SEPA

Internal Audit Report 2020/21

Cyber Attack – Lessons Learned

June 2021

SEPA

Internal Audit Report 2020/21

Cyber Attack – Lessons Learned

Audit Sponsor	*Key Contacts*	*Audit team*
[redacted]	[redacted]	[redacted]

Executive Summary

Conclusion

In December 2020, SEPA was the victim of a complex cyber-attack. SEPA decided not to pay the ransom and have been working since the attack to resume critical and essential business processes.

SEPA commissioned several reviews following the attack. This report outlines the overarching lessons learned from the following reviews:

- Azets review of SEPA's response to the emergency
- NCC Group's Incident Response Investigation Report
- SBRC's review of SEPA's preparedness prior to the attack
- Police Scotland's debrief paper

The reviews found that, for a public sector organisation of its size SEPA had in place a reasonable level of cyber security. For example, SEPA had obtained Cyber Essentials Plus certification, invested in technical protection solutions such as alert logging and monitoring solutions and antivirus solutions and conducted user phishing training. SEPA responded to the attack by quickly invoking the Emergency Management Team (EMT), rapidly identifying and prioritising critical processes, and communicating well both internally and externally.

Learnings were also identified that could support SEPA in strengthening its security posture:

- Increasing number of people and improving training for people with access to threat alerts
- Availability and testing of emergency management, disaster recovery and incident management plans
- Enhanced network segmentation controls
- Enhanced privileged account management controls
- Ensure that recovery plan activities are clearly prioritised

Background

In December 2020 the Scottish Environment Protection Agency (SEPA) was subject to a significant cyber-attack affecting its contact centre, internal systems, processes, and communications. SEPA made it clear that it will not engage with criminals intent on disrupting public services and extorting public funds. At the time this review was conducted the matter was subject to a live police investigation.

Following the attack, business continuity arrangements were enacted and SEPA's Emergency Management Team has been working with Scottish Government, Police Scotland and the National Cyber Security Centre on its response.

SEPA's approach is to take professional advice from multi-agency partners, including Police Scotland and cyber security experts, with the multi-agency response focused on eradication, remediation and recovery.

Given the scale of this incident and its considerable impact on operations, SEPA has commissioned reviews to establish: what led to this incident; what improvements are required in the recovery process; the impact of the attack on SEPA; what went well in the response and what lessons can be learnt for the management of future incidents. Due to the elevated threat on organisations from cyber-crime, SEPA is keen to identify and communicate learnings that support other organisations, particularly the Scottish public sector, in order to reduce the risk of this happening to them.

SEPA commissioned four organisations to perform reviews that together covered the elements set out above.

Scope of this paper

The purpose of a lessons learned activity following a cyber incident is to reflect, learn and improve. Lessons learned from the incident should be used to improve security measures and the incident handling process itself.

This paper is an overarching lesson learned report for SEPA. To produce this paper, information has been obtained from the following sources:

- Azets' review of SEPA's response to the emergency
- NCC Group's Incident Response Investigation Report
- SEPA's response to NCC Group Technical Forensic Investigation
- SBRC's review of SEPA's preparedness prior to the attack
- Police Scotland's debrief paper

This paper focuses on lessons learned which have been adopted by SEPA as an organisation.

Lessons learned for the wider Scottish public sector will be covered within a separate report which is being produced by Scottish Business Resilience Centre (SBRC).

Report Structure

Findings from reports have been categorised into the following areas:

- Understanding and managing areas of cyber risk
- Protection of assets
- Detecting an attack
- Responding to an incident
- Recovering from an attack

Appendix A outlines a cross-reference of findings in this paper to the original source paper.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Summary

This report collates lessons learned into the following areas:

Understanding and Managing Areas of Cyber Risk

This section relates to the development of an organisational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities. This includes understanding the business context, the resources that support critical functions, and the related cybersecurity risks which enable an organisation to focus and prioritise its efforts, consistent with its risk management strategy and business needs.

Lessons learned in this section will help SEPA to understand where to apply cybersecurity risk mitigations and therefore help to protect its assets.

Protection of assets

This section relates to the development and implementation of appropriate safeguards to ensure delivery of critical services. This supports the ability to limit or contain the impact of a potential cybersecurity event.

