequently?

Yes. IS-3 sets basic standards while also recognizing that Location-specific needs, agreements, contracts, or other obligations might necessitate stricter practices. PCI, for example, is a contract requiring annual pen tests. In section 18.1, IS-3 states that compliance with "agreements, contracts, or external obligations" is required.

Also, in some Units, prudent risk management could include more frequent penetration tests and/or penetration tests after major changes.

5. What is the Proprietor's relationship to the data they classify?

Proprietors determine the "ground rules" for the Institutional Information in their area of responsibility. A Proprietor, according to IS-3, "assumes overall responsibility for establishing the Protection Level classification, access to, and release of a defined set of Institutional Information." The UC Protection Level Classification Guide lays out a process for Proprietors to follow. This process identifies both Protection Level and Availability Level steps to follow. See also Quick Start Guide by Role: Proprietor.

6. What happened to "Data Custodians" (from the retired IS-2 policy)?

The workgroup that drafted IS-3, UC's updated electronic information security policy which replaced IS-2, created new vocabulary and retired old terms. Under IS-3, the "Unit" became the point of accountability. The term "Data Custodian" was retired and the role's responsibilities were assigned to the "Unit."

In Units, IS-3 requires that Unit Heads and Unit Information Security Leads ensure the protection and proper handling of Institutional Information and IT Resources under their area of responsibility. Assigning these duties is a proactive responsibility of Units regardless of whether their Service Providers or Suppliers are internal (UC) or external.