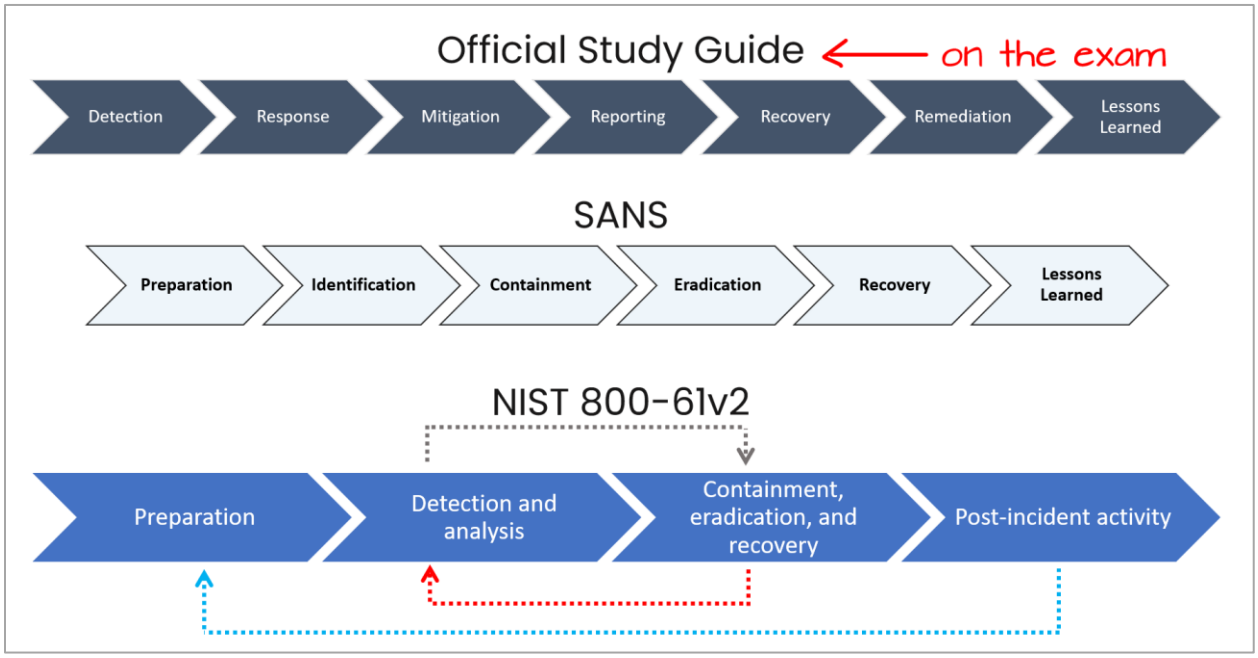
Incident Management notes for CISSP

In response to a recent question, here are some notes on the incident management process in hopes that it may be helpful to your exam preparation. It is worth noting that the CISSP incident response model is unique. It is not the model from NIST, nor from SANS. Therefore, we gain our insights from the CISSP official common body of knowledge (CBK) and study guide (OSG), which are good, though not as detailed and lengthy as the NIST and SANS frameworks. We can also learn more about the incident management and response process by drawing parallels to NIST and SANS, two widely used frameworks for incident management and response.

In these notes, you'll find:



NOTE: Also, remember that while questions on the exam will be very detailed in their language the goal of your answer, not all practice questions are created equal.

Let's start with a look at the steps in the incident management process.

Incident management steps

Here are the incident management steps from each of the frameworks:

CISSP Incident Management Steps:

1. Detection
2. Response
3. Mitigation
4. Reporting
5. Recovery
6. Remediation
7. Lessons Learned

SOURCE: OSG: pp 804-809 CBK: 502-511

NIST Incident Management Steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

SOURCE: NIST 800-61 rev 2 (Computer Security Incident Handling Guide)

SANS Incident Management Steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

SOURCE: SANS Incident Handlers Handbook

Terminology

The key differences between these terms in an incident management context are:

- **Triage -** The initial assessment and prioritization of an incident. Determining the severity and scope of the incident.

- **Containment** - Attempts to limit and control the incident from spreading. For example, disconnecting infected hosts from the network.
- **Mitigation** - Steps taken to reduce the severity of the incident. Mitigation is the phase where the organization begins to implement actions necessary to fix the incident. For example, blocking malicious IP addresses with a firewall.
- **Remediation** - Removing the underlying causes of the incident to prevent reoccurrence. For example, patching vulnerable software.
- **Eradication** - Removing artifacts of the incident like malware and backdoors. For example, completely wiping and reinstalling compromised systems.
- **Recovery** - Restoring affected systems and services back to normal operations. For example, restoring data from backups and bringing production systems back online.

The frameworks describe similar incident management processes, with some differences in categorization and naming of the steps.

- All include preparation, detection, containment/response, recovery, and lessons learned as core elements of the process.
- SANS also specifically calls out identification as a separate step.
- CISSP and SANS separate out eradication as its own step, while NIST rolls it into containment, eradication, and recovery.

