SEPA

Internal Audit Report 2020/21

Cyber Attack - Response

June 2021

SEPA

Internal Audit Report 2020/21

Cyber Attack - Response

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.

Our review found SEPA's response following the triggering of the ransomware on December 24 2020 to be effective. SEPA communicated clearly and regularly with stakeholders, quickly mobilised an emergency management team to lead on the response to the attack, engaged with support partners, and identified critical business processes for prioritisation purposes. In addition, SEPA's leadership issued effective communications from the first day of the attack, the CEO took a visible lead in efforts to respond to the attack and SEPA have created procedures to ensure that security is built into projects going forward.

However, in line with similar sized public sector organisations SEPA's capability to identify and respond to a cyber-attack in its early stages were limited [redacted]

We have noted instances where procedures could be improved to allow SEPA to better identify and respond to incidents in the future. These include creating a process to triage and analyse security alerts raised through event monitoring tools, storing emergency management and incident management plans in hard copy offsite, improving links between on-call staff to allow for quick escalation of the incident, and designing the network architecture to allow efficient containment procedures to be carried out.

We have also noted areas where SEPA could improve their current response efforts to regain normal operational capabilities. These includes clarifying the prioritisation order for the 103 projects intended to take place in March-June 2021 and creating a high-level plan to outline the recovery efforts required beyond June 2021.

Background

In December 2020 the Scottish Environment Protection Agency 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 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. Given 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 has commissioned four organisations to cover all the elements set out above. SEPA has requested Azets to deliver the following:

- A review of the impact of the cyber-attack on SEPA; and
- A review of SEPA's response to the cyber-attack.

Azets have also been asked to produce an overarching lessons-learned report for SEPA, taking information obtained from our own work and those reviews performed by NCC Group, Scottish Business Resilience Centre (SBRC) and Police Scotland.

SBRC will also produce an over-arching lessons learned report for the Scottish public sector.

Scope of this review

This review sought to assess the adequacy of SEPA's response to the cyber-attack, including the initial and ongoing response. The review considered what went well and what areas there are for improvement.

The review considered the effectiveness of SEPA's invocation of Emergency Management, Business Continuity, incident management arrangements and recovery plan to:

- respond to the incident, including the initial response upon identification, communication with Agency Management Team and wider senior management, staff, partners, police and customers
- reduce the risk of further attacks
- recover and maintain priority business services
- recover communication systems (email/Teams)
- build essential business systems
- recover data/ information
- obtain support from partners: Scottish Government Cyber Resilience, Police Scotland; Scottish Government Sponsorship Team.

The review also considered identification and management of risks and issues relating to the response.

The review was performed via interviews with approximately 20 members of SEPA staff who were involved in response efforts. Where possible, we also obtained and reviewed evidence.

Acknowledgements

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

Control Assessment

Assessment of control areas

We rated each improvement action both in terms of the impact the issue had in this instance and generally against best practice. Two ratings are given as some issues did not have a severe impact in this scenario but could have caused a bigger impact in other situations and therefore need to be addressed. See appendix A for definitions of grades.

Type of findings

Six improvement actions have been identified from this review, five of which relate to the design of controls and one of which relates to the operation of controls in place.

Finding	Severity in this scenario	Rating against leading practice
1. Investigation of Intrusion Detection System alerts	Grade 3 Design	Grade 4 Design
2. Emergency Management and Incident Management Procedures.	Grade 2 Design	Grade 4 Design
3. Out of hours access to systems management tools	Grade 2 Design	Grade 3 Design
4. Communication of cyber attack	Grade 2 Operation	Grade 3 Operation
5. Clarification of project priorities	N/A	Grade 2 Design
6. The recovery plan past 30 June	N/A	Grade 3 Design

Reasons for ratings are given within the Areas for Improvement section later in the report.

