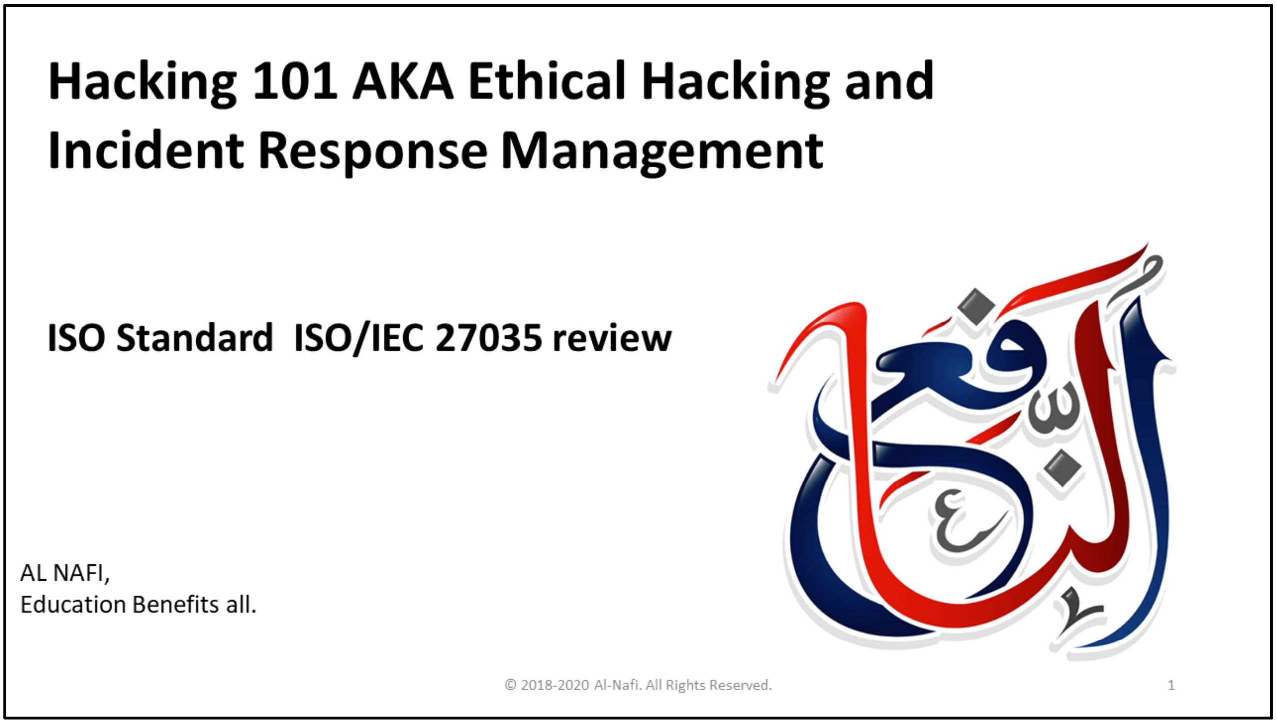
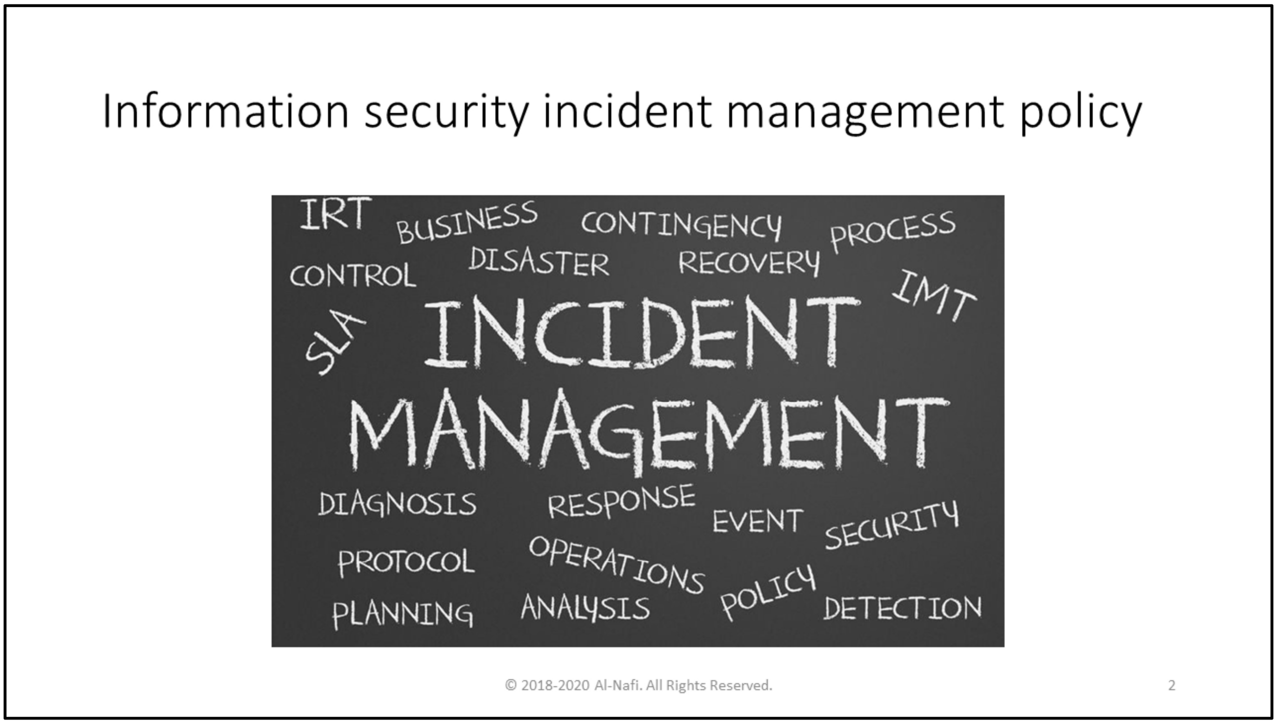


Hacking 101 AKA Ethical Hacking and Incident Response Management

ISO Standard ISO/IEC 27035 review

AL NAFI,
Education Benefits all.



