Grant Thornton

External Audit Report for Scottish Environment Protection Agency (SEPA)

Financial year ended 31 March 2021

Final External Audit Report to the Board (those charged with governance) and the Auditor General for Scotland

21 DECEMBER 2021

Contents

Your key Grant Thornton team members are:

Joanne Brown
Audit Partner
T 0141 223 0848
E joanne.e.brown@uk.gt.com

John Boyd
Audit Director
T 0141 223 0899
E john.p.boyd@uk.gt.com

Rudi Farmer
Audit Associate
T 0131 659 8543
E rudi.farmer@uk.gt.com

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our external audit process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect Scottish Environment Protection Agency (SEPA) or all weaknesses in your internal controls. This report has been prepared solely for your benefit and Audit Scotland (under the Audit Scotland Code of Practice 2016). We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Executive Summary

This table summarises the key findings and other matters arising from the external audit of Scottish Environment Protection Agency ('SEPA') and the preparation of the financial statements for the year ended 31 March 2021 for those charged with governance.

Financial Statements

Under International Standards of Audit (UK) (ISAs) and Audit Scotland's Code of Audit Practice ('the Code'), we are required to report whether, in our opinion:

- the financial statements give a true and fair view and were properly prepared in accordance with the financial reporting framework;
- expenditure and income were in accordance with applicable enactments and guidance (regularity); and,
- the audited part of the remuneration and staff report, performance report and governance statement were all consistent with the financial statements and properly prepared in accordance with the relevant legislation and directions made by Scottish Ministers.

On 24 December 2020 SEPA was subject to a ransomware cyber-attack that resulted in the organisation being unable to access a significant amount of its data. This included financial ledger records prior to the attack and all available back-ups. Following the attack, Management implemented temporary financial control arrangements for the final three months of the year and have recreated accounting records using bank transactions, prior year ledger balances and locally held information. The Finance Team undertook a significant exercise to recreate accounting records in order to prepare financial statements for the financial year ended 31 March 2021.

Given the catastrophic impact of the attack we commend Management on their ability to reproduce accounting records and prepare draft financial statements by September 2021. The issues identified below impacting our audit opinion are reflective of the underlying loss of financial information rather than the approach or response by management in preparing the financial statements.

Impact of the cyber attack on our audit

SEPA have been unable to retrieve a significant amount of its underlying financial records. This included copies of invoices and other supporting records for certain account balances. Where documentation has not been available, we sought to undertake alternative audit procedures. However, for *Income from Contracts* (£42.019 million) within the CIES, we have been unable to obtain sufficient audit evidence, in line with the ISAs, that the amounts are free from material misstatement, including whether income has been receipted in the correct financial year. This also impacts on bad debt written off in year (£2.197million) and the deferred income included within Trade and other payables (£11.210million).

Although we recognise 50% of SEPA's income is funding via grant-in-aid, this is not recorded in the CIES per FReM but the Statement of Movement in Reserves. Therefore, Income from contracts is the predominant income balance in the CIES. Given the significance of this, in the context of the CIES, we consider the inability to gain sufficient audit assurances to have a pervasive impact across the financial statements. We have therefore issued a disclaimer opinion on the financial statements. (Appendix 1)

Wider scope audit

Under the Audit Scotland Code of Audit Practice ('the Code'), the scope of public audit extends beyond the audit of the financial statements. The Code of Audit Practice requires auditors to consider SEPA's arrangements in respect of the wider dimensions of public audit covering: financial management; financial sustainability; governance and transparency; and, value for money.

In our External Audit Plan for the year ended 31 March 2021 we documented our assessment of wider scope risks and planned audit work. Through our audit procedures we have not identified any further wider scope risks. In accordance with the Code, we outline the work undertaken in response to the risks and conclude on the effectiveness and appropriateness of the arrangements in place based on the work carried out.

Financial management

As a result of the data loss from the cyber attack, including financial information, temporary financial management arrangements were put in place during the final quarter of the financial year. This has included financial performance information where there were limitations in the information available. However, SEPA did establish arrangements to ensure appropriate controls and authorisation of expenditure. As part of SEPA's ongoing recovery activity, SEPA has sought to further enhance its internal control arrangements, re-establishing systems of internal financial control that were in operation prior to the attack.

Financial sustainability

Management have yet to quantify the financial impact the cyber attack has had on the organisation. As part of the recovery process, SEPA has taken a strategic decision to build new rather than rebuild its underlying systems. This brings forward the implementation of SEPA's Digital Transformation Strategy: *Our Digital Future*, with modernisation of systems and infrastructure. It is important that SEPA revisit the financial strategy to reflect the financial impact the cyber attack has had, including the impact on expediating the implementation of the Digital strategy will have on the future financial position.

Governance and transparency

SEPA's governance arrangements were sufficiently robust to respond to challenges during the year including the Covid-19 pandemic and recovering from the cyber-attack. In response to the initial outbreak of Covid-19, between March and April 2020, SEPA formed an Emergency Management Team (EMT) to oversee response to the pandemic. SEPA's governance arrangements continued to function through the use of remote meetings and the Agency Management Team was re-established following the initial response period after the cyber attack.

Wider scope audit (continued)

Under the Audit Scotland Code of Audit Practice ('the Code'), the scope of public audit extends beyond the audit of the financial statements. The Code of Audit Practice requires auditors to consider SEPA's arrangements in respect of the wider dimensions of public audit covering: financial management; financial sustainability; governance and transparency; and, value for money.

In our External Audit Plan for the year ended 31 March 2021 we documented our assessment of wider scope risks and planned audit work. Through our audit procedures we have not identified any further wider scope risks. In accordance with the Code, we outline the work undertaken in response to the risks and conclude on the effectiveness and appropriateness of the arrangements in place based on the work carried out.

Value for money

Through taking the strategic decision to build new systems and infrastructure rather than rebuild legacy systems, SEPA will speed up the implementation of the digital transformation strategy. The Scottish government has confirmed that spending plans associated with the 2021/22 Grant-in-aid allocations can be redirected to support recovery from the Cyber attack. 2021/22 therefore represents an important year for SEPA to continue to deliver services while implementing new systems and ways of working.

With significant investment in new infrastructure and change across the organisation, there is an increase in the risks facing SEPA. This will require effective project management, including risk management, to ensure the implementation of changes do not compromise the continued delivery of SEPA's regulatory functions.

The impact of the cyber attack and SEPA's response

The cyber-attack had a significant impact on SEPA including inability to access systems and underlying data, including system back-ups and the theft of an estimated 1.2gb of data. Immediately following the Cyber attack, SEPA implemented its response. This included the Emergency Management Team meeting on the same day as the attack and emergency response plans being put in place. The EMT oversaw the agency's response to the emergency between 24 December 2020 and 31 March 2021. SEPA has 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 in response to the complex and sophisticated cyber-attack. Appendix 4 to the report provides a high level timeline of the attack and resultant actions taken by SEPA. The independent reviews have made a number of recommendations to SEPA around enhancing processes and controls in relation to cyber security and Management have agreed action plans to learn from these. These cover three key themes: readiness, response and recovery.

Acknowledgements

We would like to take this opportunity to record our appreciation for the assistance provided by the finance team and other staff amidst the pressure they were under during these unprecedented times.

Introduction

Scope of our audit work

This report is a summary of our findings from our external audit work for the financial year ended 31 March 2021 at Scottish Environment Protection Agency ('SEPA'). The scope of our audit was set out in our External Audit Plan which was presented to the Audit Committee in June 2021. The main elements of our audit work in 2020/21 have been:

- An audit of the SEPA annual report and accounts for the financial year ended 31 March 2021;
- Consideration of the wider dimensions that frame the scope of public audit as set out in Audit Scotland's Code of Audit Practice 2016 ('the Code') covering: financial management; financial sustainability; governance and transparency and value for money; relative to identified significant risks, within the audit plan; and,
- Any other work requested by Audit Scotland.

Our work has been undertaken in accordance with International Standards of Auditing (ISAs) (UK) and the Code.

This report is addressed to SEPA and the Auditor General for Scotland and will be published on Audit Scotland's website www.audit-scotland.gov.uk in due course.

Responsibilities

SEPA is responsible for preparing an annual report and accounts which show a true and fair view and that are in accordance with the accounts direction from Scottish Ministers. SEPA is also responsible for establishing appropriate and effective arrangements for governance, propriety and regularity that enable it to successfully deliver its objectives.

The recommendations or risks identified in this report are only those that have come to our attention during our normal audit work and may not be all that exist. Communication in this report of matters arising from the audit or of risks or weaknesses does not absolve management from its responsibility to address the issues raised and to maintain an adequate system of control.

Adding value through our audit work

We aim to add value to SEPA throughout our audit work. We do this through using our wider public sector knowledge and expertise to provide constructive, forward looking recommendations.

During 2021, given the significant challenges facing the organisation in recreating the accounting records and responding and recovering from the cyber attack, we had regular engagement with the Finance Team. We also remained flexible throughout the audit process recognising the challenges in producing the accounts and providing guidance on Section 22 reporting to SEPA. In addition, we engaged with our quality assurance panel to challenge our overall audit conclusions and proposed opinion.

Audit of the annual report and accounts

Key messages and judgements

We have issued a disclaimer audit opinion on the annual report and accounts. As a result of the cyber-attack and subsequent loss of underlying financial records we have been unable to obtain sufficient, appropriate audit evidence over the occurrence and accuracy of Income from Contracts recognised in the financial statements.

During the audit there was 1 adjusted misstatement to the financial statements. This related to a presentational adjustment to the cash flow statement. The financial statements have been correctly amended to reflect these adjustments. There were also 6 adjustments to the draft financial statements posted by Management in finalising the accounts. We identified 1 unadjusted misstatement to the financial statements. This related to the calculation of accruals. Audit adjustments, including those of a disclosure nature are detailed in Appendix 2.