Lessons learned in this section will help SEPA to protect its assets by both making it hard for systems and devices to be compromised, and by restricting the access an attacker has once an individual system or device has been compromised.

Detecting an attack

This section relates to the development and implementation of activities to identify the occurrence of a cybersecurity event.

Lessons learned in this section will help SEPA to ensure timely discovery of cybersecurity events which in turn will allow SEPA to respond promptly to attacks.

Responding to an incident

This section relates to the development and implementation of appropriate responses to the detection of a cybersecurity incident.

Lessons learned in this section will help SEPA in efforts to contain the impact of a potential cybersecurity incident once it was been detected.

Recovering from an attack

This section relates to the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Lessons learned in this section will help SEPA support timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Key Themes

Areas of strength
• Cyber Essentials Plus certification • Investment in protection mechanisms such as antivirus software and access control • Investment in alert logging and monitoring software such as [redacted] • Commitment of staff following the attack • Quick invocation of Emergency Management Team (EMT) following the attack • Rapid identification and prioritisation of critical processes • Effective communication with internal and external stakeholders following the attack • Incorporation of secure design when implementing new processes and systems following the attack

Areas for improvement
• Increasing number of people with access to threat alerts • Availability and testing of emergency management, disaster recovery and incident management plans • Enhanced network segmentation controls • Enhanced privileged account management controls • Ensure that recovery plan activities are clearly prioritised

These are further discussed in the Response Assessment Findings section below.

Lessons Learned Findings

Understanding and managing areas of cybersecurity risk

Areas that went well

Cyber Maturity

- SEPA had achieved Cyber Essentials Plus certification prior to the attack.
- SBRC's review assessed SEPA's cyber maturity as high, citing the implementation and adherence to recognised frameworks and the implementation of leading practices.
- SEPA has implementing the ITIL framework around governance processes for IS change management. (Although issues were identified with its application – see CM.3).

Lessons Learned:

CM.1 Evolve the use of frameworks & leading practices

Although as noted above the ITIL framework has been adopted for IS change management, respondents identified some changes had been made to systems without following the ITIL process. (SBRC p11)

Lessons Learned:

- SEPA will review and document security standards and build audits against these standards into our ongoing audit programme.
- SEPA will seek to continue to adopt leading practice approaches, including:
    - Reviewing and where necessary enhancing our policies and processes for information and data retention.
    - Continuing to work with a range of external contractors to design and build new IS systems. This will include appropriate network design, security monitoring systems, network traffic monitoring, end point device control and back up capacity.
    - Engagement of specialist contractors to help design and deliver SEPA's security posture. We will work with them to understand the threat assessment framework that best meets SEPA's needs and fully complies with NCSC guidance. We will work with them to implement an appropriate framework and introduce an appropriate LAPS.
    - Day-to-day accounts have been separated from administrative level accounts across SEPA's systems in line with recommended leading practise.
    - SEPA have worked with external contractors to develop and introduce a new enhanced end-point design which uses [redacted] to restrict and monitor user actions such as command-line tools and actions. Users have no administrator rights on the devices and are blocked from installing software not sanctioned.

CM.2 Allocation of resources

Some staff interviewed identified that the overall IS department was sufficiently resources and did not require further resourcing though respondents identified that resources were incorrectly allocated within the department and that reallocation and retraining of resources was required. (SBRC p14)

Lessons Learned:

- Management will review the ongoing resourcing requirements of the IS function.

CM.3 Cross-organisational approach to cyber

Although SEPA has adopted ITIL based change management processes, the security implications of changes were not being consistently considered. There were different opinions among staff as to where responsibility for considering security in system change sits, with staff referencing this as occurring at either the Change Advisory Board (CAB) or being performed by the Governance Department. (SBRC p19). There is no defined standard or framework against which system security is measured. (See CM 1) It was highlighted that Information Systems were not consulted on IT associated purchases until a request to install was received. (SBRC p19)

Lessons Learned:

- SEPA have already adopted digital first standards for the design and delivery of all new services. SEPA will continue to use agile methodology with dedicated business leads embedded in the process.
- SEPA will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will go through SEPA's change Control Board and be evaluated to ensure compliance with SEPA's security and governance standards prior to installation / connectivity to the network.
- SEPA will review and introduce best practice approaches such as maturity assessments to aid with decommissioning of systems.
- SEPA will review and document security standards and build audits against these standards into our ongoing audit programme.