Information security incident management policy

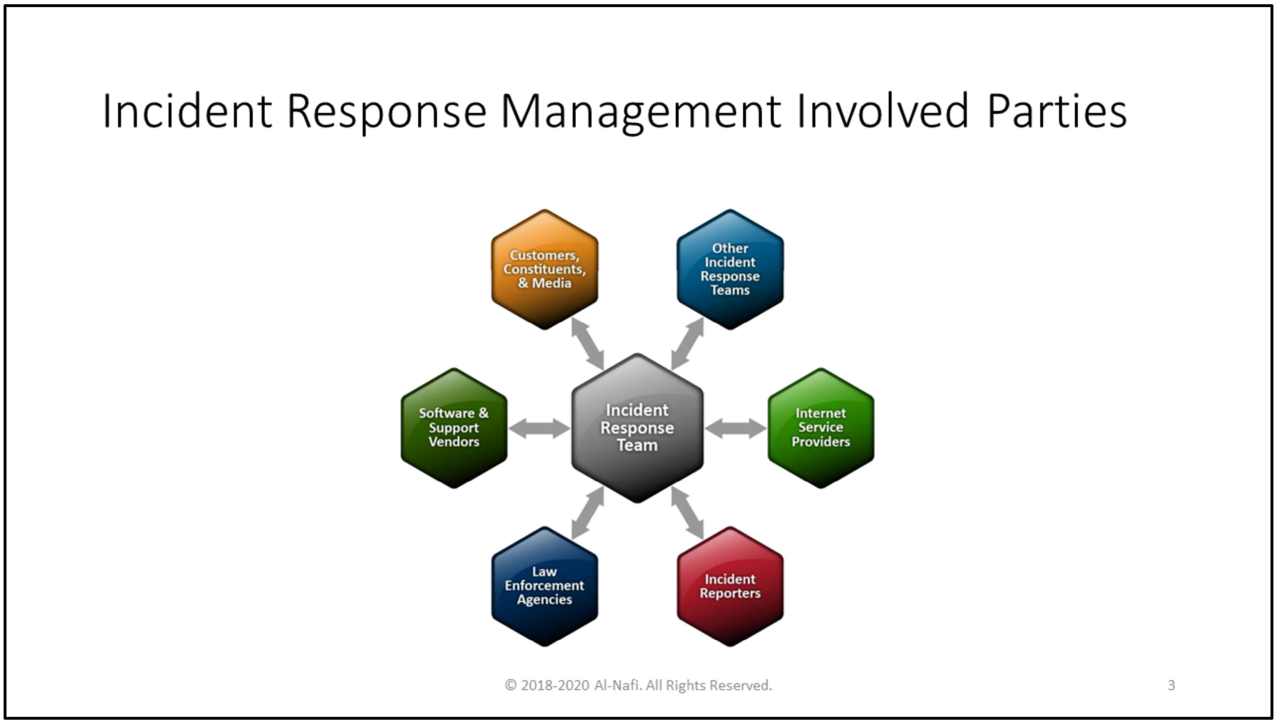
An organization information security incident management policy should provide the formally documented principles and intentions used to direct decision-making and ensure consistent and appropriate implementation of processes, procedures, etc. with regard to this policy.
Any information security incident management policy should be part of the information security strategy for an organization. It should also support the existing mission of its parent organization and be in line with already existing policies and procedures.

An organization should implement an information security incident management policy that outlines the processes, responsible persons, authority and reporting lines (specifically the primary point of contact for reporting suspected incidents) when an information security incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident response. The policy should also outline any awareness and training initiatives within the organization that is related to incident response

An organization should document its policy for managing information security events, incidents and vulnerabilities as a free-standing document, as part of its overall information security management system policy (see ISO/IEC 27001:2013, 5.2), or as part of its Information Security Policies (see ISO/IEC 27002:2013, 5.1.1). The size, structure and business nature of an organization and the extent of its information security incident management program are deciding factors in determining which of these options to adopt. An organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations. This is covered in our ISO 27001 Lead Implemented Course in further detail.

Before the information security incident management policy is formulated, the organization should identify the following regarding its information security incident management:

a) objectives;
b) interested parties internally and externally;
c) specific incident types and vulnerabilities that need to be highlighted;
d) any specific roles that need to be highlighted;
e) benefits to the whole organization and to its departments.



Incident Response Management Involved Parties

Incident Response Team

Customers, Constituents, & Media

Other Incident Response Teams

Internet Service Providers

Incident Reporters

Law Enforcement Agencies

Software & Support Vendors

A successful information security incident management policy should be created and implemented as an enterprise-wide process. To that end, all stakeholders or their representatives should be involved in the development of the policy from the initial planning stages through the implementation of any process or response team. This may include legal advisors, public relations and marketing staff, departmental managers, security staff, system and network administrators, ICT staff, helpdesk staff, upper-level management, and, in some cases, even facilities staff. An organization should ensure that its information security incident management policy is approved by a member of top management, with commitment from all of top management.

