IT Professional Standards

Information Security Discipline

Sub-discipline 607 – Incident Management, Investigation and Digital Forensics

December 2012
## DOCUMENT REVIEW

### Document Information

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Sub-discipline 607 – Incident Management, Investigation and Digital Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Reference</td>
<td>607</td>
</tr>
<tr>
<td>Document Version</td>
<td>0.5</td>
</tr>
<tr>
<td>Document Date</td>
<td>10/12/2012</td>
</tr>
<tr>
<td>Last updated</td>
<td>07/01/2013</td>
</tr>
</tbody>
</table>
Sub-discipline 607 – Incident Management, Investigation and Digital Forensics

<table>
<thead>
<tr>
<th>Sub discipline</th>
<th>3 assist</th>
<th>4 perform</th>
<th>5 manage</th>
<th>6 set strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>607.01 Incident management</td>
<td>6073.01 Assist with incident management activities under supervision</td>
<td>6074.01 Perform incident management under supervision</td>
<td>6075.01 Lead incident management</td>
<td>6076.01 Direct and be fully accountable for information security incident management, investigation and forensics</td>
</tr>
<tr>
<td>607.02 Investigation</td>
<td>6073.02 Assist with incident investigation activities under supervision</td>
<td>6074.02 Conduct incident investigations under supervision</td>
<td>6075.02 Lead incident investigation</td>
<td></td>
</tr>
<tr>
<td>607.03 Digital Forensics</td>
<td>6073.03 Assist with digital forensics examination under supervision</td>
<td>6074.03 Conduct digital forensic examination, under supervision</td>
<td>6075.03 Lead digital forensic examination</td>
<td></td>
</tr>
</tbody>
</table>

Incident Management

Level 3

Competence (6073.01): Assist with incident management activities under supervision

This competence will be demonstrated by the following Performance Criteria (6073.01C):

a) Identify the sources and nature of information security incidents to information systems
b) Correctly follow the procedures and standards relating information security incident management activities
c) Operate with integrity and confidentiality during information security incident management activities
d) Identify when and how to seek advice and guidance from other individuals during information security incident management activities
e) Complete, to defined standards and timelines, own assigned tasks and activities during information security incident management activities

Competent performance requires Understanding (6073.01U) of:

a) What is meant by an information security incident
b) What is the purpose of incident management and its role within information security
c) The value and importance of incident management in responding to and mitigating incidents
d) The need to identify and retain evidence for investigation following organisational standards
e) Why prompt and effective incident management is critical for the organisation
f) What are the processes, procedures, methods, tools and techniques used to conduct incident management activities within the organisation
g) The need for incident management activities to be carried out in accordance with any codes of conduct and organisational standards

Competent performance requires Knowledge (6073.01K) of:

a) The procedures to follow when notifying information security incidents
b) The activities involved in managing an information security incident from identification through to resolution
c) The methods, tools and techniques relating to information security incident management activities and their deliverables
d) The external legislation and regulations, internal policies and internal and external standards that are relevant to information security incident management activities

Level 4

Competence (6074.01): Perform incident management under supervision

This competence will be demonstrated by the following Performance Criteria (6074.01C):

a) Clearly and accurately define the scope of any information security incident management exercise
b) Accurately source, gather and collate information relating to information security incidents that may impact on the organisation’s information assets, engaging with stakeholders in a professional manner
c) Perform incident management, under supervision, including incident detection, classification, investigation, resolution, reporting and closure
d) Take ownership for an incident and act as the primary level of escalation
e) Critically review information and data from information security incidents to assess business impact and to determine resolution mitigation
f) Make recommendations as to the specific actions that should be applied to respond to information security incidents and escalate incidents that are outside agreed tolerance levels
g) Communicate the status of information security incidents and their outcomes effectively to stakeholders
h) Review and update procedures for incident management

Competent performance requires Knowledge (6074.01K) of:

a) The methods and tools that may be used to respond to information security incidents
b) When to escalate and communicate incidents
c) How to interpret plans to respond to and document information security incidents
d) The policies and standards that exist within the organisation for incident management
e) How to:
   • Correctly identify, source, gather and collate all relevant sources of information in order to respond to an information security incident
   • Use and apply appropriate information security incident management tools, methods and procedures
Competent performance requires Understanding (6074.01K) of:

a) The purpose of incident management and what are the outcomes
b) The significant tasks undertaken within incident management and response activities
c) The need to act professionally and sensitively with all stakeholders when responding to information security incidents
d) The elements of an incident management plan
e) The key incident management responsibilities and their corresponding roles

