IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard – Security Incident Management (SS-014)

Chief Security Office

Date: 04/07/2017

Department
for Work &
Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

Contents

1. Introduction 4
2. Purpose 4
3. Exceptions 5
4. Audience 5
5. Scope 5
6. Security Controls Assurance 6
7. Technical Security Control Requirements 6
7.1. Plan and Prepare Against Security Incidents 6
7.2. Security Incident Detection and Identification 7
7.3. Collection and Preservation of Evidence 8
7.4. Security Incident Response, Mitigation and Reporting 9
7.5. Security Incident Recovery and Remediation 10
7.6. Post Security Incident Review 11
8. Compliance 11
9. Accessibility 11
10. Security Standards Reference List 11
11. Reference Documents 12
12. Definition of Terms 12
13. Glossary 12
14. Controls Catalogue Mapping 13

1. Introduction

1.1. This Security Incident Management Standard provides the list of controls that are required to manage the security incidents to a Department of Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data to be stored or processed in order to minimise the risk from known threats both physical and logical to an acceptable level for operations.

ISO/IEC27035-1 2016 defines an information *security event* as “an occurrence indicating a possible breach of information security or failure of controls” and *security incident* as “one or multiple related and identified information security events that meet established criteria and can harm an organisation’s asset or compromises its operations.”

DWP recognises a security incident as “*a deliberate attempt, whether successful or not, to compromise Departmental assets (information, people, IT or premises) or any accident resulting in a loss of Departmental assets*”

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for Security Incident Management and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for Security Incident Management deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

2.3. The main focus of this document is to identify, assess and manage security incidents effectively to minimise the impact on the organisation. The response to Security Incident Management must be proportionate based on the organisation risk appetite and the costs of maintaining the incident management capability.

3. Exceptions

3.1. In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

3.5. Reference section 10.3 – where controls cannot be adhered to all activity MUST be carried out in accordance with the agreed guidelines (ACPO Good Practice Guide for Digital Evidence) and an auditable log maintained.

4. Audience

4.1. This standard is intended for Suppliers, System and Network Administrators, security groups, support staff, IT staff and partners, involved in securing environments for DWP networks, systems and applications and others who are responsible for managing security incidents.

5. Scope

5.1. This standard is to cover systems handling data within the Government Security Classification Policy (GSCP). All of the organisation's Security Incident Management implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all information systems that are provisioned for departmental use.

5.3. In the event of uncertainty on the controls laid out in this standard please contact the Security Front Door for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see [section 3 Exceptions] above).

7.1. Plan and Prepare Against Security Incidents

The primary objective of this section is to pre-empt, control and manage the occurrence of security incidents. The below controls will help to reduce the likelihood and impact of information security incident.

Reference	Security Control Requirement
7.1.1.	A security risk assessment MUST be performed to identify risks and determine their likelihood and impact on DWP operations and to implement appropriate controls to mitigate the identified risk.
7.1.2.	All DWP network devices and all end user devices MUST be hardened in accordance with the DWP server build standards and patterns; DWP approved anti-virus and latest security updates/patches MUST be installed in accordance with the PSN patching requirements.
7.1.3.	Information systems and network configurations MUST be reviewed to ensure the configuration remains in line with the system baseline configuration and approved change requests. The configurations MUST be reviewed at least annually, on system addition/upgrade/merge with other network or as part of security incident remediation activity.
7.1.4.	The network MUST be securely designed and configured based on the SS018 Network Security Design Standard. The design MUST be reviewed periodically to ensure its appropriateness.
7.1.5.	Vulnerability assessment MUST be performed to identify and remediate any security weaknesses within information system and protect against malicious software. The vulnerability assessment would be performed at implementation, annually or upon significant system change. The product owner would be responsible for carrying out any remediation activity.
7.1.6.	A detailed information security incident management plan MUST exist, including communication methods (as well as any out-of-band methods) and information disclosure. The information security management plan, its process and procedures MUST be tested periodically.
7.1.7.	Security Incident Response Team (SIRT) MUST be established. The team would be responsible for receiving, assessing and responding to security incidents.
7.1.8.	Security awareness training MUST be provided to all DWP employees as part of induction and also as part of annual refresh security training program. Additional training MUST be provided to personnel who are involved in security incident management to ensure that their roles and responsibilities are clear and understood.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
7.1.9.	The content of the security incidents guidance training that each DWP employee needs to be familiarised with MUST be published by DWP Contact Centre. Contact Centre will produce the guidance in consultation with SIRT.
7.1.10.	Contact Centre MUST ensure that the content of the security incidents guidance training is kept up-to-date.
7.1.11.	DWP Security Education and Awareness (SEA) team must ensure that all new joiners and all existing DWP employee as part of annual refresh complete the security incident guidance training.