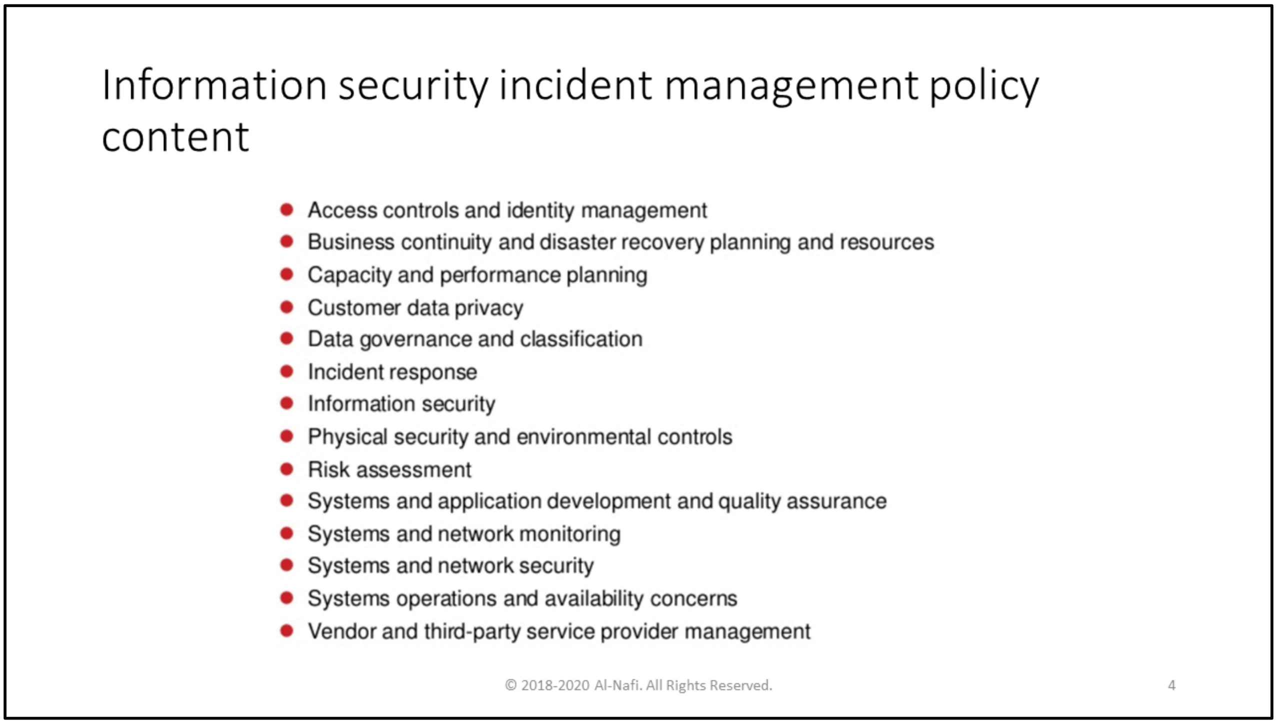
Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident, know what to do and understand the benefits of the approach by the organization. Management needs to be supportive of the information security incident policy to ensure that the organization commits to resourcing and maintaining an incident response capability.

The information security incident management policy should be made available to every employee and contractor and should also be addressed in information security awareness briefings and training.

An organization should ensure that the information security incident management plan is acknowledged by all personnel and associated contractors, ICT service providers, telecommunication providers and outsourcing companies, thus covering the following responsibilities:

a) detecting and reporting information security events (this is the responsibility of any permanent or contracted personnel in an organization and its companies);
b) assessing and responding to information security events and incidents, being involved in the post-incident resolution activities of learning, and improving information security and the information security incident management plan itself (this is the responsibility of members of the PoC (Point of Contact), the IRT, management, public relations personnel and legal representatives);
c) reporting information security vulnerabilities (this is the responsibility of any permanent or contracted personnel in an organization and its companies) and dealing with them.
The plan should also take into account any third party users, and information security incidents and associated vulnerabilities reported from third party organizations and government and commercial information security incident and vulnerability information provision organizations.

If involved parties are expected to be actively involved in handling information security incidents, then a clear division of roles and responsibilities should be made and everyone be made aware of them. Division of roles should be accompanied with the agreed incident handoff protocol so that information is exchanged in an expedient manner. If appropriate and possible, the incident handoff and information exchange should be automated to speed up the process. This kind of scenario can arise if some of the organization or IRT capabilities are outsourced to a third party. Examples of instances like this are when the organization is using cloud system run by the third party or when third party is performing digital forensics for the organization or when working with a service provider in handling incidents.



Information security incident management policy content

- Access controls and identity management
- Business continuity and disaster recovery planning and resources
- Capacity and performance planning
- Customer data privacy
- Data governance and classification
- Incident response
- Information security
- Physical security and environmental controls
- Risk assessment
- Systems and application development and quality assurance
- Systems and network monitoring
- Systems and network security
- Systems operations and availability concerns
- Vendor and third-party service provider management

The information security incident management policy should be high-level. Detailed information and step-by-step instructions should be included in the series of documents that make up the information security incident management plan.

