# The 2020/21 audit of the Scottish Environment Protection Agency

AUDITOR GENERAL

**Prepared by the Auditor General for Scotland**
Made under section 22 of the Public Finance and Accountability (Scotland) Act 2000
February 2022

## Introduction

**1.** I have received the audited annual report and accounts and the independent auditor's report for the Scottish Environment Protection Agency (SEPA) for 2020/21. I am submitting these financial statements and the auditor's report under section 22(4) of the Public Finance and Accountability (Scotland) Act 2000, together with this report that I have prepared under section 22(3) of the Act.

**2.** The auditor issued a disclaimer of opinion on SEPA's annual report and accounts for 2020/21. The auditor was unable to obtain sufficient audit evidence over certain transactions and balances within the financial statements. This was due to a cyber-attack and subsequent data loss on 24 December 2020 which resulted in SEPA being unable to retrieve a significant amount of its data, including underlying financial records.

**3.** I have prepared this report to draw the Scottish Parliament's attention to these issues and to highlight a number of lessons that can be learned from this cyber-attack.

## Key messages

**1** SEPA was the victim of a sophisticated ransomware attack on 24 December 2020. This led to SEPA being unable to access a significant amount of its systems and data. SEPA did not pay the ransom. More than twelve months on, it is still reinstating some of its systems. It was able to prioritise and find ways to continue delivering key services such as issuing flood alert and flood warnings within 24 hours of the attack.

**2** SEPA had to recreate accounting records from bank statements and HMRC records. The auditor issued a disclaimer of opinion on the financial statements as they were unable to obtain sufficient audit evidence to substantiate £42 million of income from contracts.

**3** SEPA's management is in the process of understanding the full financial impact of the cyber-attack on the organisation. Management is planning to bring forward the delivery of its digital strategy, focusing on creating a better, more resilient infrastructure to achieve longer-term benefit.

**4** SEPA commissioned a number of independent reviews to assist it and other public sector organisations in learning from the incident and help protect itself and others from ongoing cyber threats. The reviews concluded that SEPA had a high level of cyber maturity. They identified areas for further improvement and SEPA has accepted and is addressing the recommendations made in the reviews.

## Background

**4.** SEPA is a non-departmental public body of the Scottish Government and is sponsored by the Directorate of Environment and Forestry. SEPA's role is to protect and improve the environment and human health and contribute to sustainable economic growth. It provides two core functions:

- **Environmental regulation**: SEPA has regulatory powers and duties. SEPA helps businesses to reduce water use, carbon-based energy use, and all forms of waste and pollution, and to comply with required standards. It is the regulator of the Scottish Landfill Communities Fund and supports Revenue Scotland with the administration and collection of the Scottish Landfill Tax.

- **Flood risk management:** SEPA is Scotland's national flood forecasting and warning authority and strategic flood risk management authority.

**5.** SEPA employs 1,268 people who are based around Scotland. It is funded by Grant-in-Aid from the Scottish Government (£37.6 million 2020/21), income from contracts such as license fees paid by businesses and individuals (£42 million, 2020/21), and other income (£1.8 million 2020/21). In 2020/21, SEPA underspent against its departmental expenditure budget by £1.3 million. However, the auditor was unable to obtain sufficient audit evidence that income from contracts, and related transactions, were free from material misstatement and issued a disclaimer of opinion on the financial statements.

## Timeline of the cyber-attack

**6.** SEPA experienced a sophisticated ransomware attack on 24 December 2020. Employees and customers were unable to access SEPA's systems and data because malware (malicious software) had been installed by external agents after they gained access to the system. The majority of SEPA's data, was encrypted, stolen or lost.

**7.** SEPA immediately implemented its emergency management arrangements in response to the cyber-attack. It re-established its Emergency Management Team (EMT) to oversee the agency's response and worked with the Scottish Government, Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish Business Resilience Centre (SBRC) to deliver a recovery strategy. Appendix summarises the key timeline of events and SEPA's response.