Protection of assets

Areas of strength

- SEPA had invested in protection mechanisms prior to the incident, such as:
    - [redacted] endpoint protection
    - Proofpoint email filtering
    - Configuration of the VDI environment
    - Firewalls
    - Automated patch management processes
    - VPN access controls
    - [redacted] Professional Vulnerability Management
    - User phishing training

- IS Department staff have separate accounts for their day-to-day operational duties and their administrative (privileged) functions which is convergent with best practice.

Areas for improvement

PA.1 Network Segmentation

The network was segmented into Virtual Local Area Networks (VLANs) however there was no access control lists (ACLs) in place to filter traffic and all sites and networks could route to each other irrespective of if there was a need to or not. (SBRC p8, [redacted])

Lessons Learned:

- SEPA are working with contractors to design, review and implement a new network configuration. SEPA have introduced [redacted] firewalls to allow the build of a new environment for outbound services. SEPA has enhanced its core Active Directory (AD) configuration by implementing the [redacted] with advanced protection and have reinforced that core service by subscribing to [redacted]. These steps were recommended by SEPA's [redacted] advisors [redacted], in order to strengthen SEPA's security profile. [redacted].

- As SEPA builds new systems, it will continue to work with a range of external contractors to design and build new IS systems. This will include appropriate network design, security monitoring systems, network traffic monitoring and end point device control and back up capacity.

PA.2 Privileged Account Management

A limited number of users have local administrative rights to facilitate their roles [redacted] Once compromised, this facilitates lateral movement and privilege escalation. (SBRC p8, [redacted])

[redacted]

Lessons Learned:

- A new password management policy complying with current NCSC guidance has been approved by AMT and introduced. The policy includes guidance for privileged access accounts. [redacted]. They have had email and internet access disabled.

- SEPA has developed and introduced an elevated access privilege policy to manage administrator accounts. This has been applied across all SEPA domains and applications.

- SEPA have separated all day-to-day accounts from administrative level accounts across all of SEPA's systems in line with recommended best practice.

- SEPA has worked with external contractors to develop and introduce a new enhanced end-point design which uses [redacted] to restrict and monitor user actions such as command-line tools and actions. Users have no administrator rights on the devices and are blocked from installing software not sanctioned by IS.

- SEPA has reviewed the usage of all shared administrator resources. In the new limited network, SEPA has introduced only a few very tightly controlled administrative accounts. [redacted]

PA.3 Authentication

[redacted]

Lessons Learned:

- A new password policy was approved by AMT in February 2021. [redacted]

- All staff have dual reset of their passwords and access is only available via multi factor authentication.

- Sessions token revocation with two-factor authentication has been re-established in SEPA's new network.

- Multi-factor authentication for external login to SEPA services has been re-established in SEPA's new network using [redacted] multi factor authentication.

PA.4 Training & Awareness

Senior managers within the IS team had attended external cyber resilience training however no other cyber resilience training was delivered. Staff indicated a lack of training while senior managers indicated there was budget for training. This was due to expectations that employees would identify necessary training and schedule time to attend it themselves. (SBRC p18)

Lessons Learned:

- Technical training will be an important part of SEPA's recovery. This will be accessed by staff to maintain current skills and develop new skills. Prior to the incident, SEPA had signed up to [redacted]. SEPA will continue to build on this and will train further staff as required.

- When introducing a new technology platform or developing a new service, SEPA will use a blended approach working with external contractors alongside existing staff to facilitate knowledge transfer and practical learning.

- As part of the recent roll out of the [redacted] products, all staff were required to go through a mandatory "onboarding" session where cyber training was given to staff.

- SEPA will re-introduce mandatory cyber training for all staff. The take up of this training will be monitored. In addition, where there is intelligence of specific vulnerabilities, bespoke notices, advice and training will be given.

PA.5 Documentation & understanding of data held

IS documentation prior to the incident although created, was not comprehensively applied to an optimum standard, particularly in relation to old legacy systems. Documentation was not seen as a priority and pressures to deliver projects and undertaken routine maintenance took priority. [redacted]

[redacted]

Lessons Learned:

- SEPA uses data flow modelling for the design of new services. SEPA will build on this work and use it in the diagnosis and investigation of incidents going forward.