Key findings

Areas where SEPA responded effectively to the attack

- The EMT was invoked early after identification of the attack. A communication tool which was separate to the SEPA network was used to coordinate meetings. Management teams were suspended, and all work was directed by the EMT.
- 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.
- Communications with stakeholders were transparent 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.
- 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 have worked to incorporate secure design into their workplan to build new processes and systems.

Areas for improvement

- [redacted]
- Emergency Management and Incident Management Procedures were not held offline and offsite by key individuals and therefore became inaccessible when access to systems was lost. This meant that EMT members and Information Systems (IS) staff had to rely on their knowledge and experience for emergency management and cyber response procedures.
- [redacted]
- [redacted] **staff responded to the attack just after midnight on 24 December 2020 but could not escalate it to normal escalation contacts until the morning** [redacted]
- The workplan for March-June 2021 includes 103 projects. **Prioritisation order of these projects is unclear**.
- The recovery plan past 30 June is undefined. [redacted]

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

Response Assessment Findings

Areas where the SEPA response was effective

Emergency Communications

Our review found that SEPA was able to issue communications to staff on the first day of the event 24 December 2020 using their BCMS (business continuity messaging service), a service that SEPA had invested in. Communications continued to be issued to staff regularly thereafter by using the BCMS to hold weekly management and “all staff” calls to give updates. Staff were given the opportunity to ask questions at these sessions and slots were also made available for the staff union. [redacted]

Partners such as Scottish Government and Police Scotland were engaged with early. Partners, actions to communicate with them and action owners were identified at the first EMT meeting which took place at 9.30am on 24 December 2020. Partners have been given updates throughout the response by attending Operation Claybill meetings and receiving weekly performance reports.

Communications issued to the media were concise and factual. Staff were instructed not to speak to the media about the attack as it was an ongoing Police investigation. Media statements were reviewed by the CEO, Scottish Government and Police Scotland before being issued.

Due to the potential threat to personal data, the breach was reported to the Information Commissioners Office (ICO) at 3.15pm on 24 December 2020 and SEPA followed up with the ICO on 4 January 2021 to confirm that they have received the notification. SEPA have been attending regular meetings with the ICO to keep them updated.

Invocation of the Emergency Management Team (EMT)

The attack was first identified at 0:01 on 24 December 2020. [redacted] staff [redacted] responded to the attack during the early hours of the 24 December 2020. The incident was widely escalated at about 8am. The first Emergency Management Team (EMT) meeting occurred at 9.30am on 24 December 2020.

The EMT meeting was coordinated using [redacted] which is an audio and web conferencing system, [redacted] was part of SEPA’s resilience capabilities as it is separate to the network and therefore can be used in cases where SEPA’s network is unavailable. Two members of the EMT had [redacted] downloaded on an isolated SEPA device and could therefore arrange EMT meetings.

All management teams were suspended, and all work was directed by the EMT.

Use of support partners and specialists

Our review identified that SEPA engaged with and accepted help from support partners such as Scottish Government and Police Scotland from early in the response process. For example, [redacted] Manager was assigned as the Technical Lead for the forensic investigation to assist [redacted] This allowed [redacted] to have access to an individual with knowledge of SEPA's network architecture whilst performing their investigation.

SEPA has engaged a range of specialist companies to support recovery. These include independent security, networking and communication and software licensing specialists. [redacted]

SEPA also embedded senior members of the Scottish Government's IT team to provide advice to the recovery team[redacted]

We also found that SEPA engaged [redacted] to carry out a forensic investigation on the first day of the incident.

Recovery of critical services, e.g., Flood Warning System

Although they did not have access to their emergency management and incident management plans, SEPA staff clearly understood their critical processes as those critical to human safety. The continuity of these processes was prioritised. For example, SEPA prioritised and were able to issue flood warnings on 24 December 2020 even though an automated part of the process had been impacted by the attack.

Secure Design

Our review found that since the attack, SEPA have pro-actively worked to ensure that security is built into new processes and systems to limit the impact of a future attack. For example, the Information Governance team have created a project governance checklist. The checklist is intended to be used to ensure that the standing up of new systems and processes is performed securely and considers aspects such as data protection, resiliency, IT change process, risk management and COVID safe assessments.