An organization should ensure that its information security incident management policy content addresses, but is not limited to, the following topics.
a) The purpose, objectives and the scope (to whom it applies and under what circumstances) of the policy.
b) Policy owner and review cycle.
c) The importance of information security incident management to the organization and top management’s commitment to it and the related plan documentation.
d) A definition of what a security incident is.
e) A description of the type of security incidents or categories (or a reference to another document which describes this in more depth).
f) A description of how incidents should be reported, including what to report, the mechanisms used for reporting, where and to whom to report.
g) A high-level overview or visualization of the incident management process flow (showing the basic steps for handling a security incident) from detection, through

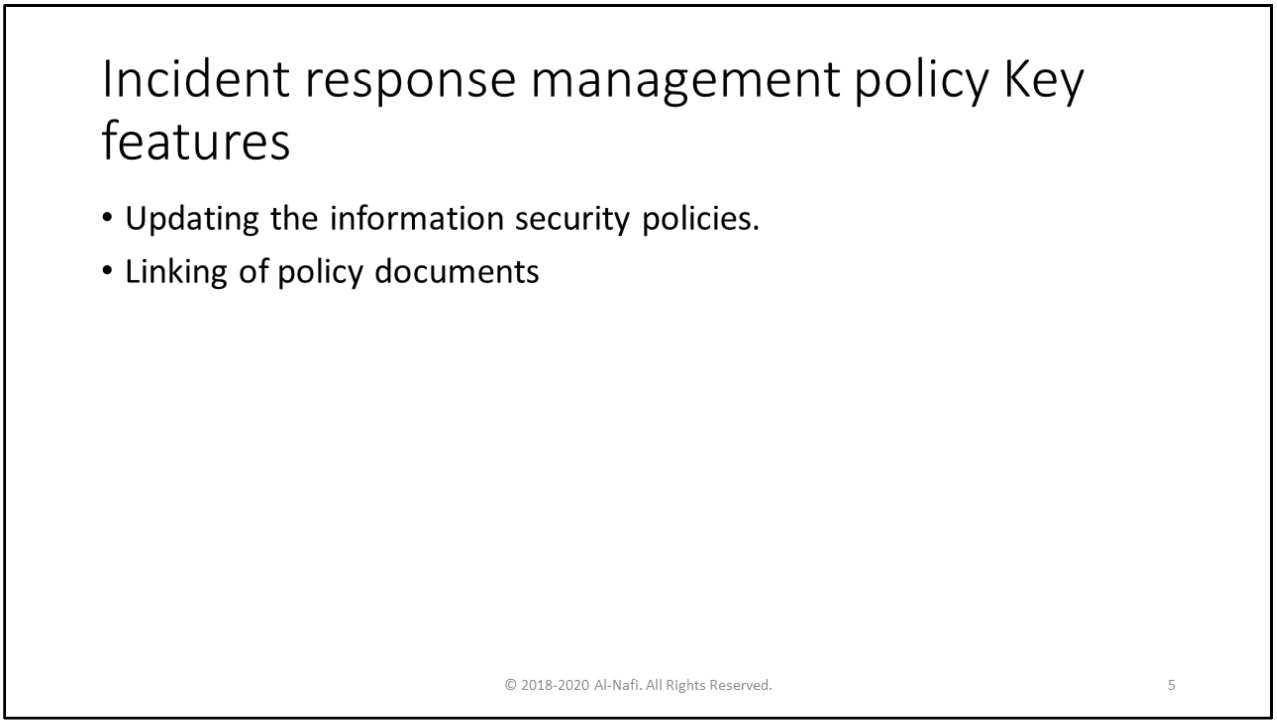
reporting, information collection, analysis, response, notification, escalation, and resolution.
h) A requirement for post information security incident resolution activities, including learning from and improving the process, following the resolution of information security incidents.
i) If appropriate, also a summary of vulnerability reporting and handling (although this could be a separate policy document).
j) Defined set of roles, responsibilities, and decision-making authority for each phase of the information security incident management process and related activities (including vulnerability reporting and handling if appropriate).
k) A reference to the document describing the event and incident classification, severity ratings (if used) and related terms. The overview should either contain a description of what constitutes an incident or a reference to the document where that is described.
l) An overview of the IRT, encompassing the IRT organizational structure, key roles, responsibilities, and authority, along with summary of duties including, but not limited to, the following:
1) reporting and notification requirements related to incidents that have been confirmed;
2) briefing top management on incidents;
3) dealing with enquiries, instigating follow up, and resolving incidents;
4) liaising with the external organizations (when necessary);
5) requirement and rationale for ensuring all information security incident management activities performed by the IRT are properly logged for later analysis.
m) A requirement that components across the organization work in collaboration to detect, analyse, and respond to information security incidents.

n) A description of any oversight or governance structure and its authority and duties, if applicable.
o) Links to organizations providing specific external support such as forensics teams, legal counsel, other IT operations, etc.
p) A summary of the legal and regulatory compliance requirements or mandates associated with information security incident management activities (for more details, see Annex A).
q) A list and reference to other policies, procedures, and documents that support the information security incident management process and related activities. Many of the items listed in the policy may have their own more detailed procedures or guidance documents.
There are other related policies or procedures that will support the information security incident management policy and could also be established as part of the preparation phase, if they don’t already exist and if they are appropriate for the