PA.6 Secure Design

Access to facilities such as the command line interface (CMD) and PowerShell were restricted to specialist users. These tools were used by the threat actor and play significant roles in the TTP's of other threat groups. (SBRC p8)

Accepted Actions:

- SEPA has made the decision to build from new rather than re-establish legacy systems. SEPA has designed a refreshed set of design principles and standards.

Detecting an attack

Areas of strength

- SEPA had invested in alert logging and monitoring mechanisms prior to the incident, such as:
    - [redacted] IDS
    - [redacted]

Areas for improvement

DA.1 Threat Detection

The [redacted] group responsible for the attack was identified in late 2019 however there was negligible threat intelligence available on the group's Tactics, Techniques or Processes (TTP's) prior to the incident.

As a result of the attack, SEPA have considered ways in which they could enhance their ability to detect cyber-attacks. One of the solutions discussed is the investment in an in-house or external Security Operation Centre (SOC). The purpose of a SOC is to provide 24/7 monitoring and response to security alerts. Operating a SOC is normally beyond the budget capacity of such a public sector organisation. (SBRC p7)

Logging and alerting were in place at the time of the attack [redacted]

Lessons Learned:

- As SEPA builds new systems, it will continue to work with a range of external contractors to review its approach to security incident management and make improvements where appropriate. This will include reviewing the available resource for security incident management, providing training for staff, development of procedures for investigating intrusion detection alerts and playbooks for dealing with identified threats. This approach will be approved by AMT and fully linked to SEPA's cyber incident response plan.

- SEPA is seeking external advice and working with partners such as Scottish Government to investigate if a 24-hour Security Operation Centre (SOC) to provide overall threat protection including monitoring, direct action and logging across the whole of SEPA's IT infrastructure is a cost effective and appropriate way forward for SEPA.

- [redacted]

DA.2 Endpoint Protection

Antivirus protections were installed on all endpoints except for thin client devices. This is an understandable risk acceptance given that user profiles and data are accessed via a Virtual Desktop Infrastructure (VDI) running antivirus. However, it was indicated that, because of VDI, users do not get to see antivirus popup warning notifications and, separately, such notifications do not get passed to the IS Support Desk. (SBRC p8)

Lessons Learned:

- SEPA has worked with external contractors to develop and introduce a new enhanced end-point design which uses [redacted] for Endpoints to restrict and monitor user actions such as command-line tools and actions. Users have no administrator rights on the devices and are blocked from installing software not sanctioned by IS.

Responding to an incident

Areas of strength

- Incident response and business continuity arrangements, including invocation of the Emergency Management Team (EMT) were promptly enacted by SEPA. Response included engagement with partners such as Scottish Government (SG), Police Scotland (PS), National Cyber Security Centre (NCSC) and [redacted] Cyber Incident Response Team ([redacted]/CIRT).

- SEPA identified critical processes quickly after the attack as those which could impact human safety. For example, Flood Warnings were prioritised and issued on 24 December 2020.

- SEPA staff showed commitment, eagerness, camaraderie and positive dedication across the response and recovery stages of the attack.

- Daily stand-up meetings within the IS team supported staff in being aware of their role and responsibilities in responding to the attack, kept staff informed and helped staff understand priorities.

- Communications with stakeholders were open, honest, and concise. Stakeholders were regularly updated. Communications were specific to the needs of each type of stakeholder.

- SEPA engaged with support partners early in the response process and used specialists to support response work where appropriate. Specifically, contact was made with the Scottish Government Cyber Resilience Unit (CRU) which instigated the national cyber incident response coordination arrangements providing structure and support at an early stage.

- The following actions taken by leadership were effective in supporting the organisations response to the attack: there were effective communications from senior leadership that commenced from the first day of the incident, the CEO took a visible lead in efforts to respond to the attack, for example the CEO chaired EMT meetings, issued media statements and led on actions such as communicating with stakeholders such as the Board and Scottish Government.
- SEPA took time at an early stage in the incident to step back and produce a broad cyber response plan with long term targets to prevent them from reacting to events as they unfolded.
- SEPA isolated its network from the wider network in the very early stages of the attack.