In addition to the Information Governance checklist, information classification levels have also been re-established and reinforced. Documents are assigned an information classification level and managed in accordance with the associated level of sensitivity.

Leadership and commitment

The CEO played a significant and high-profile role in leading SEPA's response to the cyber-attack. The EMT was chaired by the CEO and included various other members of the agency management team who were involved in evaluating the situation and making key decisions. Unison, SEPA's recognised Trade Union also sat on EMT.

The CEO and other members of the Agency Management Team reported to the Board giving them updates and the opportunity to challenge decisions made by the EMT.

The CEO was also the accountable lead internally for issuing media statements. The CEO gave statements which had been agreed in conjunction with Scottish Government and Police Scotland. Media statements were given in a calm and open manner.

Our review identified that senior leaders of SEPA placed emphasis on staff wellbeing and emotional resilience. This was through having a proactive approach in place to manage employee wellbeing and communications. Senior leaders of SEPA have also taken time off work since the attack which shows to staff the importance of taking regular breaks. The commitment and dedication shown by SEPA staff during the response has been significant. Staff have worked well beyond their normal hours and have demonstrated considerable flexibility, have worked through or given up annual leave, and public holidays.

This is in addition to working in already a complex environment because of COVID and focus on Brexit preparations.

Areas for improvement

1. Investigation of Intrusion Detection System (IDS) alerts

Issues Identified
The [redacted] Intrusion Detection System (IDS) raised [redacted] alerts on [redacted] which were triggered by the cyber-attack. [redacted] by [redacted]
[redacted]
[redacted]
Context

[redacted] is an industry leading IDS tool, many similar sized public sector bodies do not operate any IDS capability. [redacted] is one of a number of investments SEPA has made in its cyber security posture, including seeking Cyber Essentials + certification.

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

Action taken / planned
SEPA plan to explore the benefits and costs associated with engaging a Security Operations Centre (SOC) to provide 24/7 alert monitoring support [redacted]
[redacted]
Further Recommendations
[redacted]
[redacted]
[redacted]

Severity in this scenario		Rating against leading practice	
[redacted]	Grade 3 (Design)	[redacted]	Grade 4 (Design)

[redacted]

[redacted]

[redacted]

Management Action

Action:

AMT have already discussed and improved the enhancement of our security framework [redacted]

As we continue to build new systems we will work with a range of external contractors to review our approach to security incident reporting and make improvements where appropriate.

This will include reviewing the available resource for security incident management, providing training for our staff, development of procedures for investigating intrusion detection alerts and playbooks for dealing with identified threats. Our approach to security will be approved by AMT and fully linked to our cyber incident response plan.

In addition we are seeking external advice and working with partners such as Scottish Government to investigate if a 24 hours 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.

Owner: [redacted]

Deadline Date: [redacted]

2. Emergency Management and Incident Management Procedures

Issues Identified

Our review identified that emergency management and incident management procedures were not stored offline and offsite. This meant that procedures became inaccessible when system access was lost, and staff had to rely on their knowledge and experience to carry out emergency management and incident management steps.

Emergency management and incident management plans are intended to ensure that in the immediate aftermath of a serious incident, organisations can follow pre-defined steps covering all aspects of response. Due to their lack of access to the plans SEPA could not access their escalation procedures, list of prioritisation of business processes and contact details for SEPA partners.