7.2. Security Incident Detection and Identification

Reference	Security Control Requirement
7.2.1.	All DWP employees MUST read through the DWP “Security Incidents Guidance-all staff” to understand what constitutes a potential security incident, how to report a security incident, and what actions they MUST and MUST not take themselves.
7.2.2.	All security incidents identified by the DWP staff, any business partners and third parties having access to DWP’s data, information and system MUST be notified to the Contact Centre as quickly as possible. The report should contain as much information as possible. Contact Centre will validate the reported incident.
7.2.3.	Both Contact Centre and Monitoring team MUST refer to the DWP Incident Triage Matrix to determine the severity of the security incidents. The severity of incident is based on the level of hardship or distress that could be caused to the customer and/or staff as well as what reputational damage could be caused to the Department and/or Government. It determines the priority for handling the incident, who manages the incident and the timing and extent of the response. Five levels of incident severity will be used to guide incident response: Very Low, Low, Medium, High and Very High.
7.2.4.	Contact Centre MUST categorise and triage (based on DWP Security Triage Process) all security incidents reported manually relating to information assets and assess the risk using the DWP Incident Triage Matrix to decide if the incident should be referred to DWP SIRT for investigation. Contact Centre, if required, will call the ‘Security Incident Response Forum’ for advice.
7.2.5.	The detection and reporting of system security events or existence of information security vulnerability where possible MUST be automated. Automated detection capabilities include network-based and host based Intrusion Detection and Prevention systems (IDPS), anti-virus software and log analysers. The team monitoring the services MUST monitor the system events and are responsible for validating the identified security incident.
7.2.6.	Monitoring team MUST categorise and triage all system security incidents relating to information assets and assess the risk using the DWP Incident Triage Matrix.
7.2.7.	All security incident identified by Contact Centre as medium or higher MUST be referred to SIRT. The risk rating is used by SIRT to determine the proportionate follow up action to be taken. All low rated security incidents MUST be handled by the Contact Centre.
7.2.8.	All security incidents identified out of hours MUST follow the DWP Security Incident Management Process – Out of Hours.
7.2.9.	All activities, results and related decisions MUST be logged and available for review. An independent third party should be able to review those processes, if required.
7.2.10.	DWP Security Incident Response and Communication process MUST be followed to ensure appropriate DWP stakeholders are alerted during a security incident. In the event of a very high risk security incident the DWP CSO, SIRO and Permanent Secretary MUST be notified immediately. The DWP CSO and SIRO will then advise the Permanent Secretary on steps to take and to consider notifying Ministers.