## Independent reviews found that SEPA had a high level of cyber security maturity, but further improvements could be made

**8.** SEPA commissioned independent reviews of the cyber-attack so that it, and the wider public sector, could learn lessons. Police Scotland, SBRC and SEPA's internal auditors, Azets, were involved in the review process. The cyber-attack is subject to an ongoing police investigation.

**9.** The independent reviews made 44 recommendations for SEPA to enhance processes and controls in relation to information security. The key findings from the reviews and the auditor's follow-up discussions with management can be summarised under three areas:

- **Readiness** - How prepared and resilient were SEPA for a cyber-attack?
- **Response** - How efficient and effective were SEPA's arrangements in responding to the attack?
- **Recovery** - How effective are SEPA's arrangements in recovering from the incident and ensuring critical services continue to be delivered?

### SEPA's readiness

**10.** The auditor reported that prior to the attack SEPA had been proactive in mitigating the risk of a cyber-attack. Police Scotland's review concluded that SEPA 'was not and is not a poorly protected organisation'. It noted that as a Category 1 emergency responder, SEPA had a culture of resilience, incident and emergency management and that it regularly tested its response capabilities. This included performing a trial cyber exercise. The SBRC review noted that SEPA's cyber maturity assessment was high with the 'implementation and adherence to recognised frameworks and the implementation of best practices'.

**11.** The auditor noted that due to the sophistication of the attack the investigations to date have not identified the exact route source of where the cyber-attack breached SEPA's systems. However, there are indications that it was through a **phishing attack**. This means there may have been a degree of human error involved, which is very difficult to mitigate against.

**The NCSC defines phishing:**
'when attackers attempt to trick users into doing 'the wrong thing', such as clicking on a bad link that will download malware, or direct them to a dodgy website.'

#### Backups and data management

**12.** SEPA was unable to quickly restore its data from its backups. SEPA's backup policy was in line with best practice in that there were three copies of the data, located at two separate locations, with one copy stored offline. However, the sophisticated nature of the attack meant that online backups were targeted and corrupted at an early stage, meaning there was no way of accessing historical records quickly.

### Staff awareness and training

**13.** The independent reviews identified opportunities for enhancing staff awareness and training over cyber risk. The SBRC review found that throughout the autumn of 2020, mandatory cyber training was provided and completed by around 95 per cent of staff. SEPA plans to further roll out training and awareness across the organisation.

## SEPA's response

### Escalation routes and communication

**14.** A SEPA staff member received a system alert at midnight on the morning of the 24 December 2020 and went to a SEPA office to investigate. They were unable to reach the key senior management contact to escalate the issue at this point.

**15.** At the same time operational staff from the contact centre and flood service reported that they were unable to access systems. However, the standard escalation procedures to report such issues did not include Information Services (IS). The independent reviews have concluded that the delays in escalating the issues did not delay the response to try and contain the issue and minimise the impact.

### Leadership

**16.** SEPA is experienced in planning for and responding to emergencies. It has well-established governance arrangements in place to respond. Its EMT was reinstated on the morning of the attack and it engaged with partners including Police Scotland and the Scottish Government. It also notified the Information Commissioner's Office of the incident and potential data loss.

**17.** The EMT focused on ensuring critical systems such as the flood warning system were re-established. SEPA worked with the third parties who support the system to ensure the service continued to provide messages and alerts from that day.

**18.** SEPA has been open and transparent from the start to ensure that staff, the public and other public-sector organisations were aware what was happening. Due to the Covid-19 pandemic, most of SEPA's staff were working from home during this time. SEPA used a Business Continuity Messaging Service (BCMS) which was separate from its network to communicate with its staff.

**19.** The auditor reported that SEPA had a range of business continuity plans and incident response playbooks in place. However, these were stored on its systems and could not be accessed after the attack. Hard copies were kept in the office but only a limited number of staff could access them due to the Covid-19 restrictions. Management had to rely on their knowledge of SEPA's processes to coordinate its initial response. Had EMT and staff not been so familiar with its continuity plans and processes, its response may have been hindered. SEPA plans to establish new working practices to ensure it does not face these issues if there is a future incident.