Context

- Two people within the EMT team had downloaded [redacted] prior to the attack. This meant that they could arrange EMT meetings using [redacted] even though normal communication lines were disrupted. SEPA had recently tested emergency management plans through invoking them during the initial COVID-19 response. This meant staff were familiar with the process of invoking an emergency management team and prioritising business processes. Off-line hard copy versions of the plans were held in local SEPA offices, but these were inaccessible due to the COVID crisis. It is not clear whether any effort was made to recover these hard copies following the start of the crisis.
- [redacted] Resilience [redacted] did have access to a hard-copy of the Angus Smith Building Business Continuity Plan. In addition, [redacted] Resilience [redacted] held “Resilience Cards” in hard copy offsite. These cards contained information such as the role of EMT, examples of situations in which EMT should be invoked and considerations when invoking EMT. These Resilience Cards were used to form a bespoke Terms of Reference and agenda for EMT on 24 December 2020.
- Early in the response, SEPA identified who their partners were and worked to obtain contact details so that they could engage partners and inform them of the attack. On the 24 December IS obtained a Scottish Government Ransomware Playbook to use as an interim guide as they could not access their cyber incident response plan. By 27 of December, IS had created a high-level cyber incident response plan which they continued to reflect upon and update.

Action taken / planned

SEPA have begun uploading documents to [redacted] It is intended that [redacted] will store emergency management and incident management plans.

Further Recommendations

In addition to the actions already planned by SEPA to resolve this issue, we recommend that relevant individuals (EMT members and on-call staff) hold hard copies of plans [redacted] to ensure easy access as and when required.

Severity in this scenario		Rating against leading practice	
The impact in this scenario was not high as SEPA managed to invoke their EMT quickly after the attack, contact support partners quickly (albeit with more effort than is usually involved) and identify critical processes.	Grade 2 (Design)	In other situations where staff with good knowledge of procedures and support partners are no longer working for the company, this issue could have been more severe, and the availability of plans would have had a significant impact on the organisations ability to respond to the attack.	Grade 4 (Design)

Management Action

Action:

We have already established a 'home' page on [redacted] to store our 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. Document Owners will ensure that, as appropriate, individuals hold hard copies of relevant plans.

Owner: [redacted]

Deadline Date: [redacted]

3. Out of hours security coverage

Issues Identified
[redacted]
Context
[redacted] Considerable investment would be required to ensure 24/7 monitoring of security alerts. This is usually performed by a Security Operations Centre (SOC).
Action taken / planned
SEPA are exploring the benefits and costs associated with engaging a Security Operations Centre (SOC) to provide 24/7 alert monitoring support. This is part of ongoing discussions as there are many challenges of implementing a SOC.
Further Recommendations

[redacted]

[redacted]

Severity in this scenario		Rating Against Leading Practice	
[redacted]	Grade 3 (Design)	[redacted]	Grade 3 (Design)

Management Action

Action: As we build new systems we will continue to work with a range of external contractors to review our approach to security incident response and reporting. We will continue to make improvements **(as outlined in section 1)** where appropriate. In addition we are 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.

Owner: [redacted]

Deadline Date: [redacted]

4. Communication of cyber attack

Issues Identified
We identified that [redacted] staff who initially responded was alerted to the cyber-attack at approximately 00:01 on 24 December 2020. Attempts were made to contact the [redacted] and [redacted] in line with their escalation procedures however these members of staff could not be contacted until approximately 8am because they were not on-call. During this period the on-call [redacted] staff followed the arrangements in place and worked to analyse the alert and start to carry out containment procedures. **[redacted] Resilience [redacted] was alerted via escalations from Contact Centre and Flood staff that key services were becoming inaccessible overnight on 24 December 2020, [redacted] staff [redacted] did not notify [redacted] Resilience [redacted] of the cyber-attack as [redacted] resilience [redacted] was not part of their escalation path.** [redacted]
Context
[redacted] and [redacted] escalation contacts are not on-call and therefore are not required to be contactable. The [redacted] who responded to the alert has the authority to invoke containment procedures and make changes to protect SEPA systems so inability to escalate did not impact the timeliness of containment. As noted above in addition to the IS [redacted], there is also a resilience [redacted] on-call.
Action taken / planned
None planned.
Further Recommendations

We recommend that SEPA improve awareness and communications between incident management and emergency management to all staff. If staff are part of an escalation route for emergency procedures, then they must be contactable even when out of hours.