Our audit opinion

On 24 December 2020 SEPA was subject to a ransomware cyber-attack that resulted in the organisation being unable to access a significant amount of its data. This included financial ledger records prior to the attack and all available back-ups. Following the attack, Management implemented temporary financial control arrangements for the final three months of the year and have recreated accounting records using bank transactions, prior year ledger balances and locally held information. The Finance Team undertook a significant exercise to recreate accounting records in order to prepare financial statements for the financial year ended 31 March 2021.

Given the catastrophic impact of the attack, we commend Management on their ability to reproduce accounting records and prepare draft financial statements by September 2021. The issues identified below impacting our audit opinion are reflective of the underlying loss of financial information rather than the approach or response by management in recreating accounting records and preparing the financial statements.

Basis for disclaimer opinion

SEPA have been unable to retrieve a significant amount of its underlying financial records. This included copies of invoices and other supporting records for certain account balances. Where documentation has not been available, we sought to undertake alternative audit procedures. However, for *Income from Contracts* (£42.019 million) within the CIES, we have been unable to obtain sufficient audit evidence, in line with the ISA's, that the amounts are free from material misstatement, including whether income has been receipted in the correct financial year. This also impacts on bad debt written off in year (£2.197million) and the deferred income included within Trade and other payables (£11.210million).

Although we recognise 50% of SEPA's income is funding via grant-in-aid, this is not recorded in the CIES per FReM but the Statement of Movement in Reserves. Therefore, Income from contracts is the predominant income balance in the CIES. Given the significance of this, we consider the inability to gain sufficient audit assurances to have a pervasive impact across the financial statements. We have therefore issued a disclaimer opinion on the financial statements. (Appendix 2)

Materiality

The concept of materiality is fundamental to the preparation of the financial statements and the audit process and applies not only to the monetary misstatements but also to disclosure requirements and adherence to acceptable accounting practice. Our audit approach was set out in our audit plan. We updated our materiality based upon your 2020/21 draft financial statements as detailed within the annual audit plan. Financial statement materiality was set at £1.621 million, representing 2% of gross expenditure. Performance materiality was set at £0.810 million representing 50% of our calculated materiality. This was set lower in the current year reflecting the increased risk associated with the cyber-attack. We report to management any difference identified over £81,000 (being 5% of overall materiality). We applied a lower materiality threshold for disclosures within the Remuneration Report to ensure that remuneration has been disclosed within the appropriate bandings (being £1,000).

The audit process

In accordance with our annual external audit plan, our audit work commenced in September 2021. Due to the social distancing and restrictions introduced in response to Covid-19, our audit work was undertaken remotely. As a result of the cyber security breach and Management having to recreate financial records, our audit fieldwork extended into late November as additional audit testing was required primarily over income and expenditure accounts.

We would like to thank the Finance Team and wider Management for their assistance through the audit. Given the requirement to recreate the accounting records, we commend Management in being able to produced financial statements by September 2021.

Internal control environment

In accordance with ISA requirements we have developed an understanding of the control environment in place within SEPA. Our audit is not controls based and we have not placed reliance on controls operating effectively as our audit is fully substantive in nature. As part of our audit work we have considered the impact of the cyber-attack on the control environment and the processes and controls in place to recreate accounting records and the production of the accounts. We have also considered the controls in place since the attack including those over income, expenditure, payroll and journals established since the cyber attack and found these arrangements to be reasonable.

While we did not identify any material weaknesses in the financial control arrangements established following the cyber attack, the attack, and subsequent loss of data and records means it is not possible for us to validate the controls in place during the year. In response, Management have recreated accounting records, primarily from bank information and the prior year trial balance. We have modified our audit testing approach, particularly over areas of income and expenditure during the year reflecting on these deficiencies. The impact of the cyber attack has been reported within the Annual Governance Statement and narrative included in the accounts. Following the cyber attack, SEPA implemented temporary financial control arrangements. This included access to the Agresso system as well as processes and controls over income and expenditure. During 2021/22, it is important that SEPA establishes its internal financial control framework across the organisation.

SEPA's financial performance during 2020/21

SEPA's financial statements for the year reported comprehensive net expenditure for the period of £48.4 million (Prior period: Net Expenditure of £48.591 million). The results reflected the impact of Covid-19 on the level of income from contracts, being predominantly charging scheme fees and charges. While revenue was £2.922 million below the Annual Operating Plan Budget, this was offset through areas of underspend in operating costs including property, transport and supplies and services.

SEPA received Grant-in-aid funding from the Scottish government of £42.56 million during the year. This included non-cash additional allocations of £4 million: £2 million to cover depreciation and assets impairments; and, £2 million to cover expected increase in annual leave accrual and staff costs as a result of Covid-19 on untaken leave.

The Statement of Financial Position shows a net liabilities position of £161.5 million at 31 March 2021. This is caused by a pension deficit at 31 March 2021 of £190 million. The pension deficit increased from the prior year by £73 million. This was as a result of the decrease in discount rates since the last valuation. The pension fund represents a long term liability. The pension fund set contribution rates (employer and employee) to support the ongoing funding of the Scheme and Management are satisfied that they will continue to meet these obligations as they fall due.

Management are in the process of understanding the financial impact of the cyber attack on the organisation. Based on Management's 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. However, as reflected in the outturn position, SEPA did not overspend.

Funding draw downs

Under the Scottish Government Grant-in-aid funding model, SEPA are allocated cash funding each year which is drawn down as needed. For 2020/21 SEPA's cash allocation was £35.623 million. Through Management error, during 2020/21 an additional £2.014 million of cash was drawn down in the year. This is reflected in SEPA's cash and cash equivalent's balance and the Scottish Government confirmed that the cash draw down would be offset against the 2021/22 scheduled draw downs. While we recognise that the cyber attack meant operational arrangements were not in place, it is important that Management ensure there is sufficient oversight of draw downs to mitigate the risk of excess funding in future years and the risk of potentially overspending cash balances available.

Action plan point - 1

Responding to significant financial statement risks

Significant risks are defined by ISAs (UK) as risks that, in the judgement of the auditor, require special audit consideration. In identifying risks, audit teams consider the nature of the risk, the potential magnitude of misstatement, and its likelihood. Significant risks are those risks that have a higher risk of material misstatement.

Risks identified in our Audit Plan	Commentary

Management override of controls
 	
As set out in ISA 240 there is a presumed risk that management override of controls is present in all entities. This risk area includes the potential for management to use their judgement to influence the financial statements as well as the potential to override SEPA's controls for specific transactions.
Our risk focuses on the areas of the financial statements where there is potential for management to use their judgement to influence the financial statements alongside the potential to override SEPA internal controls, related to individual transactions. The risk is heightened in the current year with all transactions effectively being recorded as journals (to recreate accounting records). Our work will consider the processes and controls established to ensure transactions recorded are complete, accurate and authorised. We will test the design of controls in place over journal entry processing and risk assess journals and select items for detailed follow up testing.
With effectively all transactions being recorded as journals, including income and expenditure accounts which may have limited supporting documentation, there are inherent limitations over the assurances we can provide over these transactions. We will obtain an understanding of the business rationale of significant transactions that we become aware of that, based on our audit knowledge and understanding, are outside the normal course of business for the entity, or that otherwise appear to be unusual.
	In response to this significant risk, our audit response was as follows:
	• We considered the design of controls in place over key accounting estimates and judgements through performance of walkthrough procedures. In particular we have considered estimates over the valuation of property, plant and equipment and IAS 19 defined benefit pension liabilities as well as other assumptions used in the preparation of the accounts.
	• As a result of the cyber attack, all transactions were recorded as journals. We assessed the control environment over the processes over recreating accounting records. In addition our Journals testing included:
	  • Assessment of the design of controls in place over journal entries, including journal preparation, authorisation and processing onto the financial ledger, including controls over retrospective review and reconciliation of accounting entries; and
	  • Risk assessment of the journals population to identify large or unusual journal entries, such as those that are not incurred in the normal course of business, or those entries that may be indicative of fraud or error that could result in material misstatement. We tested these journals to ensure they were appropriate and suitably recorded in the financial ledger.
	
	Conclusion
	Through our audit procedures performed we did not find evidence of management override of controls in our testing of journal transactions or any instances of material error. Management established controls over processing journals to recreate accounting records through journals, including limiting access to finance system to authorised users and reconciliations. We did not identify any indication of fraud or inappropriate management bias in accounting estimates that could result in a material misstatement.

Risks identified in our Audit Plan	Commentary
Risk of fraud in expenditure recognition Operating expenditure is understated or not treated in the correct period (risk of fraud in expenditure). As payroll expenditure is well forecast and agreeable to underlying payroll records, there is less opportunity for the risk of misstatement in this expenditure stream. Similarly, depreciation costs, impairment and finance costs have limited opportunity for material misstatement in the accounts. We therefore focus on other operating charges (2019/20: £19.355 million). Recognising financial performance is scrutinised against the delivery against grant in aid funding levels, we consider the greatest incentive being the risk of fraud in understating expenditure. As a result of the data loss from the cyber attack there is an increased risk around the accuracy and occurrence of expenditure. Notwithstanding the identified limitations over expenditure as a result of the cyber attack, in response to the significant risk our testing will consider the completeness, accuracy and occurrence of expenditure recorded in the year. We will have a specific focus on year end cut-off arrangements.	In response to this significant risk, our audit response was as follows: • Walkthroughs of the controls and procedures over non-pay expenditure streams including those established to recreate expenditure records following the cyber attack; • Substantive testing of non-pay expenditure throughout the year to confirm its occurrence, accuracy and completeness of recording; • Focused substantive testing of non-pay expenditure recognised post year end to identify if there is any potential understatement to ensure completeness of expenditure. We extended our sample testing to the end of August 2021 to gain assurance over completeness given the increased risk associated with unrecorded expenditure associated with the cyber-attack; • Review of creditors, where material, around the year end to consider if there is any indication of understatement of balances held at year end through consideration of accounting estimates; and • Unrecorded liability testing to confirm the completeness of year end liabilities as well as the completeness of expenditure recognised during the year. **Conclusion** Sample testing at an elevated risk level of expenditure populations did not identify any issues and transactions were agreed to payments and invoice. We also considered controls in place over the recreation of accounting records and payment processing throughout the year to gain comfort that expenditure, including that before the cyber attack, had been authorised. Controls have remained in place over authorisation of bank payments and extended post year end testing did not identify any indication of unrecorded liabilities.