organization. These include, but are not limited to, the following.
— An information security incident management plan,
— A continuous monitoring policy stating that such activity is conducted by the organization and describing the basic monitoring tasks. Continuous monitoring ensures preservation of electronic evidence in case it is required for legal prosecution or internal disciplinary action.
— Authority granting the IRT access to the outputs of this monitoring or the ability to request logs as needed from other parts of the operation (this could also be put in the information security incident management policy).
— Information sharing, disclosure and communication policies which outline how and when information related to incident management activities can be shared and with whom. Information should be kept confidential and only disclosed according to the relevant legislation. In many instances, legislation requires affected parties to be notified should any personal identifiable information be compromised. Apart from the legal requirements, information should also follow any organizational requirements for disclosure. Information may need to be shared in the course of incident handling when a third party needs to be involved or modified. The scope, circumstances and purpose of this information sharing need to be described, or referenced, in the appropriate policies and procedures. An example of information disclosure guidance and markings is the use of Traffic Light Protocol (TLP). An example of TLP guidance can be seen at https://www.us-cert.gov/tlp.
— Information storage and handling policies which require records, data, and other information related to investigations to be stored securely and handled in a manner commensurate with their sensitivity. If the organization has a document labelling or classification schema, this policy will also be important to information security incident management activities and personnel.
— An IRT charter that specifies in more detail what the IRT is to do and the authority under which it operates. At a minimum, the charter should include a mission statement, a definition of the IRT's scope, and details of the IRT's top management sponsor, the IRT authority, contact information for the IRT, its list of services and core activities, its scope of authority and operation, its purpose and goals; along with a discussion of any governance structure.
— The goals and purposes of the team are especially important and require clear, unambiguous definition.
— The scope of an IRT normally covers all of the organization's information systems, services and networks. In some cases, an organization can require the scope to be different (either larger or narrower), in which case, it should be clearly documented what is in, and what is out of, scope.
— Examples of IRT authority include searching and confiscating personal belongings, detaining people and monitoring communications.
— IRT governance might include the identification of an executive officer, board

member or top manager who has the authority to make decisions on IRT and also establish the levels of authority for IRT. Knowing this helps all personnel in the organization to understand the background and set-up of the IRT and it is vital information for building trust in the IRT. It should be noted that before this detail is promulgated, it should be checked from a legal perspective. In some circumstances, disclosure of a team's authority can expose it to claims of liability.

— An overview of the information security incident management awareness and training program. This should include any training mandates, policies, or requirements for staff related employee awareness training and incident management training for the IRT members.



Incident response management policy Key features

- Updating the information security policies.
- Linking of policy documents

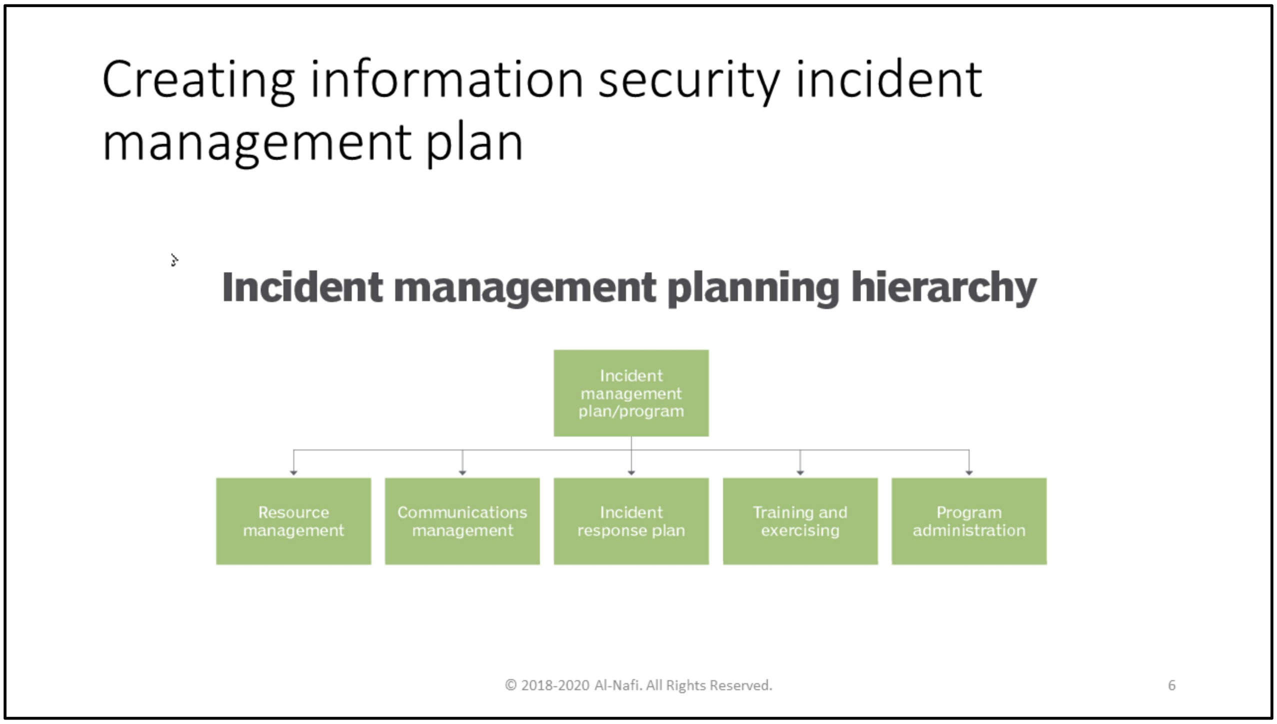
<u>Updating of Information Security Policies.</u>

An organization should include information security incident management content in its information security policies at corporate level, as well as on specific system, service and network levels and relate this content to the incident management policy. The integration should aim for the following.
a) To describe why information security incident management, particularly an information security incident reporting and handling plan, is important.
b) To indicate top management commitment to the need for proper preparation and response to information security incidents, i.e. to the information security incident management plan.
c) To ensure consistency across the various policies.
d) To ensure planned, systematic and calm responses to information security incidents, thus minimizing the adverse impacts of incidents.