7.3. Collection and Preservation of Evidence

Reference	Security Control Requirement
7.3.1.	All digital evidence MUST have a security data classification. If for any reason the security classification of the digital evidence is not determined at the time of acquisition, the highest level of security data classification MUST be applied to all evidence collected. The digital evidence could be re-classified following initial response and triage.
7.3.2.	All appropriate DWP policies, general forensic and procedures (such as ACPO Good Practice Guide for Digital Evidence) MUST be followed while collecting, storing and preserving the evidence.
7.3.3.	Any external agency responsible for evidence collection and preservation MUST be compliant with the DWP principles.
7.3.4.	All digital evidence MUST be collected only by digital professional forensic technicians. In some cases (such as cloud computing), due to system access, evidence will occasionally have to be collected by administrators under the guidance of an expert in digital forensics.
7.3.5.	All actions taken upon acquiring digital evidence and during the imaging or copying process (such as date, time, location of the image or copy was made, who performed the action, who witnessed it and the tools and program used) MUST not change the actual evidence which may subsequently be relied upon in court. In an exceptional case, where it is necessary to access original data, the person handling MUST be competent and provide evidence explaining the relevance and the implication of their actions.
7.3.6.	All actions taken in the collection and preservation of the evidence MUST be logged, preserved and available for review. An audit trail or other record of processes applied to digital evidence MUST be created and preserved. An independent third party should be able to review those processes, if required.
7.3.7.	All digital evidence MUST be labelled to preserve the chain of custody. The chain of custody MUST be filled when an investigator assumes physical control of digital electronic artefacts (and any incorporated storage devices). Storage devices MUST be removed either by powering down the device or by removing the power source. The following information regarding the collection MUST be logged: • Description of the evidence • Time and Date the evidence was gathered • Exact location of the evidence from where it was gathered • Name of the person collecting the evidence • Relevant circumstances surrounding the collection • Any controls taken in consideration • Any analysis performed on the digital evidence • Disposition methods of evidence, where applicable • Transfer details, as per 10.3.8
7.3.8.	Each person who handles the evidence MUST sign the chain of custody log indicating the time they took the responsibility for the evidence and the time they handed off to the next person in the chain of custody.
7.3.9.	All digital evidence and the log of imaging and copying process MUST be stored in a secure location.
7.3.10. D	All digital evidence preserved securely MUST be monitored at least periodically. All digital evidence MUST be reviewed, stored and destroyed in accordance with the DWP Data Retention rules.
7.3.11.	All investigation and analysis on digital evidence MUST be performed on the forensic image or copy and not on the original evidence. Forensic tool MUST be used to make forensic images or copies. The hash value of the forensic image

Reference	Security Control Requirement
	MUST be verified with the original evidence to gain assurance that the evidence has not be changed by an analysis. Additional images or copies can be made if required (for example, if evidence on the copy or image is destroyed due to forensic work, a fresh copy of the original media can be made to continue with the forensics analysis). In an exceptional case, where it is necessary to access original data, the person handling MUST be competent and provide evidence explaining the relevance and the implication of their actions.
7.3.12.	All imaging and copying process MUST keep the proof of the processes carried out for audit purposes.
7.3.13.	All high and very high rated security incidents involving actionable crime must be reported to law enforcement agencies via appropriate channels. Law enforcement should be involved in the acquisition stage, but where this is not possible evidence collected by DWP staff (or their agents) should be collected in accordance with the guidelines and Chain of Custody maintained. In some case, the security data classification or evidence of an actionable crime is only known after the initial response and analysis. In those circumstances to ensure continuity is maintained, Chain of Custody and records of acquisition and analysis should be passed to the relevant law enforcement agency. Depending upon the nature of the incident, for all high and very high rated security incidents where malicious activity is identified, and assistance from NSCS is required this should be requested via Security incident process. To ensure continuity is maintained, Chain of custody and records of acquisition and analysis should be passed to the NCSC. In all circumstances, legal advice MUST be sought from DWP legal team before informing regulatory and/or law enforcement agencies.
7.3.14.	All relevant and available network activity logs (such as IDPS logs, network flow data captured by a flow monitoring system, packet captures collected during an incident, firewall and other network devices logs) MUST be collected and correlated from disparate sources to support network forensic analysis.
7.3.15.	All relevant and available logs from application or database servers MUST be investigated to identify signs of any malicious activity. A review of software code should be conducted against the hash sets of known good files that are recorded prior to the incident.
7.3.16.	Any forensic report MUST be retained as per the DWP Data Retention Policy. The summary of findings MUST be shared with SIRT as per the security incident process. The digital forensic team might carry out a technical report after the closure of security incident solely for lessons learnt purposes. The technical report MUST be retained by the DWP Tech Ops team and stored in a secured location.

7.4. Security Incident Response, Mitigation and Reporting

Reference	Security Control Requirement
7.4.1.	All security incidents MUST be managed based on the DWP Security Incident Response Readiness Process. This will provide an analytical set of operational instructions in order to assist SIRT to respond in a correct manner to a security incident.
7.4.2.	Security incident response plan document MUST be followed before activating the team during a security incident. A formal incident response plan document MUST specify who would activate the team and under what conditions. The DWP Security Incident Activity Tree and the DWP Security Incident Call Tree MUST be followed to manage and mitigate a security incident, in order of escalation.

