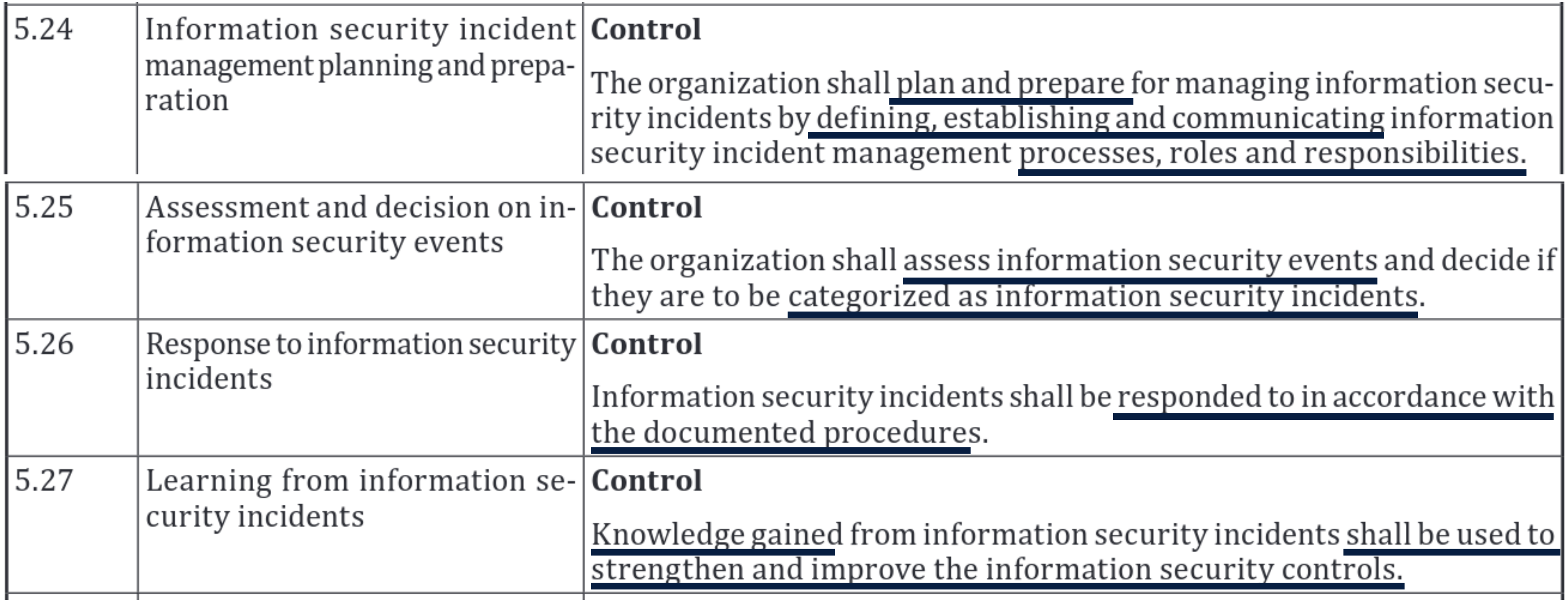
Ready to Respond

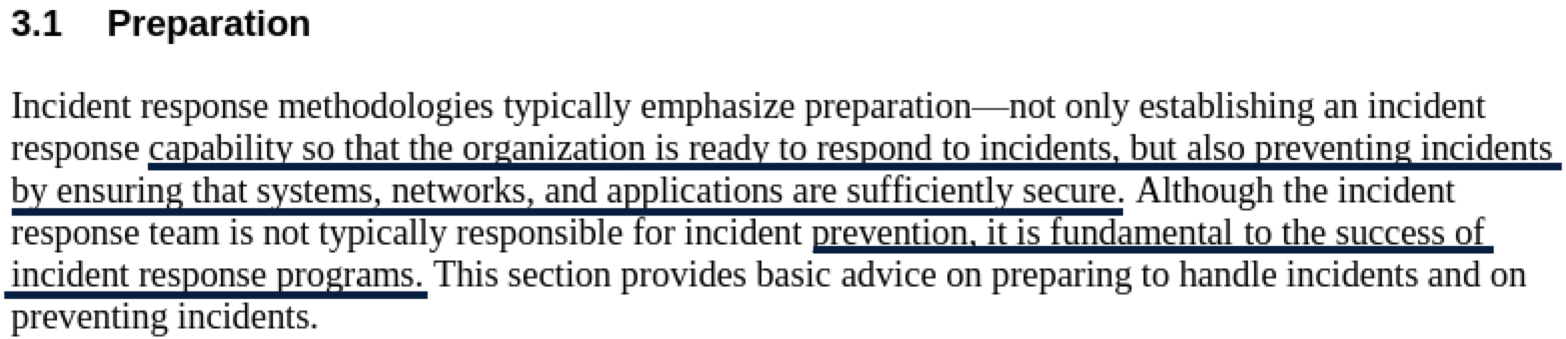
Plan, Prepare, Train, Test, and Improve

Christian Kollee
Elbsides
2024-09-13



5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
5.25	Assessment and decision on information security events	**Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents.
5.26	Response to information security incidents	**Control** Information security incidents shall be responded to in accordance with the documented procedures.
5.27	Learning from information security incidents	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