Risks identified in our Audit Plan	Commentary
Risk of fraud in revenue recognition Auditing standards require us to consider the risk of fraud in Revenue. This is considered a presumed risk in all entities. SEPA receives Grant in aid funding direct from the Scottish Government. The risk of management manipulation and fraud is therefore limited. We will also be able to gain sufficient assurance this year, from our audit procedures, of the completeness and accuracy of this income source. During 2019/20 SEPA's operating income consisted of income from contracts of £44.024 million and other income of £2.4 million (not considered a significant risk of material misstatement). We therefore focus our significant risk of material misstatement on income from contracts. Given the cyber security breach and resultant data loss, Management's process for recreating income records is through bank receipts. This reduces the risk of overstatement of income up to the cyber attack. We therefore focus our risk and audit testing on year end cut-off arrangements, where it may be advantageous for management to show an enhanced/different financial position in the context of financial performance being focused on outturn position against grant-in-aid funding. In light of data loss as a result of the cyber attack and management recreating accounting records, there is an increased risk of error in the completeness and accuracy of income from contracts recognised. We therefore focus our testing on the occurrence of revenue recognised at year end including existence of receivables at the year end and the completeness and accuracy of income from contracts during the year.	In response to this significant risk, our audit response was as follows: • We performed walkthroughs of the controls and procedures over income from contracts. • We considered the processes in place to recreate income transactions to record on the ledger to ensure complete and accurate. • Substantive sample testing was undertaken over transactions during the year. As a result of the cyber-attack we were unable to agree income samples to invoices and therefore our testing was limited to bank confirmations. • We undertook alternative audit procedures to gain assurance over the amounts recognised including: circularisation of third party customers to gain independent assurance over income recognised and analytical procedures. • Sample testing of receivable balances held at 31 March 2021 through agreeing balances held to invoices and/or other supporting records. • Performed income cut-off procedures and substantive testing over pre and post year end balances, extending our testing to August 2021 to seek to obtain assurance over the completeness of income recognised. **Conclusion** As a result of the cyber attack, we were unable to obtain sufficient audit evidence to gain assurance that Income from Contracts was free from material misstatement. This was primarily due to the loss of underlying records, including invoices, to substantiate the transactions recognised. See impact of this in our disclaimer of audit opinion.

Risks identified in our Audit Plan	Commentary
IAS 19 Defined Benefit Pension Liabilities SEPA participates in the Falkirk Pension Fund, a local government pension scheme (LGPS). The scheme is a defined benefit pension scheme and in accordance with IAS 19: Pensions, SEPA is required to recognise its share of the scheme assets and liabilities on the statement of financial position. As at 31 March 2020 SEPA had pension fund liabilities of £116.806 million. Hymans Robertson LLP provide an annual IAS 19 actuarial valuation of SEPA's net liabilities in the pension scheme. There are a number of assumptions contained within the valuation, including: discount rate; future return on scheme assets; mortality rates; and, future salary projections. Given the material value of the scheme liabilities and the level of estimation in the valuation, there is an inherent risk that the defined benefit pension scheme liability could be materially misstated within the financial statements. We will consider the work of the actuary (Hymans Robertson LLP), including the assumptions applied, using the work performed by PricewaterhouseCoopers (PwC) (commissioned on behalf of Audit Scotland to review actuarial assumptions proposed by LGPS actuaries), as well as local audit assessment. We will liaise with Ernst and Young LLP as Auditors of the Pension Fund to provide assurances over the information supplied to the actuary in relation to SEPA, including assets held and membership data, and confirm joint assurances in respect of employer and employee contributions in the year. We will review and test the accounting entries and disclosures made within SEPA's financial statements in relation to IAS 19.	• From year end planning review our risk focused predominantly around the key assumptions used in the actuarial valuation, where there was an increased risk of material misstatement. • We performed walkthroughs of the controls and procedures over the valuation of defined benefit pension liabilities, including Management oversight of the valuation; • We considered the work of the actuary (Hymans Robertson UK LLP), including the assumptions applied, using the work performed by PwC (commissioned on behalf of Audit Scotland to review actuarial assumptions proposed by LGPS actuaries), as well as local audit assessment. • We obtained assurances from Ernst & Young LLP as Auditors of the Pension Fund over the information supplied to the actuary in relation to the SEPA, including assets held and membership data, and confirm joint assurances in respect of employer and employee contributions in the year. • We performed substantive analytical procedures in the year over the pension fund movements, investigating any deviations from audit expectation. • We reviewed the accounting entries and disclosures made within SEPA's financial statements in relation to IAS 19. **Conclusion** Through our audit procedures performed we did not identify any exceptions in our review and testing over IAS 19 defined benefit pension liabilities recognised in the financial statements. Through considering the work performed by PwC, we are satisfied that the assumptions applied by the actuary are reasonable. The IAS 19 defined benefit liability increased from £117 million in 2019/20 to £190 million 2020/21. While asset values had increased reflecting market performance of investments held by the pension fund, this was offset through increasing value of liabilities driven primarily through a reduction in discount rates and salary and pension increases. The overall movement is consistent with other LGPS participating bodies.

Risks identified in our Audit Plan	Commentary
Valuation of property, plant and equipment In accordance with the HM Treasury Financial Reporting Manual (FReM), subsequent to initial recognition, SEPA is required to hold property, plant and equipment (PPE) on a valuation basis. The exact valuation basis depends on the nature and use of the assets. Specialised land, buildings and gauging stations are held at depreciated replacement costs, as a proxy for fair value. Non-specialised land, buildings and vessels, are held at fair value. There are further modifications to values depending on the nature and use of assets to ensure PPE is approximately stated. As at 31 March 2020, SEPA held PPE of £35 million. Given the value of PPE held by SEPA and the level of complexity and judgement in the estimation valuations, there is an inherent risk of material misstatement in the valuation of land and buildings and vessels. The risk is less prevalent in non land and buildings assets as these are generally held at depreciated historic costs, as a proxy of fair value and therefore less likely to be misstated. SEPA appoint Cushman and Wakefield to value land, buildings and gauging stations. Century Marine value the Sir John Murray vessel. In 2019/20, Cushman and Wakefield's valuation was subject to a material valuation uncertainty, reflecting the greater uncertainty in markets on which the valuations were based as a result of COVID-19.	• We performed walkthroughs of the controls and procedures over the valuation of property, plant and equipment. • We considered the work of the valuer Cushman and Wakefield, over the valuation of land and buildings, and Centaury Marine, for the Sir John Murry vessel, including the assumptions applied, and underlying data used to undertake the valuation. • We challenged the key assumptions applied, including market data used in assets valued based on market based information such as land and buildings and the vessel. • For gauging stations, we challenged the indexation rates used by Management and the suitability of these. This included Management obtaining assurances from Cushman and Wakefield around the suitability of the BCIS rates used; • We confirmed the completeness of the data used in the valuations through agreeing to our underlying records from the prior period audit. • We performed sample testing of asset valuations to confirm that these were appropriately classified and were based on appropriate data sources and underlying valuation assumptions. • We reviewed the accounting entries and disclosures made within SEPA's financial statements in relation to valuation movements to confirm these were in accordance with the FReM. **Conclusion** Through our audit procedures performed we did not identify any exceptions in our review and testing over property, plant and equipment valuations recognised in the financial statements. We challenged Management and the valuers' on the key assumptions and methods used in the valuation to gain assurance over the completeness and accuracy of the valuations as at 31 March 2021.

Detecting Irregularities, including fraud

Irregularities, including fraud, are instances of non-compliance with laws and regulations. We design procedures in line with our responsibilities, to detect material misstatements in respect of irregularities, including fraud. Owing to the inherent limitations of an audit, there is an unavoidable risk that material misstatements in the financial statements may not be detected, even though the audit is properly planned and performed in accordance with the ISAs (UK). The extent to which our procedures are capable of detecting irregularities, including fraud is detailed below:

- We obtained an understanding of the legal and regulatory frameworks that are applicable to SEPA and determined that the most significant which are directly relevant to specific assertions in the financial statements are those related to the reporting frameworks; International Financial Reporting Standards and the FReM.
- We enquired of management and the Audit Committee, concerning SEPA's policies and procedures relating to the identification, evaluation and compliance with laws and regulations; the detection and response to the risks of fraud; and the establishment of internal controls to mitigate risks related to fraud or non-compliance with laws and regulations.
- We enquired of management and the Audit Committee, whether they were aware of any instances of non-compliance with laws and regulations or whether they had any knowledge of actual, suspected or alleged fraud.
- We assessed the susceptibility of SEPA's financial statements to material misstatement, including how fraud might occur, by evaluating management's incentives and opportunities for manipulation of the financial statements. This included the evaluation of the risk of management override of controls. We determined that the principal risks were in relation to journal entries that altered SEPA's financial performance for the year and potential management bias in determining accounting estimates. Our audit procedures involved are documented within our response to the significant risk of management override of controls on Page 10.
- The team communications in respect of potential non-compliance with relevant laws and regulations, included the potential for fraud in expenditure recognition and significant accounting estimates.
- These audit procedures were designed to provide reasonable assurance that the financial statements were free from fraud or error. However, detecting irregularities that result from fraud is inherently more difficult than detecting those that result from error, as those irregularities that result from fraud may involve collusion, deliberate concealment, forgery or intentional misrepresentations. Also, the further removed non-compliance with laws and regulations is from events and transactions reflected in the financial statements, the less likely we would become aware of it.
- In assessing the potential risks of material misstatement, we obtained an understanding of:
  - SEPA's operations, including the nature of its operating revenue and expenditure and its services and of its objectives and strategies to understand the classes of transactions, account balances, expected financial statement disclosures and business risks that may result in risks of material misstatement.
  - SEPA's control environment, including the policies and procedures implemented to ensure compliance with the requirements of the financial reporting framework.
- As a result of the information loss, there were inherent limitations in evidencing the controls in place prior to the attack, particularly over expenditure, to mitigate against the risk of fraud. In the absence of purchase orders / authorisation documentation, the key controls that we evidenced were the authorisation of payments through Bankline and Management oversight of the recreation of accounting records. However, there are inherent limitations as a result of being unable to evidence services delivered / good received.