SEPA should do this by raising awareness of different on-call teams and incorporating a cross-organisational approach in response situations within or out with normal working hours. For example, if the [redacted] of staff could not get in touch with their normal escalation contacts they should have known who the on-call resilience officer was and been able to escalate through those channels.

Severity in this scenario		Rating Against Leading Practice	
The [redacted] staff tried to escalate to the [redacted] and [redacted] but was unable to make contact until approximately 8am. The [redacted] staff did not make any attempt to escalate to [redacted] Resilience [redacted], who in this case became aware of the issue anyway due to escalation received from the Contact Centre and Flood team. **The impact was not severe as the [redacted] did not need authorisation to carry out containment procedures however non-technical aspects of the response and further escalation could have been carried out by [redacted] resilience [redacted]**	Grade 2 (Operation)	Had the responding officer made contact with [redacted] resilience [redacted], support would have been available to aid with escalating this incident. In this scenario, there were not many steps which could have been taken to limit the impact once the [redacted] had happened therefore the severity of the rating was lower. In other incidents, the engagement of [redacted] resilience [redacted] and IS escalation contacts at an earlier stage could be critical.	Grade 3 (Operation)

Management Action

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

Owner: [redacted]

Deadline Date: [redacted]

5. Clarification of project priorities

Issues Identified
SEPA have identified 103 projects which they aim to carry out between March and June 2021. It is not currently clear to wider staff what the priority order for these projects is. Lack of clarity as to what the prioritisation order is could result in blockages and project delays due to support business areas such as resilience team, data protection team, corporate legal team etc. being overwhelmed with requests for project support and not knowing which projects to prioritise. 
Context
• Management have created a workplan and have identified at a high level what their main priorities are. Management expects a cross-organisational approach to be taken when carrying out their workplan to allow discussions to take place regarding project prioritisation. • All normal Agency Management Team (AMT) business has been suspended. AMT will focus solely on the 103 projects identified. • SEPA staff are experienced in emergency management procedures and have an awareness of the importance of resilience arrangements. There is an expectation that staff will use experience and awareness to incorporate resiliency into projects.
Action taken / planned
SEPA plan to monitor project progress through updates to agency management team (AMT) meetings. AMT will make decisions on prioritisation as and when projects progress and further clarification on prioritisation is required.
Further Recommendations
We recommend that management communicate to staff what the high-level priorities are for the workplan and clearly outline which projects align to each priority area. In addition to receiving project updates at AMT meetings, we recommend that support areas report to AMT on the number of requests they have received from projects for support and any constraints on resources in allowing them to respond to requests. We also recommend that compliance checks are carried out

to ensure that projects have considered the governance requirements set out in the checklist, have records of completed forms and have obtained support from other business areas where appropriate.

[redacted]

Severity in this scenario		Rating against leading practice	
	N/A	The impact is not presently severe as there are clear reporting lines for the projects from which staff can gain clarity over the prioritisation order.	Grade 2 (Design)

Management Action

Action: AMT met on the 18th May to review the progress against the objectives in the March to June Recovery Plan and agree remedial actions; Regular updates on overall progress and specific project developments are given to the Senior Leadership Team, all Managers and all staff on a regular basis; learnings from the performance review are being fed into the development of the Annual Operating Plan.

SEPA has secured additional technical support to further strengthen our business continuity arrangements, which will include improving the resilience of our services. Particular consideration will be given to the impact of medium to long term incidents (such as Covid or Cyber) on our services. This will be considered alongside the improvements to our Incident and Emergency Management arrangements.