<u>Linking of policy documents</u>

An organization should update and maintain its corporate information security and risk management policies, and specific system, service or network information security policies in tandem to ensure they remain consistent and current. These corporate-level policies should refer explicitly to the information security incident management policy and associated plans.

The corporate-level policies should include the requirement that appropriate review mechanisms need to be established. These review mechanisms need to ensure that information from the detection, monitoring and resolution of information security incidents and from dealing with reported information security vulnerabilities is used as input to the process designed to maintain continuing effectiveness of the policies.



Creating information security incident management plan

Incident management planning hierarchy

- Incident management plan/program
  - Resource management
  - Communications management
  - Incident response plan
  - Training and exercising
  - Program administration

The aim of an information security incident management plan is to document the activities and procedures for dealing with information security events, incidents and vulnerabilities, and communication of them. The plan stems from and is based on the information security incident management policy.

Overall, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and support tools for the detection and reporting of, assessment and decision making related to, responses to and learning lessons from information security incidents.

The plan may include a high level outline of the basic flow of incident management activities to provide structure and pointers to the various detailed components of the plan. These components will provide the step-by-step instructions for incident handlers to follow using specific tools, following specific workflows or handling specific types of incidents based on the situation.

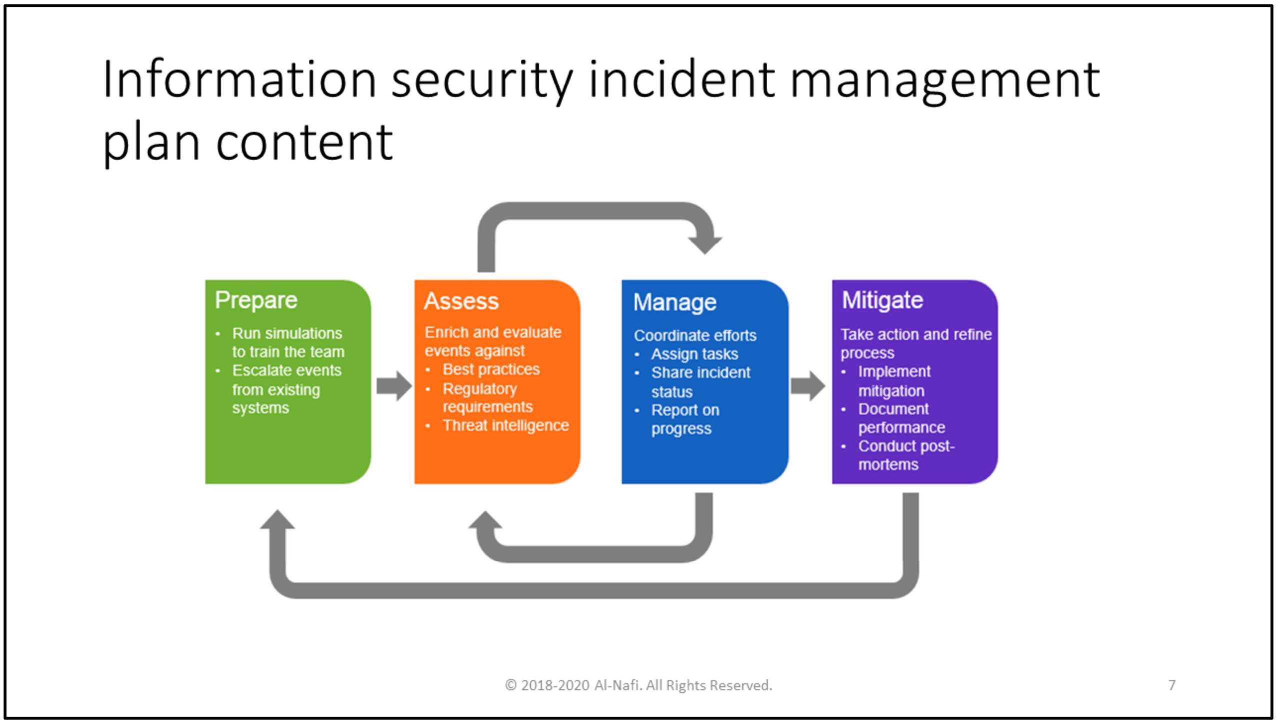
The information security incident management plan comes into effect whenever an information security event is detected or information security vulnerability is reported.

An organization should use the plan as a guide for the following:

a) responding to information security events;

b) determining whether information security events become information security incidents;
c) managing information security incidents to conclusion;
d) responding to information security vulnerabilities;
e) requirements for reporting;
f) requirements for storing information (including its format) during the whole incident management process;
g) rules and circumstances under which information sharing with internal and external groups or organizations can take place;
h) identifying lessons learned, and any improvements to the plan and/or security in general that are required;
i) making those identified improvements.

Planning and preparation of the incident response plan should be undertaken by the process owner, with a clear goal or set of goals for incident response within a defined scope based on the information security incident management policy.