Significant estimates and judgements

SEPA's financial statements include the following significant accounting estimates impacting on the annual accounts:

Significant estimate	Summary of management's approach	Audit Comments	Assessment
Property, plant and equipment valuations	In accordance with the FReM, SEPA is required to value Property, plant and equipment on the basis of current value in existing use. For land, buildings and Vessels, Management appointed independent valuers to undertake a valuation of these assets. For gauging stations, these assets are valued every five years with indexation applied in intervening years. The valuer has conducted the valuation in accordance with the FReM and RICS guidance and the valuation movements are reflected in the accounts.	We are satisfied that the approach adopted by SEPA is reasonable in estimating the value of property, plant and equipment and that there is no indication of management bias in the approach adopted. For land and buildings and vessels, Management obtained independent valuations of these assets as at 31 March 2021. For gauging stations, Management used publicised BCIS rates. We challenged Management on the suitability of these rates who obtained independent assurance from Cushman and Wakefield that the rates applied were suitable.	● [Light Purple]
Recreating accounting records	In recreating accounting records a key area of judgement made by Management was in relation to income recognised in year. Management predominantly used cash receipts during the year (and post year end) to recreate Income records during the year. Management also used an aged debtors report from November 2020 as a source to record income and matched the debtors at this date to cash receipts. There was a residual £2.197 million of debtors as at 31 March 2021 for which no cash had been received by end August 2021 (creating accounts) and therefore Management have fully provided against this balance on the assumption income will not be received.	As noted earlier in the report we are unable to obtain sufficient assurance around the £2.197 million of income (or subsequent write off). We are satisfied however that as SEPA have yet to receive any of the balance due and have no underlying records (invoices etc) to substantiate the claim on the income it is considered reasonable to provide for the amounts as at 31 March 2021 and exclude from debtors.	● [Light Purple]

Significant estimate	Summary of management's approach	Audit Comments	Assessment
IAS 19 Defined benefit pension liabilities	SEPA engage Hymans Robertson UK LLP provide an annual IAS 19 actuarial valuation of the Authority's net liabilities in the pension scheme. There are a number of assumptions contained within the valuation, including: discount rate; future return on scheme assets; mortality rates; and, future salary projections. These key assumptions are discussed with the actuary to inform the report. These are predominantly informed by the actuaries recommended assumptions. The Head of Finance reviews the draft actuarial valuation. The output is also reviewed by the Chief Officer Finance as part of accounts production process to ensure appropriate and any significant movements or unusual entries discussed with the actuary.	As noted in our Response to significant risk section, using the work of PwC we reviewed the key assumptions underpinning the actuarial valuation. We are satisfied that the assumptions adopted were appropriate for SEPA and that those applied were considered reasonable i.e. within our acceptable tolerances. We did not identify any indication of management bias in the underlying assumptions applied in the estimate and found that Management have disclosed the key sensitivities surrounding these in the draft financial statements.	● [Light Purple]

Assessment

● Dark Purple	We disagree with the estimation process or judgements that underpin the estimate and consider the estimate to be potentially materially misstated
● Blue	We consider the estimate is unlikely to be materially misstated however management's estimation process contains assumptions we consider optimistic
● Grey	We consider the estimate is unlikely to be materially misstated however management's estimation process contains assumptions we consider cautious
● Light Purple	We consider management's process is appropriate and key assumptions are neither optimistic or cautious

Other judgements disclosed in the accounts

Management have also identified the following areas of judgement and estimation in the accounts which we do not consider of critical judgements or material estimates that would change over the next 12 months:

- Evidence used to assess impairment in trade receivables
- Estimated cost of decommissioning
- Valuation of life assurance liability.

We would consider these areas of application of accounting policy rather than areas of judgment in applying accounting policies. IAS 1 requires disclosure of significant estimates where there is a risk these could change material over the next 12 months. While the financial statements cover those areas of critical judgement and estimation there is an opportunity to enhance the disclosures made in accordance with IAS 1. This includes providing the reader clarity around the key assumptions and areas of estimation that could result in a material change in the coming period and sensitivities surrounding these. In addition, the note should disclose areas where judgement has been made in applying accounting policy (not included within estimates). We would not consider life assurance liability or decommissioning costs to meet this definition. See Appendix 2.

Other key elements of the financial statements

As part of our audit there were other key areas of focus during the course of our audit. Whilst not considered a significant risk, these are areas of focus either in accordance with the Audit Scotland Code of Audit Practice or ISAs or through due to their complexity or importance to the user of the accounts.

Issue	Commentary
Matters in relation to fraud and irregularity	It is SEPA's responsibility to establish arrangements to prevent and detect fraud and other irregularity. As auditors, we obtain reasonable assurance that the financial statements as a whole are free from material misstatement, whether due to fraud or error. We obtain annual representation from Management regarding Management's assessment of fraud risk, including internal controls, and any known or suspected fraud or misstatement. We have also made inquires of internal audit around internal control, fraud risk and any known or suspected frauds in year. No instances of fraud or suspected fraud have been notified to us.
Accounting policies	We have evaluated the appropriateness of SEPA's accounting policies, including accounting estimates. We are satisfied that the accounting policies are in line with the FReM and consistent with previous years.
Matters in relation to laws and regulations	As a result of the cyber attack SEPA were non-compliant with PAYE and VAT regulations for several months. Following ongoing dialogue with HMC SEPA have made payments to account to mitigate the risk of penalties and interest payments. Management believe that in the event any penalty is imposed, there will be grounds for appeal and therefore while uncertain, any financial impact is unlikely to be material. In addition, following the attack SEPA notified the Information Commissioner's Officer (ICO) of the data theft. The ICO subsequently investigated the personal data breach and issued SEPA with a reprimand. You have not made us aware of any further significant incidences of non-compliance with relevant laws and regulations and we have not identified any incidences from our audit work.

Issue	Commentary
Matters in relation to related parties	As a result of the cyber attack, SEPA does not have a complete record of all third parties in which it has transacted with during the year. Consequently, the identification of related parties is restricted to those third parties for which it does have records of income for. Based on our review of prior year related party disclosures and understand of the organisation as well as testing performed over the data held, we are satisfied that there are no material related parties out with those currently disclosed.
Other information	We are required to give an opinion on whether the other information published together with the audited financial statements (including the Annual Report), is materially inconsistent with the financial statements or our knowledge obtained in the audit or otherwise appears to be materially misstated. As described in the Basis for disclaimer of opinion section of our report, we were unable to determine whether any adjustments might have been found necessary in respect of Income from Contracts or associated deferred income balances within Trade and Other Payables and issued a disclaimer of opinion on the financial statements. Accordingly, we have concluded that where the other information refers to amounts in the financial statements it may be materially misstated.
Remuneration and Staff report	We are required to give an opinion on whether the parts of the Remuneration Report and Staff Report subject to audit have been prepared properly in accordance with the Accounts Direction including the disclosure requirements as detailed within the FReM. We have audited the elements of the Remuneration and Staff Report, as required, and are satisfied that these have been prepared in accordance with the Accounts Direction including the disclosure requirements detailed within the FReM.
Matters on which we report by exception	We are required by the Auditor General for Scotland to report to you if, in our opinion: adequate accounting records have not been kept; or the financial statements and the audited part of the Remuneration and Staff Report are not in agreement with the accounting records; or we have not received all the information and explanations we require for our audit there has been a failure to achieve a prescribed financial objective. As a result of the matter, explained in our disclaimer of opinion, we have determined that adequate accounting records have not been kept and we have not received all information and explanations required for our audit.

Issue	Commentary
Governance statement	The governance statement is included within the Accountability Report. The report outlines the governance framework in place at the SEPA. The Report includes the Statement of the Accountable Officer's responsibilities and had been prepared in accordance with the FReM. In accordance with the Scottish Public Finance Manual (SPFM), the Accountable Officer has a specific responsibility to ensure that arrangements have been made to secure Best Value and this is confirmed in the narrative in the annual report and accounts. The governance statement highlights the areas of development over the coming year for SEPA to enhance its internal control, risk management and governance arrangements. The statement recognises the impact that the cyber attack has had on the organisation, the arrangements established in response to the attack and ongoing development of systems of internal control over the coming year. Because of the matters described in the report in relation to the disclaimer of our audit opinion, we do not express an opinion on the whether the information given in the Governance Statement is consistent with the financial statements and that report has been prepared in accordance with section 45(2) of the Environment Act 1995 and directions made thereunder by the Scottish Ministers.
Written representations	A letter of representation has been requested from SEPA, including specific representations, which is included in the Audit Committee papers. Specific representations have been requested from management in line with prior years and confirms as auditors all records have been made available to us.
Going concern	In performing our work on going concern, we have had reference to Statement of Recommended Practice – Practice Note 10: Audit of financial statements of public sector bodies in the United Kingdom (Revised 2020). The Financial Reporting Council recognises that for particular sectors, it may be necessary to clarify how auditing standards are applied to an entity in a manner that is relevant and provides useful information to the users of financial statements in that sector. Practice Note 10 provides that clarification for audits of public sector bodies. Practice Note 10 states that if the financial reporting framework provides for the adoption of the going concern basis of accounting on the basis of the anticipated continuation of the provision of a service in the future, the auditor applies the continued provision of service approach set out in Practice Note 10. The financial reporting framework adopted by SEPA meets this criteria, and so we have applied the continued provision of service approach. In accordance with Audit Scotland guidance: Going concern in the public sector, we have therefore considered Management's assessment of the appropriateness of the going concern basis of accounting and conclude that: • a material uncertainty related to going concern has not been identified • management's use of the going concern basis of accounting in the preparation of the financial statements is appropriate.