Level 5

Competence (6075.01): Lead incident management

This competence will be demonstrated by the following Performance Criteria (6075.01C):

a) Be responsible for managing information security incidents on all types of information systems
b) Act as the interface to other technical and managerial staff and other groups within the organisation in relation to specific incidents
c) Provide a prompt recovery of information systems within the business to the specified service level agreement or SLA
d) Review and apply the strategy, policies, procedures tools and techniques relating to incident response and management activities
e) Develop, implement and maintain procedures, and techniques for responding to and managing information security incident activities and their deliverables
f) Correctly identify the range of response actions that may be used to mitigate information security incidents
g) Ensure that incident management teams remain focused on the resolving incidents and have clear priorities
h) Take decisive and timely action in the event of incidents impacting the integrity of information systems
i) Develop and maintain organisational capability in incident response and management
j) Objectively analyse and clearly present the findings from incident management activities appropriately to sponsors, stakeholders and external bodies

Competent performance requires Knowledge (6075.01K) of:

a) The range of issues associated with information security incident management activities
b) How to establish escalation and communication processes and lines of authority
c) Who is responsible for a specific incident
d) How to develop plans to respond to and document information security incidents
e) What are the:
   o range of approaches that can be applied to incident management activities and their appropriateness in a range of business contexts
   o internal and external factors that may impact on incident management activities
   o legislation and external standards that apply to incident management activities
Competent performance requires **Understanding (6075.01U)** of:

a) The importance of using lessons learned in order to inform future incident management activities
b) The nature of any incident in order to assign the appropriate resources and competences
c) The incident impact tolerance levels specified for managing information security incidents
d) The importance of maintaining information security incident records and documentation
e) Relevant internal and external standards relevant to information security incident management
f) The need to be accountable for:
   - the successful management of information security incidents
   - the implications and consequences of failure to respond to/mitigate/control incidents that arise

**Level 6**

**Competence (6076.01): Direct and be fully accountable for information security incident management, investigation and digital forensics**

This competence will be demonstrated by the following **Performance Criteria (6076.01C):**

a) Be fully accountable for information security incident management, investigation and digital forensics
b) Define the strategy, policies and standards for information security incident management, investigation and digital forensics
c) Ensure that information security incident management, investigation and digital forensics is sufficient to provide the business with full assurance of information integrity and resilience
d) Direct resource allocation and professional development strategy for incident management, investigation and digital forensics activities
e) Oversee the alignment of information security incident management, investigation and digital forensics across and between enterprises
f) Monitor the quality and effectiveness of incident management, investigation and digital forensics activities, critically reviewing the approach and process and making recommendations for improvement where appropriate
g) Provide timely and objective advice and guidance to others on all aspects of information security incident management, investigation and digital forensics activities including best practice and the application of lessons learned
h) Develop communication processes for internal and external parties (e.g., media, law enforcement, customers) relating to information security incident management, investigation and digital forensics
i) Authorises the issue of formal reports to management on the effectiveness and efficiency of information security incident management, investigation and digital forensics
j) Provide thought leadership on the discipline of information security incident management, investigation and digital forensics, contributing to internal best practice and to externally recognised publications, white papers etc
Competent performance requires **Knowledge (6076.01K)** of:

a) The need to advise and guide others on all aspects of incident management, investigation and digital forensics activities  
b) How to organize, train and equip teams to respond to information security incidents  
c) How lessons learned may be applied to information security activities of other programmes  
d) Sources of best practice in incident management, investigation and digital forensics activities

Competent performance requires **Understanding (6076.01U)** of:

a) How to design and develop the strategy, policies, plans and standards for incident management, investigation and digital forensics to ensure the alignment with all relevant legislation, regulations and external standards  
b) The need to ensure that timely and effective review of incident management, investigation and digital forensics procedures takes place  
c) How to objectively analyse the findings from reviews of incident management, investigation and digital forensics activities and report to sponsors and stakeholders  
d) The importance of using lessons learned in order to inform future activities

**Incident investigation**

**Level 3**

**Competence (6073.02): Assist with incident investigation activities under supervision**

This competence will be demonstrated by the following **Performance Criteria (6073.02C):**

a) Correctly follow the procedures and standards relating information security incident investigation activities  
b) Assist ensuring that all applicable logs and other records are preserved as evidence are  
c) Identify how access was obtained during information security incident  
d) Operate with integrity and confidentiality during information security incident investigation activities  
e) Identify when and how to seek advice and guidance from other individuals during information security incident investigation activities  
f) Identify the need for detail digital forensic examination as part of an investigation  
g) Document, report and communicate the findings of an investigation