Information security incident management plan content

Prepare
- Run simulations to train the team
- Escalate events from existing systems

Assess

Enrich and evaluate events against
- Best practices
- Regulatory requirements
- Threat intelligence

Manage

Coordinate efforts
- Assign tasks
- Share incident status
- Report on progress

Mitigate

Take action and refine process
- Implement mitigation
- Document performance
- Conduct post-mortems

Key decision-making criteria and processes to support expected management phases should be defined and reviewed before the planning and preparation process considers specific incident types and the corresponding response processes. This requires available policy, formal or informal understanding of assets and controls, and contribution from participants and management support.
The content of the information security incident management plan should give an overview, as well as specifying detailed activities. As noted above, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and support tools.

The detailed activities, procedures and information should be associated with the following.

a) Plan and prepare.

1) A standardized approach to information security event/incident categorization and classification, to enable the provision of consistent results. In any event, the decision should be based on the actual or projected adverse impacts on the organization’s business operations, and associated guidance.

2) An information security database structured for the exchange of information is likely to provide the capability to share reports/alerts, compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems. The actual format and use of the database will depend on the organization’s requirements. For example, a very small organization may use documents, while a complex organization may use more sophisticated technology such as relational databases and application tools.

3) Guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Based on the guidance provided in the information security incident management plan, anyone assessing an information security event, incident or vulnerability should know under which circumstances it is necessary to escalate matters and to whom it should be escalated. In addition, there are unforeseen circumstances when this may be necessary. For example, a minor information security incident could evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident.

4) Procedures to be followed to ensure that all information security incident management activities are properly logged and that log analysis is conducted by designated personnel.

5) Procedures and mechanisms to ensure that the change control regime is maintained covering information security event, incident and vulnerability tracking and information security report updates, and updates to the plan itself.

6) Procedures for information security evidence analysis.

7) Procedures and guidance on using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), ensuring that associated legal and regulatory aspects have been addressed. Guidance should include discussion of the advantages and disadvantages of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC 27039.

8) Guidance and procedures associated with the technical and organizational mechanisms that are established, implemented and operated in order to prevent information security incident occurrences and to reduce their likelihood, and to deal with information security incidents as they occur.

9) Material for the information security event, incident and vulnerability management awareness and training program.

10) Procedures and specifications for the testing of the information security incident management plan.

11) The plan of organizational structure for information security incident management.

12) The terms of reference and responsibilities of the IRT as a whole, and of individual members.

13) Important contact information.

14) Procedures and guidance regarding information sharing as agreed with the organization’s public affairs office, legal department and top management or relevant departments.

b) Detection and reporting.

1) Planning and preparation requirements for detection and reporting should enable and support the development and operation of processes to find or accept information about information security incidents.
2) Criteria for acceptance of an incident report should be defined, based on the completeness of the report and verification of one or more information security events. To support later decision-making, minimum criteria for acceptance of any event detection alert or manual report should be defined prior to the planning process, and should include at least identification of an affected environment or asset, a statement of one or more suspected or confirmed events or qualified event type, and the time received. In order to support decision making, the planning process should include a method for returning detection or reports that have insufficient information.
3) Reporting output or notification should be defined in the context of the organization, the incident response policy, and assignment of technical and management roles. The format of reports and notification should match the incident classification scale or a consistent related metric.

4) Detecting and reporting the occurrence of information security events (by human or automatic means).
5) Responding to incorrect use of the reporting process (potentially including taking action outside the scope of the incident management plan).
6) Collecting the information on information security events.
7) Detecting and reporting on information security vulnerabilities.
8) Recording information gathered in the information security database.

c) Assessment and decision.

1) Planning and preparation requirements for assessment and decision should enable and support the development and operation of processes to evaluate and direct actions in response to information security incidents.
2) Prior to development of assessment and decision processes, the process owner should ensure that the minimum information for identification and classification of a security incident is defined, consisting of specific items of required and supporting information. This definition will allow response planners to develop consistent processes for completeness and classification of detected and reported events. The information sufficiency required to differentiate between true positive and false positive reports should be defined and allow for accumulation of information to

support estimation of and response to false negative detection and reports.
3) If the incident planning process is to depend on automated information management and decision support systems, the functions, implementation, and on-going operation of these systems should be defined. The incident handling process owner should ensure an information security database is sufficiently defined prior to developing the response processes that depend on it.
4) The PoC conducting assessments of information security events (including escalation as required), using the information security event/incident classification scale (including determining the impacts of events based on the affected assets/services) should decide whether events should be classified as information security incidents.
5) The IRT assessing information security events should confirm whether an event is an information security incident or not. To do this, another assessment should be conducted using the information security event/incident classification scale to confirm the details of the event (suspected incident) type and affected resource (categorization). This should be followed by decisions being made on how the confirmed information security incident should be dealt with, by whom and in what priority, as well as escalation levels.
6) Assessing information security vulnerabilities (that have not yet been exploited to cause information security events and potential information security incidents), with decisions made on which need to be dealt with, by whom, how and in what priority.
7) Fully recording all assessment results and related decisions in the information security database.

d) Responses.

1) Planning and preparation requirements for response should enable and support the development and operation of processes to respond to information security incidents. Prior to response planning, the incident handling process owner should gather definitions or create working thresholds or categories for priority of information and information system, impact of each intrusion types, damage scale, intrusion alarm level, and severity. These can be qualitative or quantitative as long as they are consistent with assessment and decision preparations, and enable the IRT manager to assign the incident actions or tasks to responders.