Wider scope audit

This section of our report sets out our findings and conclusion on our audit work on the wider scope audit dimensions: financial management; financial sustainability; governance and transparency and value for money. We take a risk based audit approach, utilising our cumulative audit knowledge of the organisation and understanding of its risks and priorities. Within our annual audit plan we identified significant wider scope risks in relation Financial Management, Financial Sustainability, and Governance and Transparency, including the impact of the cyber-attack on SEPA. As part of our audit work we have not identified any further wider scope audit risks.

Wider scope dimension	Wider scope risk identified in our audit plan	Wider scope audit response and findings	External Audit conclusion
Financial Management Financial management is about financial capacity, sound budgetary processes and whether the control environment and internal controls are operating effectively	The cyber attack has had a significant impact on SEPA's financial management arrangements including financial processes, systems and controls. As part of SEPA's recovery programme, the organisation is looking to re-establish its financial control environment. SEPA established interim arrangements to support critical services following the attack including basic payroll functionality and payment of suppliers. A key challenge for SEPA is to establish systems and processes, with sufficient and robust testing, while continuing to operate.	Following the cyber attack, the majority of SEPA's operations were suspended as a result of staff being unable to access core systems, applications or data. Management prioritised the recovery of core functions and implemented a redeployment programme to enable staff support critical recovery activity and prioritising key services. Management recognise that there was inevitably a period of inefficiency as a result inactivity and underutilisation of groups of staff. Prior to the cyber attack, SEPA had well developed systems of internal financial reporting, including reporting of performance to Management and Non-Executives. However, since December Management have had limited financial information in which to monitor financial performance and make decisions. As part if the recovery programme, the Finance Team had three key workstreams: re-establishing key financial systems such as payroll, invoicing and expenditure; recreating accounting records to support the production of the 2021 financial statements including a new version of Agresso finance system (Agresso v1); and, creating a new system for 2021/22 and beyond (Agresso v2) and subsequent Management information.	As a result of the data loss from the cyber attack, including financial information, temporary financial management arrangements were put in place during the final quarter of the financial year. This has included financial performance information where there were limitations in the information available. However, SEPA did establish arrangements to ensure appropriate controls and authorisation of expenditure. As part of SEPA's ongoing recovery activity, SEPA has sought to further enhance its internal control arrangements, re-establishing systems of internal financial control that were in operation prior to the attack.

Wider scope dimension	Wider scope risk identified in our audit plan	Wider scope audit response and findings	External Audit conclusion
Financial Management (continued)	With various workstreams underway as the organisation looks to establish key services it will be important that there is sufficient capacity and oversight to ensure appropriate financial controls are in place to support effective and efficient use of resources while delivering key services, alongside the delivery of a range of projects. In response to the wider scope risk, we will consider the financial management arrangements established by Management in response to the cyber attack as well as the arrangements developed to support the organisation remobilise its services including financial monitoring and reporting arrangements.	Management have made good progress in re-establishing key financial processes. However, further work is required to establish the Agresso 2 system as an operating system used across the whole organisation.	

Wider scope dimension	Wider scope risk identified in our audit plan	Wider scope audit response and findings	External Audit conclusion
Financial sustainability Financial sustainability looks forward to the medium and longer term to consider whether SEPA is planning effectively to continue to deliver its services or the way in which they should be delivered.	SEPAs 2020-2024 Financial Strategy contained scenario based forecasts over the period of the strategy. SEPA projected that by 2024 there was an estimated budget gap of between £6,000 (best case scenario) and £17.9 million (worst case scenario). SEPA were in the process of implementing a strategic change programme, aiming to ensure resources are prioritised on key strategic outcomes. Part of this was the removal of 50 Full Time Equivalent posts and reducing staff costs by approximately £2.5 million per annum alongside alignment of regulatory expenditure with charging. SEPA has estimated that the cost in addressing the cyber attack is approximately £1.2 million up to 31 March 2021, with potentially further costs in 2022. In addition, Management has estimated that it will need to write off approximately £2 million of revenue in the year that it will be unable to collect in fees due to loss of underlying records.	Response to significant risk: The cyber attack has had a significant impact on SEPAs operations and underling financial plans. The Financial Strategy 2020-24 had already identified potential budget gaps of up to £17.9 million. Management have been unable to fully quantify the financial impact on SEPA of the attack. Alongside investing in new infrastructure, applications and ways of working, SEPA will need to ensure continued focus on the continued delivery of critical services. In response to the cyber attack, rather than rebuild legacy systems, SEPA have proposed investing in new, fit for purpose IT infrastructure and systems to deliver SEPA's Digital Transformation Strategy: *Our Digital Future*. It is envisaged that in doing so this will help transform how SEPA operates driving efficient and effective ways of working. For 2021/22 the Scottish Government has confirmed Grant-in-aid funding can be used for recovery and re-establishment of critical systems. Management have budgeted for £6.2 million of capital investment from Scottish Government funding.	Management have yet to quantify the financial impact the cyber attack has had on the organisation. It is important that SEPA revisit the financial strategy to reflect the financial implications the attack has had on the organisation. This includes understanding the cost to the organisation as well as well the impact of expediating the implementation of the Digital Transformation Strategy. With the implementation of the Digital strategy and rationalisation of IT systems there may be opportunities to generate increased efficiencies over the coming years. *Action Plan Point – 2*

Wider scope dimension	Wider scope risk identified in our audit plan	Wider scope audit response and findings	External Audit conclusion
Governance and transparency Governance and transparency is concerned with the adequacy of governance arrangements, leadership and decision making, and transparent reporting of financial and performance information.	Significant risk identified: As outlined within our audit plan we identified a significant wider scope audit risk in relation to governance arrangements as a result of the cyber attack. We have consider the impact of the cyber attack, including governance arrangements, below. As part of our wider scope audit work we consider SEPAs governance arrangements in response to the Covid-19 pandemic.	Response to significant risk: Governance arrangements during Covid-19 Following the initial outbreak of Covid-19, between March and April 2020 SEPA formed an Emergency Management Team (EMT) to oversee response to the pandemic, focusing on adapting to help the nation get through the public health emergency in a way that protects and improves Scotland's environment and communities. The organisation transitioned to remote working arrangements and reestablishment of standard working practice. This included Board and committee meetings which took place virtually. We did not identify any significant issues as a result of governance arrangements as Covid-19.	SEPA's governance arrangements were sufficiently robust to respond to challenges during the year including the Covid-19 pandemic and recovering from the cyber-attack. SEPA's governance arrangements continued to function through the use of remote meetings and the Agency Management Team was re-established following the initial response period.

Wider scope dimension	Wider scope risk identified in our audit plan	Wider scope audit response and findings	External Audit conclusion
Value for money Value for money is concerned with using resources effectively and continually improving services.	No significant wider scope risks identified	Through our cumulative audit knowledge and planning risk assessment we did not identify any significant audit risks in relation to the SEPA's value for money arrangements. Immediately following the Cyber attack, the EMT sought to re-established core services with priority being those relating to health and safety i.e. flood warning systems and alerts. This included ensuring that flood alerts were issued on 24 December 2020. The EMT established a recovery plan covering 103 individual projects as it has sought to re-establish its core service, including regulatory responsibilities. This includes Regulation including permits, waste management licences, flood alerts and mapping. SEPA have worked with key partners including Revenue Scotland to support Scottish Landfill tax services. A number of these are through temporary arrangements as SEPA builds its infrastructure and systems. In addition, there are a number of services that SEPA are unable to deliver or deliver in full including: flood mapping; enabling access on the public register; and waste consignment notes and other services. SEPA continues to work towards re-establishing these services over the coming year. Management have sought to maximise opportunities arising from the attack through expediating the implementation of SEPA's Digital Transformation Strategy: *Our Digital Future*. SEPA, in dialogue with the Scottish Government, have proposed bringing forward investment in its it infrastructure and digital capability, including moving to cloud based systems. Instead of rebuilding legacy systems, the focus is on building new, future ready operating systems. This will require higher initial upfront investment.	Through taking the strategic decision to build new systems and infrastructure rather than rebuild legacy systems, SEPA aim to expediate the implementation of the Digital Transformation Strategy. SEPA hope to achieve longer term benefit and value for money as more resilience in light of the cyber attack. The Scottish government has confirmed that spending plans associated with the 2021/22 Grant-in-aid allocations can be redirected to support recovery from the Cyber attack. 2021/22 therefore represents an important year for SEPA to continue to deliver critical systems while implementing new systems and ways of working. With significant investment in new infrastructure and change across the organisation, there is a significant increase in the risks facing SEPA. This will require effective project Management and risk management to ensure the implementation of significant changes does not compromise the continued delivery of critical functions.

Impact of the cyber attack

Significant risk identified through our audit plan:

SEPA established emergency management arrangements in response to the cyber-attack. While the Board and Audit Committee meetings continued to operate, the loss of data and access to the performance information resulted in limitations on the performance information that can be provided to the Board. SEPA commissioned a joint review of the cyber attack. The review involved Police Scotland, Scottish Business Resilience Centre, NCC Group, and Azets. The review considered what led to the incident and why, what impact the incident had on SEPA; what improvements are required in SEPA's recovery to avoid a repeat of this incident; what went well in SEPA's response and learning lessons for the management of future incidents. As part of our external audit we have considered the impact of the cyber-attack on SEPA and the findings of the joint review.

Audit findings

In response to the Cyber attack, SEPA immediately implemented its response to the challenges faced. Following the initial identification of the cyber attack the Emergency Management Team (EMT) had met on the same day and emergency response plans put in place. SEPA re-established the EMT to oversee the agency's response to the emergency between 24 December 2020 and 31 March 2021. SEPA has 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 in response to a complex and sophisticated cyber-attack. Appendix 4 to the report provides a high level timeline of the attack and resultant actions taken by SEPA in response to the attack. The independent reviews have made a number of recommendations to SEPA around enhancing processes and controls in relation to cyber security and Management have agreed action plans to learn from these. The key findings from these reviews and our follow up discussions with SEPA Management are summarised below. These cover three key themes: 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; and, Recovery – How effective are SEPAs arrangements in recovering from the incident. In particular ensuring critical services are operational in a timely manner.