Reference	Security Control Requirement
7.4.3.	All security incidents MUST be prioritised based on the functional impact of the incident (such as the current and likely future negative impact to business functions), the functional impact of the incident (such as effect on the confidentiality, integrity and availability of the information) and the recoverability from the incident (such as the time and types of resources that must be spent on recovering from the incident). Mechanisms MUST be put in place to monitor and quantify the types, volumes, and costs (in terms of man hours to investigate an incident) of information security incidents.
7.4.4.	All efforts MUST be undertaken to limit the effect or scope of an incident. Depending upon the nature of incident, SIRT would recommend containment steps. Containment will involve combination of technical controls, such as disconnect the affected device(s) from the network either by unplugging the network cable and leaving it running since shutdown can destroy evidence, block specific protocol or TCP/UDP port or some other network interface in order to prevent propagation of the malware, disable wireless interface while leaving the computer running, freeze log rotation in order to keep the logs intact. Containment steps MUST be followed on the affected system(s) from doing any further damage to the computer or the data on it. This steps would depend on the nature of the compromise/malware, the need for preserving evidence – don't do anything to the computer until images of RAM and the hard drive are captured, the urgency of restoring the service hosted on the affected systems and the time and resources available.
7.4.5.	SIRT MUST hand off the security measures necessary to improve security and prevent reoccurrence of the incident the Product Owner (SRO). Responsible SRO MUST ensure that the recommended mitigations are followed.
7.4.6.	Security incident if identified to be having "major impact on IT and potentially its availability" MUST follow the DWP Major Security Incident Handling Process. The 'Security Incident Response Forum' would run alongside the 'Major Service Incident Process' and alongside the 'Business Disruption' forums, to ensure that the causes, operational impacts, decisions and public communications are all aligned.
7.4.7.	A summary of the findings MUST be documented in a report. Reports will be circulated to the key DWP stakeholders, based on the severity rating of the security incident. All report documenting high rated and very high rated security incidents MUST be informed to the DWP CSO, SIRO and Permanent Secretary.
7.4.8.	Depending upon the nature and the severity level of the security incident (as identified in 10.3.13) MUST be reported to NCSC and other OGDs. SIRT in some cases, depending upon the nature of the security incident, might recommend reporting to Information Commissioner's Office (ICO). The report to ICO will be only sent on receiving an approval from DWP CSO or DWP SIRO.

7.5. Security Incident Recovery and Remediation

Reference	Security Control Requirement
7.5.1.	Compromised system MUST be restored to normal operation. It may involve restoring systems from clean backups, rebuilding system from scratch, replacing compromised files with clean versions, installing patches, changing passwords or tightening network perimeter security. Compromised system when rebuilt from scratch MUST be configured effectively and MUST be secured to a known good condition. Configuration information can be found from the configuration management and change management programs.
7.5.2.	Once the reason for the incident is established, corrective action MUST be taken and additional controls introduced to prevent the same course of events happening again in the future. This action involves working closely with suppliers and staff to close any vulnerability that existed and were exploited during the incident.

Reference	Security Control Requirement
7.5.3.	SIRT MUST hand off any outstanding risk to the department's security risk assessment team and the product owner to ensure either remediation activity is carried out or the relevant security incident risk is accepted and managed by the respective product owner. The recommended risk would also be taken to SRAF in order for the respective product owner to take the remediation steps.

7.6. Post Security Incident Review

Reference	Security Control Requirement
7.6.1.	Post security incident/lessons learnt review meeting of security incidents MUST be completed within two weeks of the security incident resolution. It is mandatory for security incident rated as high and very high.
7.6.2.	Root cause analysis MUST be performed to identify the root cause of the security incident and confirm how the security incident happened including who and what is at risk.
7.6.3.	Security incidents MUST be re-classified based on the actual impact.
7.6.4.	A follow-up report of all security incidents MUST be created and maintained. The report will be produced either during the incident closure state or lesson learned activity The report MUST be sent to all relevant attendees from the "Response Forum" and also as stated in control 10.4.6.
7.6.5.	The report of security incidents MUST be regularly reviewed as part of the information security management lifecycle to identify changes in the threat environment that might request for amendments to the security incident management plan, security risk assessment, security policy and or security standards and procedures.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process	TBD	N/A
DWP Baseline Control Set	DWP Controls Catalogue	1.0
Standard Master List	DWP Security Standards	N/A

11. Reference Documents

1. NIST Computer Security Incident Handling Guide Special Publication 800-61 Revision 2 August 2012
2. CESG Security Incident Management (GPG24) Issue No: 1.2, October 2015
3. ACPO Good Practice Guide for Digital Evidence, March 2012