In short:

- **Triage** is the *initial assessment*.
- **Containment** and **mitigation** are about *controlling* the incident.
- **Remediation** and **eradication** are about *removing the causes* of the incident.
- **Recovery** is about *restoring normal operations* after the incident.

Declaring an incident

At which step in each of these processes is an incident declared?
The step where an incident is declared in each framework is covered below. For the CISSP, we should examine both the CBK and the OSG for guidance.

CISSP (OSG):

In the Detection step. The CISSP official study guide states:

“After detecting and verifying an incident, the next step is response.”

The quote above is the first line of the section on Response (pg. 806), indirectly telling us that Detection is where the incident is declared. Also, in the in the official study guide:

"Notice that just because an IT professional receives an alert from an automated tool or a user complaint, this doesn’t always mean an incident has occurred. IT personnel investigate these events to determine whether they are incidents.”

CISSP CBK:
The CBK offers some additional details:

In the Detection (pg. 505) section, we see:

“...the detection may go through a review process during which an analyst reviews the incident and conducts some basic research to determine if the incident is legitimate or a false positive. If the analyst deems the incident valid, response procedures are initiated.”

The Response (pg. 506) section states:

“Triage is an early-stage response process for confirmed incidents and is designed to identify the criticality and categorization of the incident type.”

Specifically, when an event or alert is detected, it undergoes triage and analysis to determine if it is a legitimate incident that requires further response.

This statement in the Response section of the CBK (pg. 506) may be a bit confusing to the question of declaration:

“If the detection is validated as an actual incident, then the incident response procedures are formally initiated, and stakeholders are notified that an incident has been declared.”

From the more detailed language of the CBK, we see identification of an incident happens in the Detection phase, and more detailed classification (priority and criticality) happens after initial triage in the Response phase. Because of this and the statement “If the analyst deems the incident valid” (pg. 506) this may be viewed by some as a formal declaration, as it may trigger specific responses, such as invoking BC and DR plans.

Because the language in real exam questions tends to be precise, there should be enough detail between the CBK and the OSG to guide us.

NIST:
In the Detection and Analysis step. *The NIST document states:*

"Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it."

SANS:
In the Identification step. The SANS document states:
"This particular step requires one to gather events from various sources such as log files, error messages, and other resources, such intrusion detection systems and firewalls, that may produce evidence as to determine whether an event is an incident."

In short:

- Detection tools or humans notice an anomalous event.
- The event is analyzed to see if it is a real incident.
- If analysis validates it as an incident, then the incident is formally declared and response procedures kick off.
- Declaration of the incident starts the remaining steps of response, mitigation, reporting, recovery, etc.

So, the declaration happens during the response phase, after initial detection but before subsequent incident management steps proceed. This allows proper analysis and confirmation that an incident has genuinely occurred before committing resources to further incident handling.

Containing an incident

The step where containment is performed in each framework is:

CISSP:
In the Mitigation step. The CISSP framework states:
"Mitigation steps attempt to contain an incident. One of the primary goals of effective incident management is to limit the effect or scope of an incident."

NIST:
In the Containment, Eradication, and Recovery step. The NIST framework states: "Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions)."

SANS:
In the Containment step. *The SANS framework states:*

"The primary purpose of this phase is to limit the damage and prevent any further damage from happening ("Uf it security," 2011)."

Incident Management Activities

Here are the steps and key activities for each incident response framework:

CISSP:

1. **Detection** - Monitoring and identifying potential incidents through alerts and user reports.
2. **Response** - Activating the incident response team and coordinating initial response.
3. **Mitigation** - Containing the incident and taking steps to limit its impact.
4. **Reporting** - Notifying appropriate parties internal and external to the organization.
5. **Recovery** - Restoring affected systems and services to normal operations.
6. **Remediation** - Identifying and mitigating vulnerabilities that led to the incident.
7. **Lessons Learned** - Documenting the incident and identifying improvements to policies and controls.

NIST:

1. **Preparation** - Developing incident response policies, procedures, and resources.
2. **Detection and Analysis** - Discovering the incident and determining its scope and impact.
3. **Containment, Eradication, Recovery** - Containing the incident, eliminating components, and restoring systems.
4. **Post-Incident Activity** - Documenting and reporting the incident and identifying improvements.

SANS:

1. **Preparation** - Developing incident response capabilities and resources.
2. **Identification** - Discovering the incident and determining if an event is an incident.

3. **Containment** - Isolating affected systems to limit the incident's impact.
4. **Eradication** - Eliminating incident components from systems.
5. **Recovery** - Returning affected systems back to normal operations.
6. **Lessons Learned** - Documenting the incident and identifying improvements.

Conclusion

Note that the language in questions on practice quizzes may be less precise than the actual exam.

I hope these notes are helpful. Feel free to reach out with questions.

Good luck on the exam!