### Recovery

**20.** The EMT established a recovery plan and identified 103 projects to deliver between March and June 2021. These included the development of basic core and regulatory functions, such as rebuilding finance systems and processes, as well as investigatory and data recovery activity. SEPA also worked with key partners including Revenue Scotland to support the continued administration of the Scottish landfill taxes.

**21.** It will take time for SEPA to fully recover from the attack. It views this as an opportunity to accelerate the delivery of its digital strategy and get longer-term benefit. It has taken the decision to build from new rather than re-establish legacy systems. It aims to transform the way SEPA operates and delivers services.

## Impact of the cyber-attack on financial management and the audit of the annual report and accounts

**22.** The auditor reported that prior to the cyber-attack SEPA had well-developed systems of internal financial control and reporting. However, the attack meant that SEPA could not access any of its financial systems and a significant amount of its data. This meant, since December 2020, Management has had limited financial information in which to monitor performance and make decisions as it prioritised re-establishing business critical systems.

**23.** SEPA was unable to record any income received or payments made or match them to pre-existing information held on its systems, such as sales and purchase orders. Many internal controls which management rely on, such as authorisation levels, are inbuilt into financial systems. Without these systems in place the control environment was weakened. Temporary financial arrangements were put in place to ensure there were appropriate controls and authorisation of expenditure, such as paying staff and suppliers.

**24.** The finance team had to recreate accounting records from the prior year trial balance and record transactions in manual journals. It created payroll/staff costs information from HMRC records, and income and expenditure information from bank records. There are inherent limitations in recreating records this way. It meant there was not the level of detail required to substantiate the completeness, accuracy and authenticity of financial transactions for 2020/21.

**25.** The auditor reported that, as part of SEPA's ongoing recovery activity, SEPA has sought to re-establish and further enhance its internal financial control arrangements.

## The auditor issued a disclaimer of opinion on the annual report and accounts

**26.** As a result of the cyber-attack and subsequent impact on SEPA's underlying financial records, the auditor was unable to obtain sufficient evidence over income from contracts (£42.097 million) to gain assurance that this was free from material misstatement or fraud, including whether income had been receipted in the correct financial year. This also impacted on bad debts written off in year (£2.197 million) and the deferred income included within trade and other payables (£11.210 million) recorded in the Statement of Financial Position.

**27.** Income from contracts is a substantial proportion of income received in the Statement of Comprehensive Net Expenditure. As such, the auditor considered this issue to be pervasive to the financial statements as a whole and has provided a disclaimer of audit opinion on the financial statements.

## SEPA does not yet know the full financial cost of the cyber-attack

**28.** Based on management forecasts during the year, the Scottish Government gave SEPA authority to overspend by £2.5 million to cover the impact of Covid-19 and the cyber-attack if required. However, as reflected in SEPA's outturn position (paragraph 5), it did not have to do so.

### Financial sustainability

**29.** SEPA recognises that the cyber-attack has increased the medium to longer term financial pressures on the organisation. Its financial strategy 2020-24 had already identified potential variability in future income and expenditure streams of up to £17.9 million as a worst-case scenario. Fully restoring its financial analysis capabilities is essential to SEPA being able to manage this variability and associated risks.

**30.** For 2021/22, the Scottish Government has confirmed Grant-in-Aid funding can be used for the recovery and re-establishment of critical systems. SEPA's management has forecast a surplus of £6.2 million that will be used to support strategic investment.

## Conclusions

**31.** The cyber-attack on SEPA's systems on 24 December 2020 was highly sophisticated and continues to have a significant impact on its operations and performance. SEPA continues to monitor its performance against 20 revised targets. It will be challenging for it to meet all of these in the coming year as it recovers and rebuilds.

**32.** Both the auditor and the independent reviews commissioned by SEPA have identified that the organisation had good cyber security arrangements in place, with a number of areas of good practice. These include, SEPA's quick response and business continuity arrangements that enabled it to continue delivering critical services, and its open and transparent communication with staff and the wider public.