12. Definition of Terms

Term	**Definition**
Contact Centre	Contact Centre is the DWP Security Advice Centre (SAC) and is the single point of contact for all DWP security enquiries.
Monitoring Team	Monitoring team is part of CRC and is the single point of contact for cyber security monitoring, threat/vulnerability assessment and incident response.
Incident Triage Matrix	In the event of an information asset being compromised the rating or the severity of the security incident is determined based on the DWP Risk Matrix.
Security Education and Awareness Team	The Security Education and Awareness (SEA) team are responsible for the security and resilience education and awareness programme within DWP.
Security Incident Response Forum	Security Incident Response Forum' would run alongside the 'Major Service Incident Process' and alongside the 'Business Disruption' forums, to ensure that the causes, operational impacts, decisions and public communications are all aligned.

13. Glossary

Abbreviation	**Definition**
CRC	Cyber Resilience Centre (CRC)
DA	Design Authority (DA)
DWP	Department of Work and Pensions (DWP)
GSCP	Government Security Classification Policy (GSCP)
ISO	Information Commissioner's Office (ISO)
NCSC	National Cyber Security Centre (NCSC)
NIST	National Institute of Standards and Technology (NIST)
OGD	Other Government Bodies (OGD)
SAC	Security Advice Centre (SAC)
SIRT	Security Incident Response Team (SIRT)
SRAF	Security Risk and Assurance Forum (SRAF)

14. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27001:2013 and NIST 800-61.

SS-14 Security Incident Management STANDARD	DWP Controls Catalogue – Baseline Control Set	
Control Statement	**Control Reference**	**Descriptor**
10.1.1	A.16.1.1 Responsibilities and procedures 5.2 Plan and Prepare (b)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.1.2, 10.1.3, 10.1.4	A.16.1.1 Responsibilities and procedures 5.2 Plan and Prepare	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.1.5	A.16.1.1 Responsibilities and procedures 5.2 Plan and Prepare (e)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.1.6	A.16.1.1 Responsibilities and procedures 5.2 Plan and Prepare (c, h)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.1.7	A.16.1.1 Responsibilities and procedures 5.2 Plan and prepare (d)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.1.8, 10.1.9, 10.1.10, 10.1.11, 10.2.1, 10.2.9	A.16.1.1 Responsibilities and procedures 5.2 Plan and Prepare (g)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.2.8	A.16.1.2 Responsibilities and procedures A.16.1.3 Reporting information security weaknesses 5.3 Detection and Reporting (a, e)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.2.2, 10.2.5	A.16.1.2 Responsibilities and procedures A.16.1.3 Reporting information security weaknesses 5.3 Detection and Reporting (b, d)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.2.3, 10.2.4, 10.2.6, 10.2.7, 10.2.10	A.16.1.4 Assessment of and decision on	ISO/IEC 27001:2013

SS-14 Security Incident Management STANDARD	**DWP Controls Catalogue – Baseline Control Set**	
	information security events 5.4 Assessment and Decision (c)	ISO/IEC 27035-1:2016
10.2.9	A.16.1.1 Responsibilities and procedures 5.3 Detection and Reporting (e)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.3.7, 10.3.8, 10.3.9, 10.3.10, 10.3.11, 10.3.12, 10.3.13, 10.3.14, 10.3.15, 10.3.16	A.16.1.17 Collection of Evidence 5.3 Detection and Reporting (d, g, d, g, d, i, l)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.4.1, 10.4.5, 10.4.6	A.16.1.4 Assessment of and decision on information security events 5.4 Assessment and Decision (b)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.4.2	A.16.1.4 Assessment of and decision on information security events 5.4 Assessment and Decision (a)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.4.3, 10.4.4, 10.4.7, 10.5.1, 10.5.2, 10.5.3	A.16.1.5 Response to information security incidents 5.5 Responses	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.4.5	A.16.1.5 Response to information security incidents 5.5 Responses (c)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.6.1, 10.6.2	A.16.1.6 Learning from information security incidents 5.6 Lessons Learnt (a)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.6.3, 10.6.4	A.16.1.6 Learning from information security incidents 5.6 Lessons Learnt (b, c, d)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016
10.6.5	A.16.1.6 Learning from information security incidents 5.6 Lessons Learnt (e)	ISO/IEC 27001:2013 ISO/IEC 27035-1:2016