Areas for improvement

RI.1 Availability and testing of plans

Plans such as the Business Continuity Plan, Disaster Recovery Plan and Cyber Incident Response Plan could not be shared during the incident as there was no offline version or hard copy available. The plans, along with all the other files on the Storage Access Network (SAN), became unavailable as a result of the incident. (SBRC p13, [redacted])

Only very senior managers within the IS Department were aware of the Cyber Incident Response Plan's existence. There was an acceptance that the plan was not up to date, those who were aware of it understood their roles, responsibilities and where they fitted within the structure. There was no evidence that this plan was ever exercised. (Azets p12)

Lessons Learned:

- SEPA has established a “home” page on [redacted] to store its recovered resilience and business continuity management plans including incident and emergency management plans, Business Impact Assessment, Service Recovery Plans etc. Secure access to this site will be given to all staff who are required to access these plans. Training will be provided to staff authorised to use the site.

- SEPA’s Resilience team will work with document owners to ensure that they are kept up to date with periodic reviews.

- SEPA’s suite of business continuity and disaster recovery documentation. These will be exercised periodically.

- Document owners will ensure that, as appropriate, individuals hold hard copies of relevant plans.

- New playbook routines for the [redacted]

RI.2 Communication of an attack

The security event could not be escalated to usual security escalation contacts until approximately eight hours after the high priority alert was received on 24 December 2020. [redacted] Incident escalation processes did not require escalation to [redacted] resilience [redacted]. (Azets p16)

Lessons Learned:

- SEPA will provide refresher training and support for staff involved in the investigation and escalation of incidents.

RI.3 Incident Logging

[redacted]

- SEPA is seeking advice from external contractors on the best approach to storing and handling logs within reasonable space constraints. This work includes investigating the possibility of sending logs of all devices to a centralised logging storage area. This will allow [redacted] to implement event and incident management logging across all of SEPA’s IT infrastructure.

- SEPA will maintain its current SIRG approach for monitoring and managing incidents. On completion of the design of the network, SEPA will review its existing approach to security incident reporting and make improvements where appropriate.

RI.4 Availability of specialists

SEPA used an external, NCSC approved company to provide containments and forensic investigation services. The requirement for SEPA to secure contractors, at a cost, to undertake detailed forensic analysis that would also support any prosecution was regarded as unusual as this does not align to traditional, non-cyber crime processes. However, is recognised across Law enforcement that Private Sector CIR companies hold significant resource and capability in this regard. As such, the focus remains on a collaborative approach. (PS Debrief recommendation 1)

Lesson Learned:

- SEPA has reviewed and let a contract with a specialist cyber incident response company to ensure the availability of necessary expertise.

Recovering from an attack

Areas of strength

- SEPA has worked to incorporate secure design into their workplan to build new processes and systems.

Areas for improvement

RA.1 Backups

SEPA implemented leading practice in backups policy following the 321 principles, however, could have achieved greater maturity with increased offline storage capacity and speed. (SBRC p1)

Lesson Learned:

- SEPA will seek to review and where necessary enhance its policies and processes for information and data retention.

- As new systems are built, SEPA will continue to work with a range of external contractors to design and build new IS systems. This will include appropriate network design, security monitoring systems, network traffic monitoring, end point device control and back up capacity.

RA.2 Recovering Securely

Recovering systems back to their pre-incident state may present, if implemented, ongoing risks and vulnerabilities. (SBRC p9) It is important that a process is in place for the implementation and verification of each system/service before it goes live and before the next priority is tackled. (SBRC p22) [redacted]

Lessons Learned:

- SEPA has made the decision to build from new rather than re-establish legacy systems. SEPA has established a refreshed set of design principles and standards. SEPA will not recover unsupported systems to a production state. Legacy systems that are recovered will be designed and delivered via an appropriate environment.

- SEPA has undertaken a full active directory rebuild. [redacted]

- SEPA has blocked all IOCs in the [redacted] A separate rule has been applied to the new Checkpoint configuration. SEPA will continue to monitor CREW and CISP and other available monitoring services for compromised environments and threats and take action to block access where appropriate.

- SEPA has up to date anti-virus scanning software. In addition, SEPA has introduced a comprehensive subscription based advanced threat protection package as part of its [redacted] introduction. This includes anti-phishing, anti-spam, safe attachments, anti-malware, safelinks and domain key identified mail signatures.