Readiness

Prior to the attack SEPA had been proactive in looking to mitigate the risk of cyber attacks as demonstrated through achieving cyber essentials plus, investment in IS security infrastructure and that cyber security was a recognised risk from the Board level down. Specifically Police Scotland concluded that SEPA "was not and is not a poorly protected organisation". SEPA had attained Cyber essentials Plus accreditation and had invested in its cyber and information security platforms.

Due to the sophistication of the attack the investigations, including forensic investigatory work, has not identified the exact route source of where the cyber attack breached SEPA's systems. However, there is indication that this was through a phishing attack which allowed access to SEPA's systems.

The reviews identified opportunities for enhancing staff awareness and training over of cyber risks. Management are taking forward action plans to further roll out training and awareness across the organisation. Similarly, SEPA have revised its security arrangements to limit the number of personal devices connected to the network to help manage risk.

SEPA had invested in an Intrusion Detection System (IDS). However, the reviews found that whilst the IDS was in operation, there were limitations around continuous system monitoring. The sophistication of the attack meant that although threat detection measures were in place and detected activity prior to 24 December, the magnitude of the attack was not understood until the attack was launched on the 24th by which time only containment measures could be taken. SEPA recognise that considerable investment would be required to ensure 24/7 monitoring of security alerts, usually through a Security Operations Centre (SOC). This is estimated between £2 - £4 million per year which given the size of SEPA would potentially represent a disproportionate level of investment. However, SEPA are working with the Scottish Government to see if, given the sensitive data held across the wider public sector, could some joint working arrangement be established.

Back-up and data management

Backups were taken in line with best practice in that there were three copies of the data, located at two separate locations, with one copy stored offline. In addition to live data, a backup was held on local servers, with an additional backup stored on remote server space off site. The sophistication of the attack meant the back-ups themselves were corrupted and therefore no way of accessing historical records. Following the attack, SEPA are looking to bring forward its digital transformation strategy, including moving to cloud-based storage and back-ups. This should enhance the organisations IS resilience and recovery arrangements.

Response

SEPA staff received system alerts on the morning of the 24th of December, just after midnight. Following the alerts, SEPA staff attended the office to further investigate and performed a controlled containment of the systems. As the event took place out of hours further escalation wasn't successfully undertaken until early morning (around 8am). Alongside systems alerts, operational staff from the contact centre and flood service escalated instances where systems were becoming inaccessible overnight but a connection to the cyber-attack was not made at this time. The investigations concluded that these issues did not impact the timeliness of the containment. It is recognised that the response taken reflects the level of resources available to SEPA. Management are working with staff to raise awareness of escalation procedures and ensuring there is a clear communications across the organisation of incidents.

Leadership and tone from the top

By 9.30 am on 24 December an Emergency Management Team (EMT) meeting had convened using SEPA's audio and web conferencing system. This was held separately from core systems as part of SEPAs resilience planning. The Agency Management Team was suspended and the EMT co-ordinated the response to the emergency. SEPA engaged with partners including Police Scotland and the Scottish Government to support throughout the recovery process. SEPA also notified the Information Commissioners Officer (ICO) of the incident and have had regular engagement throughout the recovery process. The EMT immediately focused on ensuring those critical services, 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 even from the day of the attack.

Emergency communications and response

SEPA used their Business Continuity Messaging Service (BCMS), a communication tool which was separate to the SEPA network, to communicate to staff throughout the incident to keep them aware of events and instructions to follow in the weeks following the attack.

SEPA had a range of business continuity plans and incident response playbooks. However, these were primarily stored electronically or hard copies in the office where there was limited staff present due to Covid-19 restrictions. Therefore, Management had to primarily rely on expert knowledge and experience of these process and systems to follow to co-ordinate the initial response.

Recovery

Following the attack SEPA focused on recovery of key systems and processes. Although they did not have access to their emergency management and incident management plans, staff clearly understood their critical processes as those critical to delivery of SEPA's statutory purpose. The continuity of these processes was prioritised. For example, SEPA prioritised and were able to issue, flood warnings on 24 December 2020 even though systems had been impacted by the attack. SEPA have continued to work with third parties to ensure these services continue to function effectively while SEPAs on recovery process is ongoing. SEPA worked with the Scottish Government and other strategic partners to develop some core functions including the payment of staff throughout the recovery process.

EMT and clear priorities

The EMT identified 103 projects to deliver between March and June. These included the development of basic core functions such as finance systems and processes as well as the investigatory and data recovery activity. There has been continued oversight from the EMT and Board throughout the process and clear communication strategy with staff and Management.

Communications

SEPA have sought to be as transparent as possible throughout the process provide regular clear communications through the website (including system status updates) and through media releases. Internally the BCMS tool continue to update staff alongside the roll out of new laptops and establishment of new systems access / email access for staff.

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.

Continued security

The independent reviews concluded 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. This includes new governance frameworks in place over any new project to ensure that the implementation 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. As part of the wider Digital Strategy in implementing new arrangements, SEPA are looking to reduce the reliance of in-house or bespoke systems to ensure there is greater ongoing technological support through third party (off the shelf) applications.

Going forward

SEPA has taken the decision to build from new rather than re-establish legacy systems. Any systems or data that needs to be recovered will be subject to extensive analysis and testing to ensure there is no risk of residual threat that the data could be compromised through the attack.

During 2021/22 SEPA will continue to progress with recovery and delivery. As systems and processes are established, this will continue to support the level of services being delivered by SEPA. SEPA initially prioritised health and safety and business critical services but has since established arrangements to support other statutory services such as licences and fees and charges as well as enforcement activity. In some instances these are through operational work arounds as underlying systems and infrastructure is developed. Members of the AMT are leads for individual recovery and delivery projects as the organisation looks to step forward into the new norm.

Conclusions

The investigations into the cyber attack have identified that SEPA has taken a proactive approach to Cyber Security.

The investigations identified areas of good practice in terms of SEPA's readiness and response to the cyber attack. These have included: the timeliness of response; the leadership and tone from the top in the initial response and subsequent recovery; the business continuity arrangements, including working with key partners to keep critical systems such as flood warning system operational; and, clear communication to staff and wider public, as SEPA have sought to be open and transparent.

The reviews concluded that SEPA's cyber maturity assessment was high with the implementation and adherence to recognised frameworks and implementation of best practice including back up policy following industry principles. However, the reviews did identify that greater maturity could be achieved through increased offline storage capacity and speed. Management recognise no system is going to fully mitigate the risk of cyber attack. Going forward, SEPA in consultation with the Scottish Government are exploring the level of IS security arrangements as to what is appropriate and proportionate to an organisation such as SEPA.

Management, as well as the independent reviews, have identified opportunities for improvement. In particular, the development of new systems and processes to enhance security arrangements, including cloud based back ups, to help reduce the risk of catastrophic loss of data. In addition, more advanced management of security alerts raised to ensure those of high risk receive appropriate focus. There are opportunities for developing staff awareness and training around cyber security threats as well as understanding of business continuity and disaster recovery plans.

Management have developed a detailed response to the cyber attack actions and these have been progressed and monitored across the AMT and Board.

Appendices

1. Disclaimer of opinion

Independent auditor's report to the members of the Scottish Environment Protection Agency, the Auditor General for Scotland, and the Scottish Parliament

Reporting on the audit of the financial statements

Disclaimer of opinion on financial statements

We were appointed by the Auditor General for Scotland to audit the financial statements in the annual report and accounts of the Scottish Environment Protection Agency for the year ended 31 March 2021 under the Public Finance and Accountability (Scotland) Act 2000. The financial statements comprise the Statement of Comprehensive Net Expenditure, Statement of Financial Position, Statement of Cash Flows, Statement of Changes in Taxpayers' Equity and notes to the financial statements, including a summary of significant accounting policies. The financial reporting framework that has been applied in their preparation is applicable law and International Financial Reporting Standards (IFRSs) as adopted by the European Union, and as interpreted and adapted by the 2020/21 Government Financial Reporting Manual (the 2020/21 FReM).

We do not express an opinion on the accompanying financial statements. Because of the significance of the matters described in the *Basis for disclaimer of opinion* section of our report, we have not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on these financial statements.

Basis for disclaimer of opinion

The cyber-attack suffered by the Scottish Environment Protection Agency on 24 December 2020, as described in the Performance Report, resulted in the loss of the body's financial records. Consequently, these financial statements have predominantly been created using cash records. However, there are limitations in this approach, including lack of supporting documentation for some transactions and balances included in the financial statements. For Income from Contracts (£42.092 million) we were unable to obtain sufficient audit evidence over the underlying substance of the transactions, whether the income belonged to the Scottish Environment Protection Agency and whether the income was accounted for appropriately. The Agency also used an aged debtors listing that existed prior to the attack to help reconstruct income and debtors as at November 2020. However, £2,197 million of these amounts were not paid and were written off as bad debts within other Operating Charges. We have been unable to gain sufficient audit evidence over the amount written off. The Agency has also recognised deferred income as part of the Accruals and Deferred Income balance (£9.648 million) included within Trade and Other Payables (£11.210million). We have been unable to obtain sufficient audit evidence over the completeness and accuracy of the deferred income balance.

As a result of these matters, we were unable to determine whether any adjustments might have been found necessary in respect of income balances and bad debts written off recorded in the Statement of Comprehensive Net Expenditure and deferred income balances recorded in the Statement of Financial Position. This also impacts on the related entries in the Cash Flow Statement and Statement of Changes in Tax Payers' Equity. Income from Contracts represents substantially all of Total Operating Income recognised in the Statement of Comprehensive Net Expenditure, therefore we have concluded that the possible effects on the financial statements of undetected misstatements could be both material and pervasive.

Conclusions relating to going concern basis of accounting

We have concluded that the use of the going concern basis of accounting in the preparation of the financial statements is appropriate.

