LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

JULY 2023

RISK MANAGEMENT

"The cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed."

— The Defense Science Board Report, Resilient Military Systems, and the Advanced Cyber Threat.

Risk Management processes are essential in developing, implementing, and maintaining the protection measures necessary to address stakeholder needs and the current threats to organization operations and assets, individuals, other organizations, and the nation.

The Department of Defense Has outlined key steps in implementing a Risk Management Framework (RMF). According to documentation provided by the Defense Counterintelligence and Security Agency:

"RMF provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of information systems."

RMF is a unified information security framework for the entire federal government that replaces legacy certification and accreditation processes applied to information systems.

RMF Covers:

- Physical Security
- Personnel Security
- Program Management
- Configuration and change management
- Information technology
- Supply chain risk management

RMF Process – The Six Steps

In documentation provided by the Defense Security Service, they explain that, "RMF is a six step process designed to build information security capabilities into Information Systems (IS) throughout the NISP through the application of community best practices for IS management, operational, and technical security controls."

The six steps outlined by the Defense Security Service are:

1. Categorize Information System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information System
6. Monitor Security Controls

Why is Continuous Monitoring so Important?

Here is what the Defense Counterintelligence and Security Agency has stated: "Continuous Monitoring activities support the concept of near real-time risk management through ongoing security assessments and risk analysis, and by recording results in IS security documentation. Continuous Monitoring requires both automated and manual processes."

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

RISK MANAGEMENT AND IT

At LIS, we take the protection of confidential data seriously. Whether it's government Controlled Unclassified Information (CUI), Personal Identifiable Information (PII) or any other sensitive information — it must be safeguarded at all times.

This means that we must keep not only hard copy documents safe, but also any electronic equipment or media that stores that information. Be it laptop, tablet, cell phone, or removable media such as thumb drives or CDs, etc.

To minimize any potential risk, we require all staff to follow basic security procedures when working with electronic devices, applications such as email, and the internet. Here are some of the most commonly used and vulnerable procedures that we must pay attention to:

Cell phones:

- Use lock, PIN, retinal, or fingerprint scan.
- Keep in a secure location. If lost or stolen, report to IT & Security immediately as your LIS login password will need to be changed immediately. Once LIS begins to use Mobile Device Management (MDM), LIS will have the ability to instantly erase the LIS portion of the phone (leaving your personal data & account on the phone intact).

Laptops:

- Follow the guidelines found in the IT Equipment User Responsibilities Sign-off form you received when assigned your LIS laptop. Some of those guidelines are:
  - Don't leave the laptop unattended in a public place.
  - Lock the console or logout if stepping away for even a few moments no matter where you are (office, home, client's office, coffee shop, etc.)
  - When traveling, do not check it with baggage. It should always be kept with you as a carry-on luggage.
  - Removable media:
    - Do not leave removable media such as a Thumb drive (USB memory stick), etc. (even if plugged-in) if you must step away for a few moments.
    - Do not leave CDs, Zip disks, external hard drives, etc. unattended, even if actively plugged-in/inserted in your laptop.