Owner: [redacted]

Deadline Date: [redacted]

6. The recovery plan past 30 June

Issues Identified
Our review found that SEPA have not planned any projects for recovery beyond June 2021 [redacted] The 3-month workplan plan that is currently being followed is focused on ensuring adequate service delivery and building of organisational capacity.
Context
• The focus for SEPA has been the creation of the next 3-months recovery plan. The recovery plan has been scoped out to identify critical business processes which need to be undertaken by 30 June 2021. • SEPA have documented which systems are being built from scratch instead of rebuilding existing systems, the vision for these systems and the benefits of doing so. SEPA have based decisions on criticality of the process the system supports. [redacted] • SEPA are following a set of nine principles to guide their decisions on whether systems should be re-built or build from new. [redacted]
Action taken / planned
SEPA plan to develop a 2021/22 Operating Plan during the 3-month recovery phase to be reported to the Board at the June 2021 meeting. SEPA plan to dedicate an AMT meeting to discuss this on 18 May 2021. They are also planning to run sessions mid-May to early-June on specific business areas to identify further work required and take into account the progress of the 103 projects.

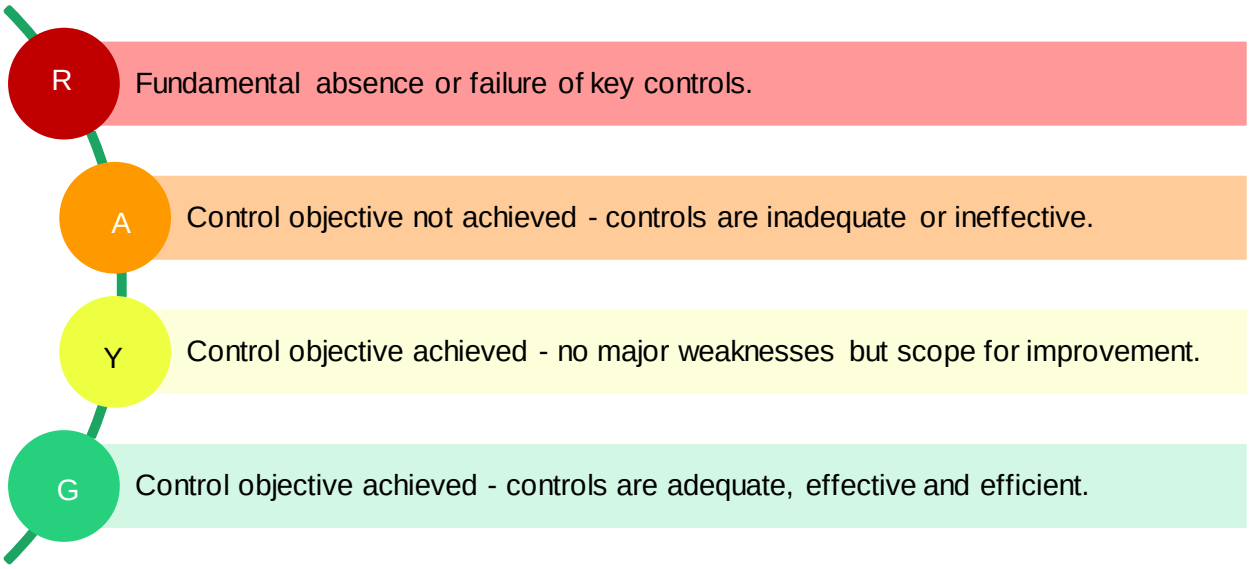
Further Recommendations
We recommend that SEPA develop a high-level plan which shows SEPA's capability at the end of each phase of recovery, the focus of each phase of recovery, what functionality SEPA needs to have before it can be considered that they have returned to normal business operations and an expected timeframe for when this will be.

Severity in this scenario		Rating against leading practice	
	N/A	[redacted]	Grade 3 (Design)

Management Action
Action: Our recovery plan for beyond 30th June 2021 will be incorporated into SEPA's Annual Operation Plan which will be presented to the Board in June. The development of this plan is well underway with a number of sessions with the Board, AMT, Strategic Leadership Team, managers and staff having been undertaken. This ambitious plan will set out a range of organisational priorities, key activities and measures of success. The plan is set against the context of the climate and nature emergency, the global pandemic and the cyber-attack. **Owner:** [redacted] **Deadline Date:** [redacted]

Appendix A – Definitions

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.