https://www.iso.org/standard/27001



3.1 Preparation

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Preparation is the key to gain the defender’s advantage

> “The defenders are at a disadvantage because we must be right all the time, but the attacker needs to be right just once.”
>
> - Unknown (Version from Lenny Zeltser (2024))

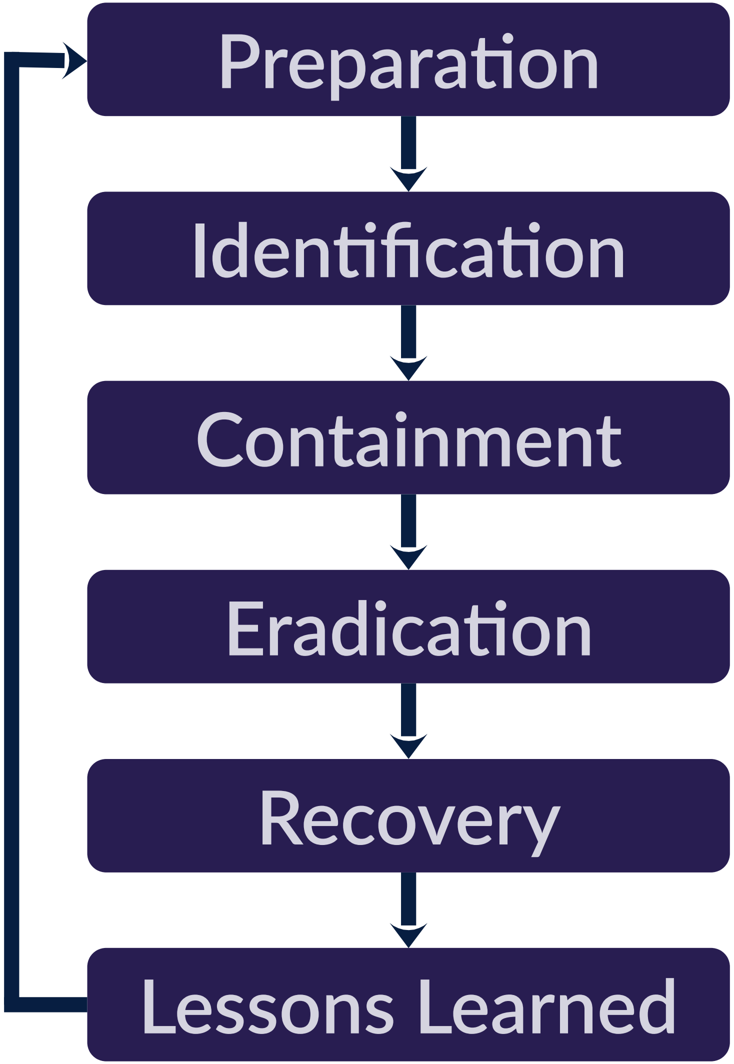
> “Defender only needs to detect one of the indicators of the intruder’s presence in order to initiate incident response within the enterprise.”
>
> - Richard Bejtlich (2009)

“Also, attackers usually operate with imperfect knowledge of their environment, figuring things out as they go, and this fumbling around is likely to set off alarms.”

- David J. Bianco (2023)

