ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.4. Assessment and decision on information security events
Information security events are required to be assessed and the organization needs to decide whether they are to be considered information security incidents.

Contact point provides initial triage – review of each event and evaluate the Impact to decide whether it has to be classified as information security incident.

Criteria for classification of incidents to prioritize the actions.

The contact point may not be the single decision layer with regards to incidents – the organization may have an information security incident response team (ISIRT) and the incident will be escalated here for assessment and decision.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.5. Response to information security incidents
After assessment the organization should respond to information security incidents according to documented procedures.

Incidents should be responded to with the first goal being to resume "normal security level" and then initiate recovery.

ISO/IEC 27002 provides some guidance on what the response should include:

- collect evidence as soon as possible after the occurrence of the incident;
- perform forensics analysis;
- escalate the incident if necessary;
- communicate to all parties that need-to-know about the incident (be it inside or outside the organization);
- find the weaknesses that lead to the incident and deal with them;
- record the incident and close it.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

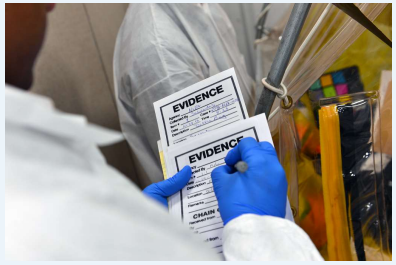
Control – 16.1.6. Learning from information security incidents
The organization is required to use the knowledge it gets from dealing with security incidents to learn reduce the likelihood and impact of future incidents.

Besides resolving security incidents its important that people learn from the security incidents to avoid them happening in the future or if they happen to deal with them more effectively.

Case studies and anecdotes from actual security incidents can be used in awareness training as examples of what can happen, how to avoid situations and how to respond

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.7. Collection of evidence
The organization should collect and preserve information which can serve as evidence according to established procedures.



In most cases its not clear whether a certain incident will end up in court or not.
The organization should collect information that can serve as evidence for every information security incident.

The organization should have procedures to deal with evidence collected.

ISO/ IEC 27037 - guidelines for identification, collection, acquisition and preservation of digital evidence.