Competent performance requires **Understanding (6073.02U)** of:

a) What is meant by a information security investigation  
b) What is the purpose of a information security investigation  
c) How intruders can gain unauthorised entry to information systems system  
d) What the motivation of an intrusion is (financial or other)  
e) The importance of conducting investigations and identifying and retaining evidence for investigation following organisational standards and procedures
f) The importance of and documenting the incident under investigation

g) Why prompt and effective investigation is critical

h) When to inform police and other authorities

Competent performance requires Knowledge (6073.02K) of:

a) What information can be collected to support incident investigation

b) How to contain damage during an investigation

c) The processes, procedures, methods, tools and techniques used to conduct investigations

d) The activities involved in investigating an information security incident

e) Where to seek information to support investigations

Level 4

Competence (6074.02): Perform incident investigations under supervision

This competence will be demonstrated by the following Performance Criteria (6074.02C):

a) Clearly and accurately define the scope of any information security incident investigation

b) Identify potential sources of evidence to investigate

c) Accurately source, gather and collate information and evidence relating to information security investigations, engaging with stakeholders in a professional manner

d) Perform incident investigations under supervision

e) Take ownership for an investigation and act as the primary contact

f) Critically review information and data from information security incidents to inform the investigation

h) Communicate the status and results of information security incident investigations clearly and effectively to stakeholders

i) Review and update procedures for investigations using information from past investigations

Competent performance requires Knowledge (6074.02K) of:

a) The methods and tools that may be used to investigate information security incidents

b) The policies and standards that exist within the organisation for incident investigation

c) How to:
   • Correctly identify, gather, secure and document all relevant sources of evidence
   • Use and apply appropriate information security investigation tools, methods and procedures

Competent performance requires Understanding (6074.02K) of:

a) How to conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk
b) The purpose of investigation in identifying and analyzing a information security incident in order to respond in the most effective way

c) The significant tasks undertaken within incident management and response activities

d) The need to maintain own capability to investigate information security incidents

e) The need to act professionally and sensitively with all stakeholders when investigating information security incidents

Level 5

Competence (6075.01): Lead incident investigation

This competence will be demonstrated by the following Performance Criteria (6075.01C):

a) Be fully accountable for managing information security investigations on all types of information systems

b) Act as the interface to other technical and managerial staff and other groups within the organisation in relation to specific investigations

c) Provide a prompt investigation of information systems within the business to the specified response level

d) Review and apply the strategy, policies, procedures tools and techniques relating to incident investigation

e) Develop, implement and maintain procedures, and techniques for investigating information security incidents

f) Develop and maintain organisational capability in incident investigation

g) Objectively analyse and clearly present the findings from incident investigation activities appropriately to sponsors, stakeholders and external bodies

Competent performance requires Knowledge (6074.02K) of:

a) The range of issues associated with information security investigations

b) What are the:
   o range of approaches that can be taken for information security investigation activities
   o internal and external factors that may impact on information security investigation activities
   o regulations, legislation and external standards that may apply to information security incident investigation activities

c) Who is responsible for a specific investigation

Competent performance requires Understanding (6074.02U) of:

a) The importance of using lessons learned in order to inform future investigations

b) How to manage the effective response to information security incidents through investigation

c) The nature of any incident in order to assign the appropriate resources to undertake investigations

d) The need to periodically test and refine information security investigation plans and processes

e) The importance of maintaining information security investigation records and documentation
f) Relevant internal and external standards relevant to information security incident investigation

g) The need to be accountable for:
   - the successful management of information security incident investigation
   - the implications and consequences of failure to fully investigate incidents that arise

Digital Forensics

Level 3

Competence (6073.03): Assist with digital forensic examinations under supervision

This competence will be demonstrated by the following Performance Criteria (6073.03C):

   a) Correctly follow the procedures and standards relating digital forensic examination activities
   b) Apply digital forensic examination procedures to develop leads to help to identify instigators of information security incidents
   c) Collect evidence relating to all records of the unauthorized access that lead to the incident
   d) Operate with integrity and confidentiality during digital forensic examinations
   e) Preserve the “crime scene” from alteration
   f) Collect and analyze data as part of a digital forensic examination
   g) Identify when and how to seek advice and guidance from other individuals during digital forensic examinations
   h) Document all information, reporting the findings of a digital forensic examination

Competent performance requires Understanding (6073.03U) of:

   a) What is meant by a digital forensic examination
   b) What is the purpose of a digital forensic examination as part of information security incident management
   c) How to apply the tools and techniques specified for collecting and analysing data
   d) The prioritisation of where to look for evidence
   e) The technical aspects of data storage including hard disk configuration and slack space
   f) The need for digital forensic examinations to be undertaken in accordance with any codes of conduct and organisational policies and standards
   g) The importance of documenting the damage caused by the incident under investigation