- SEPA is building a new network. Devices which have been reused from the old network have been scanned and cleansed following the guidelines and processes provided by [redacted].

- SEPA will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will be verified by SEPA's Change Control board to ensure compliance with security and governance standards prior to go live.

- SEPA has secured additional technical support to further strengthen its business continuity arrangements which will include improving the resilience of its services. Particular consideration will be given to the impact of medium to long term incidents (such as Covid or Cyber) on SEPA's services.

RA.3 Recovery Plan

At the time of review, a total of 103 projects were identified that required completion before June 2021 and each of projects had dependencies. Workload is therefore now significantly greater than it was prior to the incident. The prioritisation order of these projects is unclear. It is important that this workload is constantly managed to avoid mistakes, misconfigurations and vulnerabilities. (Azets p18, SBRC p21)

Recovery past 30 June 2021 is undefined. [redacted]

Lessons Learned:

- SEPA's future workload priorities will be developed and approved through its Annual Operating Plan, which is planned to be presented to the Board in June. This will be considered in conjunction with the review of ongoing resourcing requirements of the IS function.

RA.4 Emergency Recovery

In circumstances where there has been a serious cyber-attack on an organisation, others with physical network connections to the organisation are likely to withdraw services without notice as a preventative measure. This can have unforeseen consequences. (PS Debrief recommendations 3 & 4)

Lessons Learned:

- SEPA will review existing business continuity and disaster recovery plans. SEPA will work with partner agencies and key contacts across the public sector to explore options for temporary IT and mutual aid support.

- SEPA will document all network connections with external stakeholders and engage with them on withdrawal protocols in the event of a cyber incident.

Appendix A – Cross reference of findings

Finding	Reference to original report	Reference in this report
Investigation of IDS alerts	Azets F1	DA.1
Availability of Emergency Management and Incident Management Plans	Azets F2	RI.1
Out of hours security coverage	Azets F3	DA.1
Communication of cyber attack	Azets F4	RI.2
Clarification of project priorities	Azets F5	RA.3
Recovery plan past 30 June 2021	Azets F6	RA.3
[redacted]	[redacted]	RA.2
[redacted]	[redacted]	PA.1
[redacted]	[redacted]	DA.1
[redacted]	[redacted]	RI.3
[redacted]	[redacted]	PA.2
[redacted]	[redacted]	RI.3
[redacted]	[redacted]	RI.1
[redacted]	[redacted]	PA.2
[redacted]	[redacted]	PA.3
[redacted]	[redacted]	PA.3
[redacted]	[redacted]	PA.3
[redacted]	[redacted]	PA.3
[redacted]	[redacted]	PA.2, PA.6
[redacted]	[redacted]	RA.2
[redacted]	[redacted]	RA.2
[redacted]	[redacted]	RA.2
Consider value of retaining a cyber incident response (CIR) specialist company	PS SR1	RI.4
Adapt / develop plans accessible without organisational network	PS SR2	RI.1
Adapt / develop emergency recovery structures and processes	PS SR3	RA.4
Recognise implications of network connection withdrawal by external partners	PS SR4	RA.4

Training, testing and exercising	PS SR7	RI.1
Crisis communications plans	PS SR9	RI.2
Explore options for the engagement of a SOC	SBRC R1	DA.1
Do not recover unsupported systems to a production state	SBRC R2	RA.2
Utilise business and systems analysts to work with the different business areas to identify better and more effective ways of working	SBRC R3	CM.3
Introduce suitable dataflow modelling	SBRC R4	PA.5
Security baselines	SBRC R5	CM.1
Improve cyber security posture by implementing best practices	SBRC R6	CM.1, PA.1, PA.2, DA.2 RA.1
Business Continuity, Disaster Recovery and Incident Management Plans	SBRC R7	RI.1
Restructure IS department to allow for appropriate allocation of resources	SBRC R8	CM.2
Training bundles	SBRC R9	PA.4
Cyber prevention training for all staff	SBRC R10	PA.4
Purchase and introduction of new equipment	SBRC R11	CM.3
Review workload and priorities for recovery plan	SBRC R12	RA.3
Process for implementation and verification of systems before go-live	SBRC R13	RA.2