**33.** The financial impact of this incident is not yet known and SEPA will continue to experience the consequences of this attack for a while to come. Key systems have been rebuilt, such as SEPAs financial accounting system, with others being built from new and data recovered or recreated securely, and this will take time.

**34.** The independent reviews identified a number of recommendations which SEPA's management has accepted. Public-sector bodies should review these recommendations and learn lessons from what has happened to SEPA. This incident highlights that no organisation can fully mitigate the risk of the ever-increasing threat and sophistication of a cyber-attack but it's crucial that organisations are prepared.

# Appendix

## Timeline of key events

| Date | Event |
|---|---|
| **Pre 24 December 2020** | • Estimated date when the cyber-attack penetrated SEPA's systems. Investigations have yet to determine the original source of the attack. However, experts believe that it was most likely through a form of phishing email.<br>• The attackers infiltrated SEPA's infrastructure undetected, leaving complex and sophisticated devices to encrypt and destroy data. This went undetected. |
| **24 December 00:00** | • The cyber-attack started with the majority SEPA's data and information being encrypted, stolen or deleted.<br>• SEPA's backup policy was in line with best practise. However, the sophisticated nature of the attack meant that online backups were targeted and impacted in the early stages of the attack.<br>• A SEPA staff member was alerted at home by automatic alarms and immediately logged onto the system to investigate. They then attended the office and, in a phased manner, began isolating and shutting down systems.<br>• Operational staff, including flood warning team, escalated issues around accessibility of key systems. |
| **24 December 08:00** | • As the event took place out of hours, further escalation was not completed until early morning.<br>• The Head of Governance was notified of the issue and contacted the IS team member who confirmed the attack. The issue was immediately escalated to the Chief Executive. |
| **24 December 09:30** | • An Emergency Management Team (EMT) meeting was established through the use of communications software held separately from SEPA's systems for business continuity purposes. |
| **24 December 09:30-11:00** | • EMT met to plan initial emergency response.<br>• Scottish Government Cyber Resilience Unit (CRU) contacted. It initiated the national cyber incident response coordination arrangements providing structure and support at an early stage.<br>• At 11:00 SEPA confirmed a serious and significant cyber-attack had occurred to staff, stakeholders and media.<br>• Data breach reported to the Information Commissioner's Office (ICO).<br>• Critical services maintained and essential flood warnings issued. |
| **31 December** | • Emergency SEPA Board meeting to discuss cyber-attack and planned response. |

| Date | Event |
|---|---|
| **14-31 January 2021** | • SEPA confirmed ongoing ransomware attack likely to have been carried out by an international serious and organised cyber-crime group intent on disrupting public services and extorting public funds.<br>• Cyber security specialists identified the theft of circa 1.2 GB of data (equivalent to a small fraction of the contents of an average laptop hard drive).<br>• Dedicated data theft support website, enquiry form and support line available for regulated business and supply chain partners. Data theft mitigation and support package made available to all staff.<br>• SEPA identify and report that data stolen is likely to have been published illegally online and establishes arrangements to notify data subjects that may be affected. |
| **28 January 2021** | • SEPA develops its overarching approach to the delivery of services for the first half of 2021.<br>• Weekly service status updates published online. |
| **February – June 2021** | • SEPA implements its recovery programme, covering 103 projects, focusing on establishing business critical systems and processes.<br>• The projects are overseen by EMT and Board and includes recreating accounting records to support the 2021 financial statements as well as financial controls and processes for 2021/22. |
| **27 October** | • SEPA publishes its lessons learned reports and hosts a webinar - Cyber-crime: ready, resilient, and responsive. |
| **Ongoing** | • Next phase of recovery and delivery focusing on the building or buying of new systems and infrastructure, rather than rebuild legacy systems. |

# The 2020/21 audit of the Scottish Environment Protection Agency



Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500 Email: **info@audit-scotland.gov.uk**
**www.audit-scotland.gov.uk**

AS.4.0