NIST 7 Step Process

Reading

1h

Status | Incomplete

Introduction

The NIST RMF outlines an approach which integrates security, privacy, and cyber supply chain risk management into the system development life cycle.

Read the posted articles listed below to assist you in understanding the RMF, and to get you thinking about how it might shape our IR plans.

As you develop your own plans, do not forget that you are answering business needs. While you do inform those needs, in the end they drive us, and you are responsible for meeting them.

Required Reading #1

As you revisit NIST RMF, focus more specifically on the seven step process.

1. Prepare
2. Categorize
3. Select
4. Implement
5. Assess
6. Authorize
7. Monitor

Required Reading #2

In this second reading, About the Risk Management Framework (RMF), try to picture how each of these phases may impact the IR plan and playbooks that you create.

As an example, you can see how the Categorize step could affect or add to the information you have as you create escalations in your playbook. It is important that you understand each of these phases, how they inform each other or interconnect, and how they can drive the IR plan creation and playbooks.

It bears repeating that what you do in these plans is driven by your organization's needs, not just by your perceived needs and threats.

Optional Reading and Activity

If you wish an in-depth look at the RMF, here is a three hour course on it by NIST.

Many of you might find this helpful, and if you do not look at it now, you might wish to save it to your PKM for use later.

RMF for Systems and Organizations Introductory Course

Conclusion

In real world implementation, the NIST RMF, or some other framework, is introduced to senior management and a process is established to create a risk policy. This policy will then have procedures or actions attached to it to ensure that the policy has sufficient resources, tools, and rights so that it can function in the organization.

As a result, other policies are spun off or adopted, as an example, a policy that allows data monitoring might spin off a data use and retention policy.

It is important to understand where you fit in this active, ongoing development, and how you can affect and inform it.

✓ Mark Completed

Previous
IR, Playbooks and Policy

Next
Incident Playbook Case Study

The Incident Escalation Process

W06D3 Schedule »