Based on the work we have performed, we have not identified any material uncertainties relating to events or conditions that, individually or collectively, may cast significant doubt on the body's ability to continue to adopt the going concern basis of accounting for a period of at least twelve months from when the financial statements are authorised for issue.

Risk of material misstatement

We report in a separate Annual Audit Report, available from the Audit Scotland website, the most significant assessed risks of material misstatement that we identified and our judgements thereon.

Responsibilities of the Accountable Officer for the financial statements

As explained more fully in the Statement of Accountable Officer's Responsibilities, the Accountable Officer is responsible for the preparation of financial statements that give a true and fair view in accordance with the financial reporting framework, and for such internal control as the Accountable Officer determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Accountable Officer is responsible for assessing the body's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless deemed inappropriate.

Auditor's responsibilities for the audit of the financial statements

Our responsibility is to conduct an audit of the financial statements in accordance with applicable law and International Standards on Auditing (UK) (ISAs (UK)) as required by the Code of Audit Practice approved by the Auditor General for Scotland, and to issue an auditor's report. However, because of the matters described in the *Basis for disclaimer of opinion* section of our report, we were not able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on the financial statements.

We were appointed by the Auditor General on 31 May 2016. The period of total uninterrupted appointment is five years. We are independent of the body in accordance with the ethical requirements that are relevant to our audit of the financial statements in the UK including the Financial Reporting Council's Ethical Standard, and we have fulfilled our other ethical responsibilities in accordance with these requirements. Non-audit services prohibited by the Ethical Standard were not provided to the body.

Reporting on regularity of expenditure and income

Disclaimer of opinion on regularity

Because of the matters described in the *Basis for disclaimer of opinion* section of our report, we do not express an opinion on whether in all material respects the expenditure and income in the financial statements were incurred or applied in accordance with any applicable enactments and guidance issued by the Scottish Ministers.

Responsibilities for regularity

The Accountable Officer is responsible for ensuring the regularity of expenditure and income. In addition to our responsibilities to detect material misstatements in the financial statements in respect of irregularities, we are responsible for expressing an opinion on the regularity of expenditure and income in accordance with the Public Finance and Accountability (Scotland) Act 2000.

Reporting on other requirements

Opinion prescribed by the Auditor General for Scotland on audited part of the Remuneration and Staff Report

We have audited the parts of the Remuneration and Staff Report described as audited. In our opinion, the audited part of the Remuneration and Staff Report has been properly prepared in accordance with section 45(2) of the Environment Act 1995 and directions made thereunder by the Scottish Ministers.

Statutory other information

The Accountable Officer is responsible for the statutory other information in the annual report and accounts. The statutory other information comprises the Performance Report and the Accountability Report excluding the audited part of the Remuneration and Staff Report.

Our responsibility is to read all the statutory other information and, in doing so, consider whether the statutory other information is materially inconsistent with the financial statements, or our knowledge obtained in the audit or otherwise appears to be materially misstated. If we identify such material inconsistencies or apparent material misstatements, we are required to determine whether this gives rise to a material misstatement in the financial statements themselves. If, based on the work we have performed, we conclude that there is a material misstatement of this statutory other information, we are required to report that fact. As described in the *Basis for disclaimer of opinion* section of our report, we were unable to determine whether any adjustments might have been found necessary in respect of Income from Contracts or associated deferred income balances within Trade and Other Payables and issued a disclaimer of opinion on the financial statements. Accordingly, we have concluded that where the other information refers to amounts in the financial statements it may be materially misstated.

Opinions prescribed by the Auditor General for Scotland on Performance Report and Governance Statement

Because of the matters described in the *Basis for disclaimer of opinion* section of our report, we do not express an opinion on whether:

- the information given in the Performance Report for the financial year for which the financial statements are prepared is consistent with the financial statements and that report has been prepared in accordance with section 45(2) of the Environment Act 1995 and directions made thereunder by the Scottish Ministers; and
- the information given in the Governance Statement for the financial year for which the financial statements are prepared is consistent with the financial statements and that report has been prepared in accordance with section 45(2) of the Environment Act 1995 and directions made thereunder by the Scottish Ministers.

Matters on which we are required to report by exception

We are required by the Auditor General for Scotland to report to you if, in our opinion:

- adequate accounting records have not been kept; or
- the financial statements and the audited part of the Remuneration and Staff Report are not in agreement with the accounting records; or
- we have not received all the information and explanations we require for our audit.

As set out in the *Basis for disclaimer* of opinion section of this report, we have determined that adequate accounting records have not been kept and we have not received all information and explanations required for our audit.

Conclusions on wider scope responsibilities

In addition to our responsibilities for the annual report and accounts, our conclusions on the wider scope responsibilities specified in the Code of Audit Practice are set out in our Annual Audit Report.

Use of our report

This report is made solely to the parties to whom it is addressed in accordance with the Public Finance and Accountability (Scotland) Act 2000 and for no other purpose. In accordance with paragraph 120 of the Code of Audit Practice, we do not undertake to have responsibilities to members or officers, in their individual capacities, or to third parties.

2. Audit Adjustments

We are required to report all non trivial misstatements to those charged with governance, whether or not the accounts have been adjusted by management. There was one corrected misstatement to the financial statements identified during our audit. This related to the statement of cash flows that also required the restatement of the prior year disclosure. We identified one uncorrected misstatements to the financial statements in respect of the estimated accrual for job evaluation.

Impact of adjustment – cash flow statement current and prior year

There was one adjusted misstatement greater than £81,000 during the 2020/21 audit which is set out below.

Detail	Cash Flow Statement 2020/21 £'000	Cash Flow Statement 2019/20 £'000
Being presentational adjustment to the Cash Flow Statement in the current year to only reflect the adjustment for non-cash related movements through the Comprehensive Net Expenditure Statement (including removal of provisions and capital payables and receivables). As material to the prior period, the movement in decommissioning provisions was incorrectly included in the cash flow statements in the prior year (non-cash movement). The prior period comparative information has been updated to appropriately reflect this adjustment.		
Cr Net cash outflow from operating activities	(1,136)	(2,448)
Dr Net cash outflow from investment	1,136	2,448
Overall impact	-	-

Impact of adjustments in preparing the draft financial statements

In finalising the financial statements Management made a number of adjustments to the first draft financial statements presented to audit. These were primarily presentational adjustments and the recognition of IAS 19 actuarial valuation on receipt of Hymans Robertson's valuation report as at 31 March 2021. The adjustments below summarise those above £81,000.

Detail	Comprehensive Net Expenditure £'000	Statement of Financial Position £' 000
Being adjustments to recognise IAS 19 valuation (received from Hymans Robertson) including late pension adjustment		
Dr Superannuation contributions	6,651	
Cr IAS 19 Pension provision		(72,848)
Dr Actuarial loss on pension	63,436	
Dr staff costs	2,761	
Being reclassification of WEF to Scottish Landfill Tax		
Cr Income from Contracts	(152)	
Dr Other income	152	
Being adjustment to recognise income and expenditure based on final year end transactions		
Cr Staff costs	(37)	
Dr Other operating charges	47	
Cr Income	(249)	
Dr Other Income	9	
Dr Cash & cash equivalents		236
Cr Trade and other payables		(6)

Detail	Comprehensive Net Expenditure £'000	Statement of Financial Position £'000
Being adjustments to correct revaluation in year		
Cr Depreciation	(20)	
Dr Property, plant and equipment – Leased property		191
Cr Property, plant and equipment – Revaluation		(191)
Dr Accumulated depreciation		20
Being adjustment to correct accounting records based on year end reconciliation of staff costs and operating costs and VAT		
Cr Other operating charges	(354)	
Dr Trade and other payables		396
Cr Staff costs	(129)	
Dr Other operating charges	30	
Dr Other income	57	
Being a reclassification of EU grant deferred income to accruals and deferred income		
Dr EU Grant deferred income		253
Cr Accruals and deferred income		(253)
Overall impact	72,202	(72,202)

There were a number of reallocation adjustments between account codes but these do not impact on the primary financial statements, so have not been replicated within this appendix.

Unadjusted misstatements

We identified one audit misstatement during our audit in relation to overstatement of Job evaluation accruals. Management have not adjusted for the misstatement on the basis of it not being material to the financial statements.

Detail	Comprehensive Net Expenditure £'000	Statement of Financial Position £' 000
Being overstatement of job evaluation accrual due to computational errors in the calculations used.		
Dr Payables – Job evaluation accruals		148
Cr staff costs	(148)	
Overall impact	(148)	148

Misclassification and disclosure changes

The table below provides details of misclassification and disclosure changes identified during the audit which have been made in the final set of financial statements.

Disclosure	Auditor recommendations	Adjusted?
Critical judgements	International Financial Reporting standards prescribe the required disclosures in relation to critical judgements. It also requires separate consideration of accounting estimates. Significant Estimates relate to assumptions and estimates at 31 March that have a significant risk of resulting in a material adjustment to the carrying amounts of assets and liabilities within the next financial year. Judgements relates to areas of material judgement in the application of accounting policy that aren't significant estimates. In the draft accounts, Management have combined critical estimates and judgements. It is unclear from the disclosure what critical judgements have been applied. For significant estimates, it is unclear where Management consider the key assumptions where there is an increase risk of a material change in the estimate over the next 12 months. There is an opportunity to enhance the disclosure to focus on those key areas of estimation that may have a significant risk of material misstatement in the next 12 months. This should focus on those key areas of assumptions such as pension fund discount rate or key assumptions in the valuation.	No - Audit are satisfied that this is not material disclosure misstatement to the financial statements.
Accounting policies	The draft financial statements accounting policies, including basis of preparation and accounting framework adopted were based on FRS 101 and Companies Act. The FReM adapts and interprets International Financial Reporting Standards and there SEPA were required to update accounting policies to reflect those as outlined in the FReM. In particular, the basis of preparation and valuation of property, plant and equipment.	Yes

Disclosure	Auditor recommendations	Adjusted?
Staff costs	An unquantified misstatement between staff costs and other operating costs in relation to amounts paid (via payroll) to staff for the reimbursement of expenses. This has been estimated by Management at £300,000 and would be a disclosure adjustment between other operating costs and payroll costs.	No – we are satisfied that the impact would not be material to the financial statements.
Accounting disclosures	As a result of the cyber attack Management have been unable to complete a number of disclosures in the financial statements including: segmental reporting disclosures in accordance with IFRS 8; financial instrument disclosures and trading accounts. We have concluded that this omission does not lead to a material disclosure misstatements in the accounts as it would not materially influence the users of the accounts.	No – Management are unable to produce segmental reporting information and other disclosures. However, we are satisfied these are not material disclosure misstatements.