Competent performance requires Knowledge (6073.03K) of:

   a) What information can be collected to support digital forensic examination
   b) Digital forensic requirements for collecting and presenting evidence
   c) The processes, procedures, methods, tools and techniques used to conduct digital forensic examinations
   d) The external legislation and regulations, internal policies and internal and external standards that are relevant to digital forensic examination activities
d) The activities involved in digital forensic examinations

e) Where to seek information to support digital forensic examinations

Level 4

Competence (6074.03): Conduct digital forensic examination, under supervision

This competence will be demonstrated by the following Performance Criteria (6074.03C):

a) Correctly use and apply the processes and procedures, methods tools and techniques to conduct digital forensic examinations

b) Accurately source, gather and collate data in order to conduct digital forensic analysis of digital activities

c) Analysing system information (e.g. system logs, network traffic, hard disks, virtual memory, etc) for evidence of breaches of information security policy or laws

a) Critically analyse software for malware products

b) Examine monitoring systems to identify potential information security breaches

c) Analyse system information for evidence of breaches of information security policy

d) Report and escalate suspicious traffic/activities in a timely manner

e) Take appropriate and proactive action to secure information assets from any potential threats identified by digital forensic analysis until such time as these threats are mitigated

f) Seize evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business and maintaining evidential weight

Competent performance requires Understanding (6074.03U) of:

a) What is the purpose of digital forensic examination and its role within information security

b) The value and importance of digital forensic examination in identifying and classifying incidents, identifying sourcing and retaining evidence for investigation

c) The importance of using information contained in system logs, network traffic, hard disks, virtual memory as part of digital forensic activity

d) What is meant by digital forensics and its role in detecting and preventing intrusions and inappropriate access to information assets

e) The fact that digital forensics frequently requires the analysis of transient and volatile whereas other aspects of digital forensic examination involves the analysis of information and data that is more static

f) The differences and relationships between digital forensic examination for law enforcement and the focus within commercial environments

g) The role of digital forensic examination in the prevention of industrial espionage, malicious damage/hacking and serious crime

h) The fact that a significant proportion of information security breaches and/or illegal accesses to information assets are conducted from within the organisation
Competent performance requires **Knowledge (6074.03K)** of:

- a) The range of methods, tools and techniques that can be used to conduct digital forensic examinations
- b) The legislation and regulation that are relevant to digital forensic examination
- c) The potential threats that pose the highest risk to the organisation and which are prioritised during digital forensic examination
- d) The specific risks and vulnerabilities that apply to information assets as they are transmitted across networks
- e) The legal requirements for preservation of digital forensic evidence
- f) How to access, use and analyse information and data as digital forensic evidence where appropriate

**Level 5**

**Competence (6075.03): Lead digital forensic examination**

This competence will be demonstrated by the following **Performance Criteria (6075.03C):**

- a) Be responsible for managing digital forensic examinations on all types of information systems
- b) Act as the interface to other technical and managerial staff and other groups within the organisation in relation to specific digital forensic examinations
- c) Review and apply the strategy, policies, procedures tools and techniques relating to digital forensic examination
- d) Develop, implement and maintain procedures, and techniques for undertaking digital forensic examinations and their deliverables
- e) Ensure that digital forensic examination teams remain focussed and have clear priorities
- f) Lead and manage a digital forensic examination team, prioritising resource allocation and capability management for digital forensic activities
- g) Develop and maintain organisational capability in digital forensic examination
- h) Advise, mentor and supervise less experienced members of the digital forensic examination team
- i) Objectively analyse and clearly present the findings from digital forensic examinations appropriately to sponsors, stakeholders and external bodies

Competent performance requires **Knowledge (6074.03K)** of:

- a) How to use and apply a range of digital forensic examination tools and techniques to examine information security incidents
- b) The range of issues that may arise during digital forensic examination activities
- c) How to identify and select the most appropriate tools and techniques for a particular incident
- d) Who is responsible for a specific digital forensic examination
- e) How to establish escalation and communication processes and lines of authority
- f) How to develop digital forensic examination plans to respond to investigate information security incidents
- g) What are the:
- range of approaches that can be applied to digital forensic examination activities and their appropriateness in a range of different contexts
- internal and external factors that may impact on digital forensic examination activities
- regulations, legislation and external standards that apply to digital forensic examination activities

Competent performance requires **Understanding (6074.03U) of:**

a) The importance of using lessons learned in order to inform future digital forensic examination activities
b) Relevant internal and external standards and their application to digital forensic examination
c) The optimum digital forensic approaches for recovering evidence
d) The detailed application of several forensic techniques including advantages and disadvantages for different scenarios
e) How to align appropriate resources and competences to specific information security incidents
f) The importance of maintaining detailed digital forensic examination records and documentation
g) The need to be accountable for:
   - the successful completion of digital forensic examinations in relation to information security incidents
   - the implications and consequences of failure to effectively identify causes of information security breaches through digital forensic examination