Risk Management Framework (RMF) for DoD software development

International SWAT Conference
Aarhus, Denmark
June 26-30, 2023

Ms. Lora L. Johnson

Computer Scientist

ERDC – Environmental Laboratory

June 28, 2023

US Army Corps of Engineers®

ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

Cyber Security

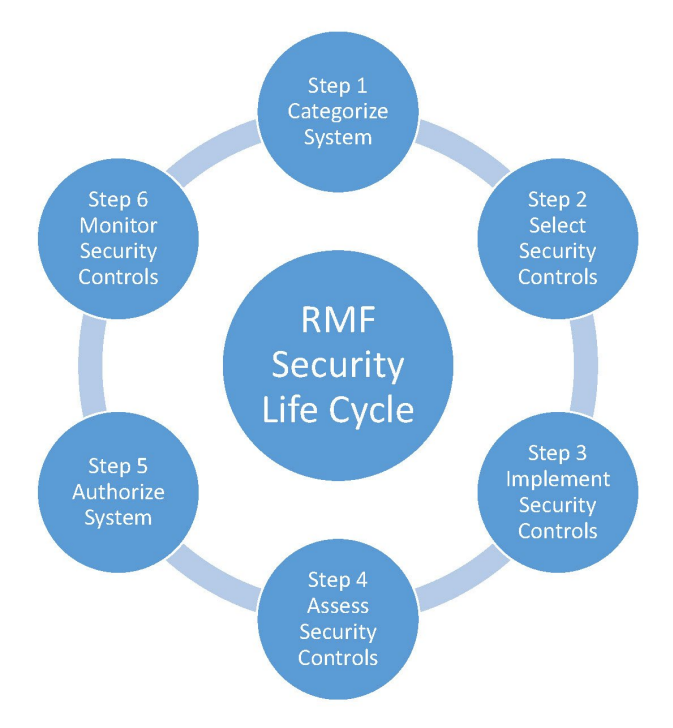
Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

Cyber security may also be referred to as information technology security.

Why should Cyber Security Implications be important to ERDC

- In order to perform Technology Transfer for ERDC clients, software products must be certified not to harm client IT systems.
- Previously, ERDC needed to get a Certificate of Network Worthiness (CoN) before a client (e.g. military installation) could install a software package.
- Risk Management Framework (RMF) has replaced the CoN process. A RMF Certificate is required by many ERDC clients before they will install new software.

Cyber Security is here to stay!!!



Risk Management Framework

Architecture Description
Mission/Business Processes
FEA Reference Models
Segment and Solution Architectures
Information System Boundaries

Repeat as Necessary

Risk Management Strategy

Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance,
Strategic Goals and Objectives,
Information Security Requirements,
Priorities, and Resource Availability

Step 1
Categorize
Information Systems
FIPS 199 / SP 800-60

Step 2
Select
Security Controls
FIPS 200 / SP 800-53

Step 3
Implement
Security Controls
SP 800 Series

Step 4
Assess
Security Controls
SP 800-53A

Step 5
Authorize
Information Systems
SP 800-37

Step 6
Monitor
Security Controls
SP 800-53A

Risk Management Framework

Security Life Cycle

Note:CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS). The NIST RMF.

What are Security Requirements?

A security requirement is a security feature required by system users or a quality the system must possess to increase the users trust in the system they use.

In general, a security requirement is considered as a non-functional requirement.

Basic Principles of Software Security

There are a number of basic guiding principles to software security. Stakeholders' knowledge of these and how they may be implemented in software is vital to software security. These include:

- Protection from disclosure
- Protection from alteration
- Protection from destruction
- Who is making the request
- What rights and privileges does the requester have
- Ability to build historical evidence
- Management of configuration, sessions and errors/exceptions

Pitfalls to not considering Cyber Security during the Software Design Process

- Not identifying critical security requirements up front
- Creating conceptual designs that have logic errors
- Using poor coding practices that introduce technical vulnerabilities
- Deploying the software improperly
- Introducing flaws during maintenance or updating

Security Testing

Common attributes of security testing include authentication, authorization, confidentiality, availability, integrity, non-repudiation, and resilience.

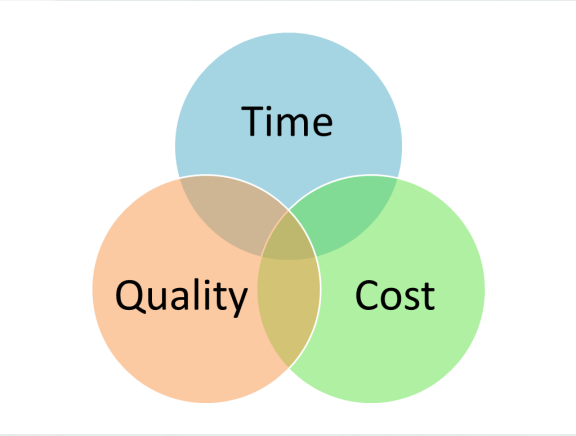
Security testing is essential to ensure that the system prevents unauthorized users to access its resources and data.

Some application data is sent over the internet which travels through a series of servers and network devices. This gives ample opportunities to unscrupulous hackers.

Conclusion

The benefits to employing a Modern Software Design Process that includes Cyber Security is:

- A mores structured design process that all project team members can understand and who have contributed too.
- A reduction in overall time to get the software product to a release stage ready for delivery to the client.
- A higher quality product for the client.
- An overall reduction in project costs due to a reduction in redoing tasks, starting over on a task, and debugging the product based on user feedback.



Questions