3. Action plan and recommendations

We have set out below, based on our audit work undertaken in 2020/21, the significant recommendations arising from our audit work:

Recommendation	Agreed Management response
1. Cash draw downs Through error, during 2020/21 an additional £2.014 million of cash was drawn down in the year. This is reflected in SEPA's cash and cash equivalent's balance and the Scottish Government have agreed that the cash draw down for 2021/22 cash funding will be reduced. While we recognise that the cyber attack meant operational arrangements were not in place, it is important that Management ensure there is sufficient oversight of draw downs to mitigate the risk of excess funding in future years and the risk of potentially overspending cash balances available.	We agree with this recommendation, and the recognition of the impact of the cyber attack had on operational arrangements. As soon as we identified the error we contacted the SG and agreed how this would be handled. In normal operating environment we had sufficient controls in place to mitigate the risk as outlined in the recommendation, and these have been reinstated. Responsible Manager: Chief Officer Finance. Implementation Date: April 2021
2. Financial strategy Following the cyber attack, it is important that SEPA revisit the financial strategy to reflect the financial impact the cyber attack has had on the organisation as well the impact on expediating the implementation of the Digital strategy to ensure there is a clear strategic approach to addressing the financial challenges facing the organisation. This includes understanding the potential savings achieved through the strategic investment in technology and service redesign.	We agree with this recommendation. We submitted a response on the 10th September to the SG Commission on the Comprehensive Spending Review for the period 2022 to 2027. In this paper we articulated our planning assumptions and strategic priorities, the propose spending plans for CSR period and outlined some high level savings plans. The board noted the income and expenditure position and the level of capital investment required for future years. This work will inform our financial strategy which will be refreshed as we work through the detail our 2022/23 budget preparation. Responsible Manager: Chief Officer Finance. Implementation Date: March 2022

4. Response to the cyber attack

The timeline below summarises the key line of events taking place from the cyber attack and Management's response to the attack

Date	Key event
Pre 24 December 2020	• Estimated date where the cyber attack initially penetrated SEPA's system. Investigations have yet to determine the original source of the attack. However, expert opinion the report is most likely through a form of phishing email.
Pre 24 December 2020	• The attackers infiltrated SEPAs infrastructure and leaving complex and sophisticated devices to encrypt / destroy data. This went undetected.
Evening of the 23 December 2021	• The cyber attack started with all of SEPA's data and information being encrypted, stolen or deleted. • SEPA's back up policy was in line with best practice. However, the sophisticated nature of the attack meant that online backups were targeted and impacted in the early stages of the attack. • A SEPA staff member was alerted at home by automatic alarms just after midnight on 24 December, they immediately logged onto the systems and investigated. They then attended the office and in a phased manner began isolating and shutting down systems. • Operational staff, including Flood warning team, escalate issues around accessibility of key systems.
8am – 24 December	• As the event took place out of hours, further escalation wasn't completed until the early morning of the 24th. • The Head of Governance is notified of the issues and contacts IS team member who confirm the attack. The issue is immediately escalated to the Chief Executive.
9.30am – 24 December	• An Emergency Management Team meeting was established through the use of communications software held separately from SEPA's systems for business continuity purposes.

Date	Key event
9.30 am – 11.00am – 24 December	• Executive Management Team meeting where initial emergency response to the plan was developed • SEPA contacted the Scottish Government Cyber Resilience Unit (CRU) which instigated the national cyber incident response coordination arrangements providing structure and support at that early stage. • 11:00hrs - SEPA confirms serious and significant cyber-attack to staff, stakeholders and media. Critical services maintained and essential Flood Warnings issued. Data breach reported to the Information Commissioner's Office (ICO).
31 December	• Emergency SEPA Board meeting held to discuss the cyber attack and planned response.
14 – 31 January 2021	• SEPA confirms ongoing ransomware attack likely to be by international serious and organised cyber-crime groups intent on disrupting public services and extorting public funds. 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). • 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 • 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 effected
28 January 2021	• SEPA develops its overarching approach to the delivery of services for the first half of 2021. • Weekly service status updates published on line.
February – June 2021	• SEPA implement recovery programme covering 103 projects focusing on establishing business critical systems and processes. The projects are overseen by the EMT and Board to monitor progress or key challenges in delivery. The projects include the recreating accounting records to support the 2021 financial statements as well as financial controls and process for 2021/22.
27 October 2021	• SEPA publishes its lessons learned reports and hosts a webinar – cyber crime: ready, resilient and responsive.
Ongoing	• SEPA moving into next phase of recovery and delivery focusing on the new build of systems and infrastructure rather than rebuild of legacy systems.

5. Follow up of 2019/20 recommendations

We have set out below our follow up of recommendations raised in the prior year:

Recommendation

1. Professional valuations (Property, pant and equipment)

Original recommendation

In our correspondence with the professional valuers of the Sir John Murray, Century Marine Services Limited, they noted that while the valuation of the vessel at March 2020 reflected the impact of Covid-19 it did not consider the prolonged period which Covid-19 would impact the economy. As a result, there may be a fall in the value of the vessel in financial year 2020/21. We recommend SEPA liaises with its valuer in order to ensure the depreciation charge for the vessel is appropriate for 2020/21.

Initial Management Response:

We will liaise with the valuer as recommended and make appropriate accounting adjustments in the accounts for the year to 31 March 2021.

2020/21 update: Recommendation closed – Management engaged a professional valuation of the vessel as a 31 March 2021 and this is reflected in the financial statements.

2. Performance Management (raised in 2018/19)

The annual report and accounts provides a summary of the progress made against these actions as well as work out standing to address these. The performance targets align to operational plan targets and subsequently supporting the assessment of progress towards strategic outcomes. However, these could be more focused on SEPAs outcomes and deliverables as there are a number of the measures focused on inputs. In addition, for targets such as 'Make the waste sector less attractive to criminals" these are very subjective and difficult to quantify the performance outcomes from SEPA's activities. SEPA continue to refine performance information to enable ongoing scrutiny of operational performance against corporate priorities.

Initial Management Response:

Performance targets continue to be refined and aligned to priorities.

2020/21 updated: Superseded – The Performance Information included in the accounts provides an overview of SEPAs performance in delivering key strategic objectives and those covered in the Annual operating Plan. As a result of the cyber attack the level of information and data to produce the report has been limited. However, Management have produced a balance report that provides the reader of the accounts an understanding of SEPAs performance in the year. As services are re-established and systems built this will continue to support the level of performance information available to Management and to include in the annual report.

6. Audit fees and independence

External Audit Fee

Service	Fees £
External Auditor Remuneration	72,590
Pooled Costs	9,810
Contribution to Audit Scotland costs	2,170
Contribution to Performance Audit and Best Value	-
2020/21 Fee	84,570

Fees for other services

Service	Fees £
We confirm that for 2020/21 we did not receive any fees for non-audit services	Nil

Client service

We take our client service seriously and continuously seek your feedback on our external audit service. Should you feel our service falls short of expected standards please contact Joanne Brown, Head of Public Sector Assurance Scotland in the first instance who oversees our portfolio of Audit Scotland work (joanne.e.brown@uk.gt.com). Alternatively, should you wish to raise your concerns further please contact Jon Roberts, Partner and Head of Assurance, 30 Finsbury Square, London, EC2A 1AG. If your feedback relates to audit quality and we have not successfully resolved your concerns, your concerns should be reported to Elaine Boyd, Assistant Director, Audit Scotland Quality and Appointments in accordance with the Audit Scotland audit quality complaints process.

Transparency

Grant Thornton publishes an annual Transparency Report, which sets out details of the action we have taken over the past year to improve audit quality as well as the results of internal and external quality inspections. For more details see Transparency report 2020 (grantthornton.co.uk)

Independence and ethics

- We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention.
- We have complied with the Financial Reporting Council's Ethical Standards and therefore we confirm that we are independent and are able to express an objective opinion on the financial statements.
- We are required by auditing and ethical standards to communicate any relationships that may affect the independence and objectivity of the audit team.
- We can confirm no independence concerns have been identified.
- We confirm that we have implemented policies and procedures to meet the requirements of the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements.

7. Communication of audit matters

International Standards on Auditing (UK) (ISA) 260, as well as other ISAs, prescribe matters which we are required to communicate with those charged with governance, and which we set out in the table below.

Our communication plan	Audit Plan	Annual Report
Respective responsibilities of auditor and management/those charged with governance	•	
Overview of the planned scope and timing of the audit, including planning assessment of audit risks and wider scope risks	•	
Confirmation of independence and objectivity	•	•
A statement that we have complied with relevant ethical requirements regarding independence. Relationships and other matters which might be thought to bear on independence. Details of non-audit work performed by Grant Thornton UK LLP and network firms, together with fees charged. Details of safeguards applied to threats to independence	•	•
Significant matters in relation to going concern	•	•
Views about the qualitative aspects of the SEPA's accounting and financial reporting practices, including accounting policies, accounting estimates and financial statement disclosures		•
Significant findings from the audit		•
Significant matters and issues arising during the audit and written representations that have been sought		•
Significant difficulties encountered during the audit		•
Significant deficiencies in internal control identified during the audit		•
Significant matters arising in connection with related parties		•
Identification or suspicion of fraud involving management and/or which results in material misstatement of the financial statements		•
Non-compliance with laws and regulations		•
Unadjusted misstatements and material disclosure omissions		•
Expected modifications to the auditor's report, or emphasis of matter		•

grantthornton.co.uk