2) Classes of response should also be defined prior to the planning process, organized by cost, time, technical resource minimums, and other metrics to enable assignment of response class relative to the known information about the reported and assessed incident. Immediate or deferred response should be included, as well as a definition of how single or cyclic incident tasks will be managed in the response process.
3) Review by the IRT to determine if the information security incident is under control,
i) if the incident is under control, instigate the required response, either immediately

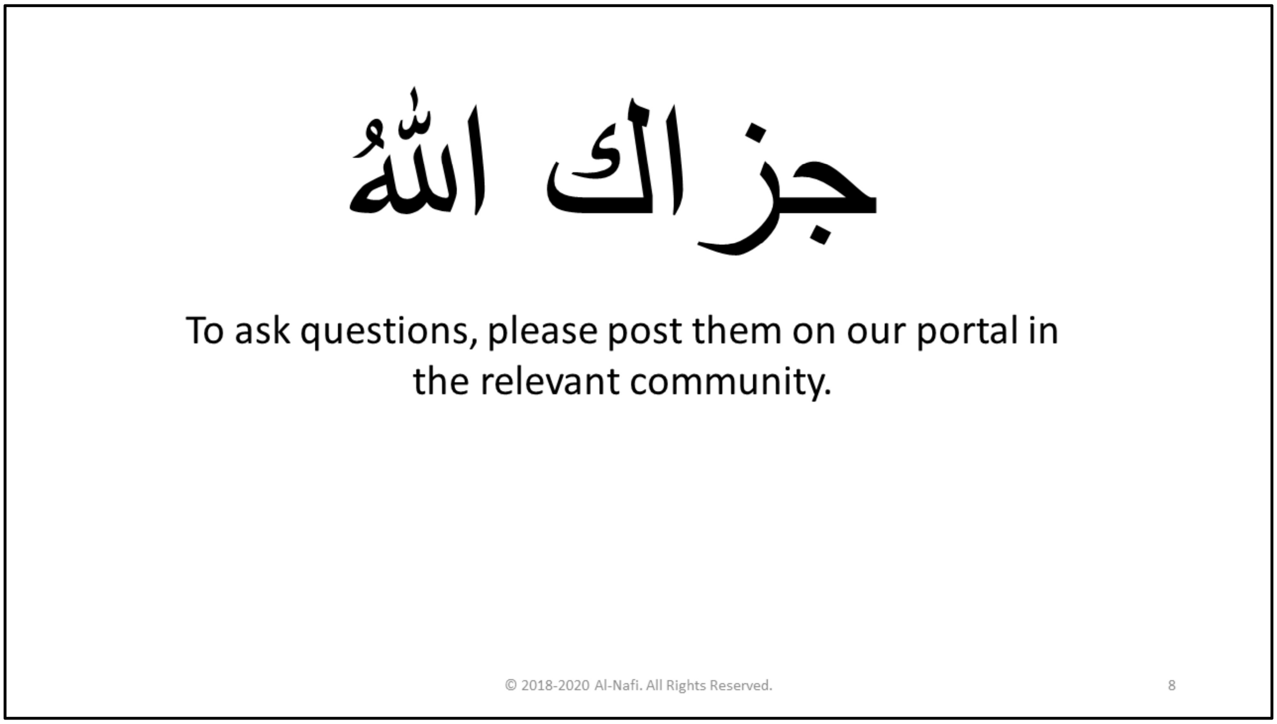
(in real-time or in near real-time) or at a later time, and
ii) if the incident is not under control or it is going to have a severe impact on the organization’s core services, instigate crisis activities through escalation to crisis handling function.
4) Defining a map of all internal and external functions and organizations that should be involved during the management of an incident.
5) Containing and eradicating the information security incident as appropriate to mitigate or prevent the scope and impact of the incident from increasing.
6) Conducting information security evidence analysis, as required.
7) Escalation, as required.
8) Ensuring that all involved activities are properly logged for later analysis.
9) Ensuring that electronic evidence is identified, collected/acquired and preserved.
10) Ensuring that the change control regime is maintained and thus that the information security database is kept up-to-date.
11) Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations.
12) Dealing with information security vulnerabilities.
13) Once the incident has been successfully dealt with, formally closing it and recording this in the information security database.
14) Post-incident activity should include further analysis as required.

e) An organization should ensure that the information security incident management plan documentation allows for information security incident responses, both immediately and longer-term. All information security incidents should undergo an early assessment of the potential adverse impacts on business operations; both short and longer-term (for example, a significant disruption could occur sometime after an initial information security incident). Further, it should allow for some responses necessary for information security incidents that are completely unforeseen, where ad hoc controls are required. Even for this situation, organizations should encompass general guidelines in the plan documentation on the steps that can be necessary.

f) Lessons learned.

1) Identifying the lessons learned from information security incidents and vulnerabilities.
2) Reviewing, identifying and making improvements to information security control implementation (new and/or updated controls), as well as information security incident management policy, as result of the lessons learned.
3) Reviewing, identifying and if possible, making improvements to the organization’s existing information security risk assessment and management review results, as a result of the lessons learned.

4) Reviewing how effective the processes, procedures, the reporting formats and/or the organizational structure were in responding to assessing and recovering from each information security incident and dealing with information security vulnerabilities, and on the basis of the lessons learned identifying and making improvements to the information security incident management plan and its documentation.
5) Updating the information security database.
6) Communicating and sharing the results of review within a trusted community (if the organization so wishes).



جزاك اللهُ

To ask questions, please post them on our portal in the relevant community.