Security is a process

The Incident Response Cycle



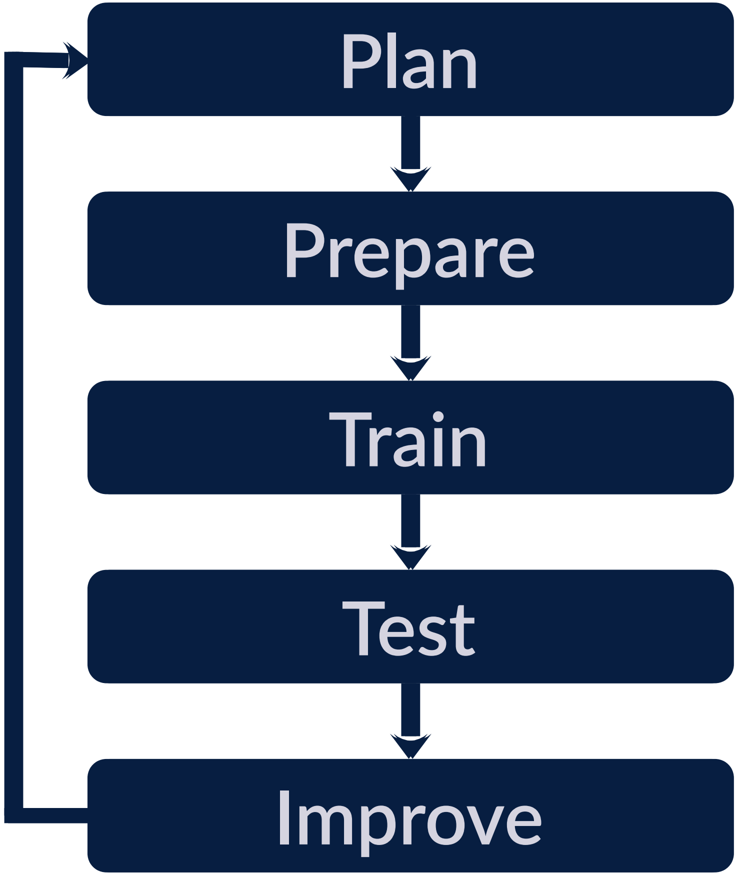
Environments change

Requirements change

Adversaries evolve

Preparation is a cycle

A (possible) Preparation Cycle



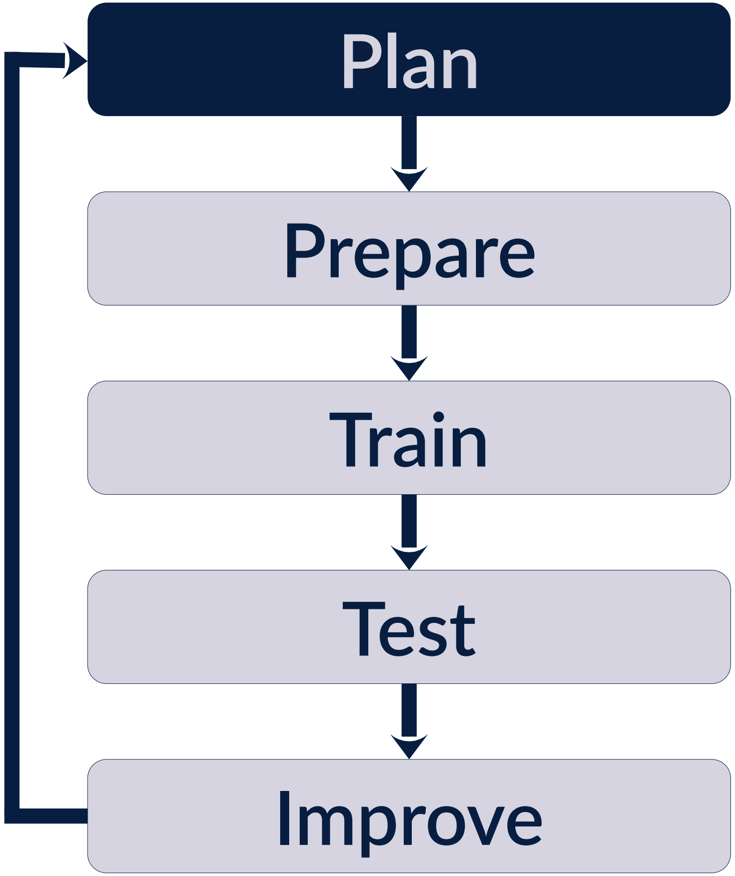
Plan

Prepare

Train

Test

Improve



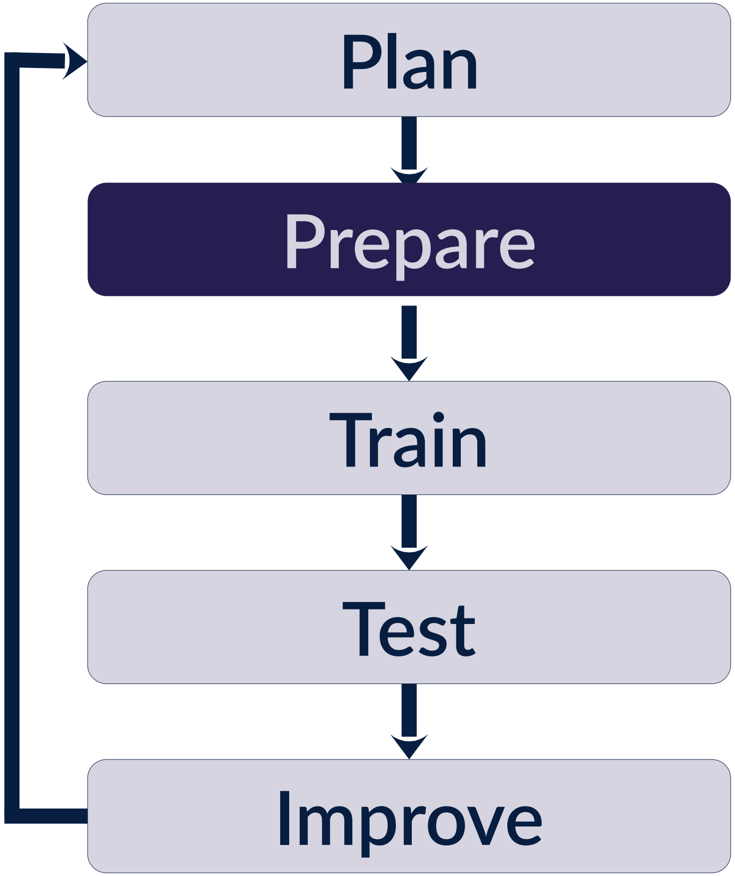
Plan

Prepare

Train

Test

Improve



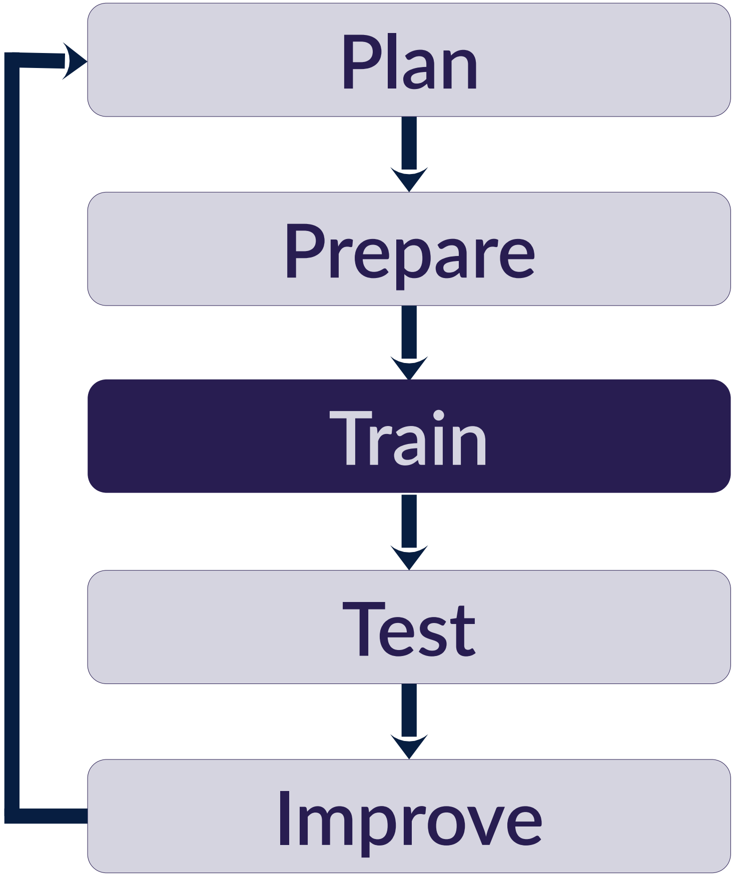
Plan

Prepare

Train

Test

Improve



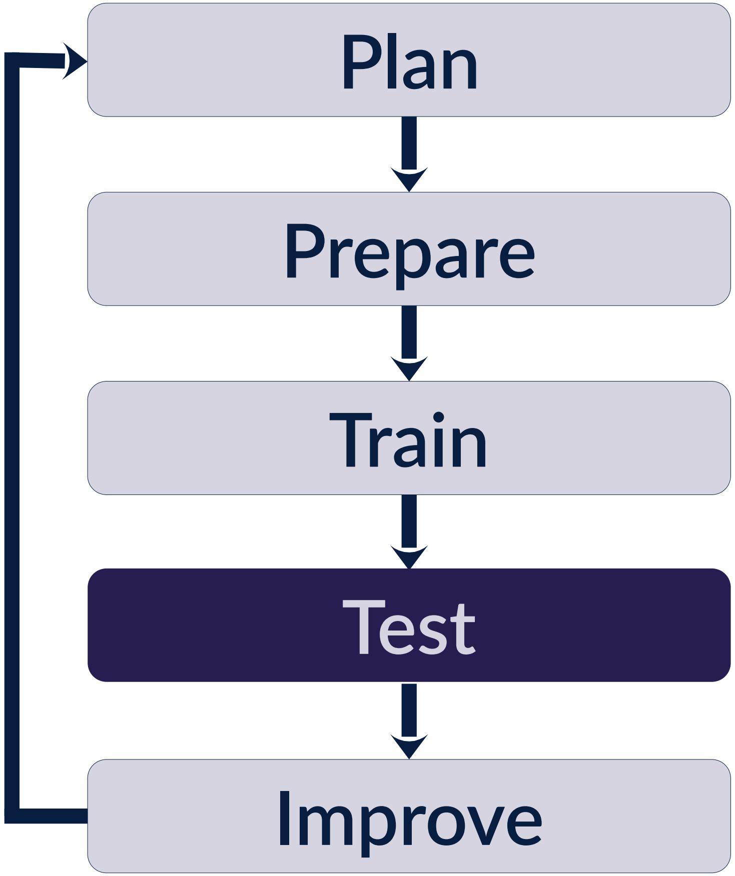
Plan

Prepare

Train

Test

Improve



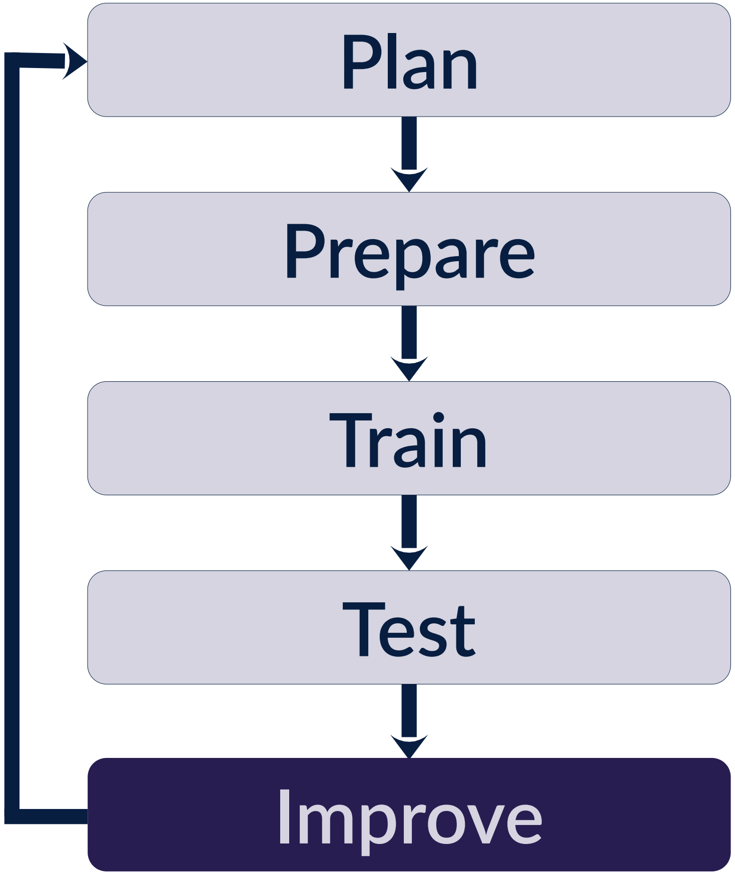
Plan

Prepare

Train

Test

Improve



Plan

Prepare

Train

Test

Improve

Preparation is the key to gain the defender's advantage

Security is a process

Preparation is a cycle

Preparation is essential to be ready to respond!

By Thegreenj - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?

Ready to Respond - Plan, Prepare, Train, Test, and Improve

Repeat

What questions can I answer first?

References

International Organization for Standardization, ISO/IEC 27001:2022

https://www.iso.org/standard/27001

National Institute of Standards and Technology, Computer Security Incident Handling Guide (SP-800-61r2)

https://csrc.nist.gov/pubs/sp/800/61/r2/final

Lenny Zeltser, Transform the Defender’s Dilemma into the Defender’s Advantage

https://zeltser.com/defenders-advantage/

Richard Bejtlich, Defender's Dilemma vs Intruder's Dilemma

https://taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html

David J. Bianco Cybersecurity teams, beware: The defender’s dilemma is a lie

https://techcrunch.com/2023/02/07/cybersecurity-teams-beware-the-defenders-dilemma-is-a-lie/