Performance & Audit Committee
Friday 6th March 2020
Item 10. Cyber Resilience Update

Cyber Resilience

1. INTRODUCTION

1.1 This purpose of this report is to provide the Committee with an update on the ongoing Cyber Resilience programme of work being undertaken by SEStran.

2. BACKGROUND

2.1 Reports were brought to previous meetings of the Performance & Audit Committee and Partnership Board detailing the requirements of the Scottish Government (SG) Cyber Security Public Sector Action Plan.

2.2 One of the key actions placed on public sector bodies was to achieve Cyber Essentials certification.

2.3 Following pre-assessment in March 2018, Cyber Essentials was awarded to the partnership in January 2019. This was followed by an independent audit of SEStran's IT systems and the higher level accreditation of Cyber Essentials PLUS was gained February 2019.

3. CYBER SECURITY

3.1 Cyber Essentials

3.1.1 It is recommended that assessment for Cyber Essentials is carried out on an annual basis and re-assessment, followed by an independent audit of the full network was conducted in February 2020, resulting in SEStran retaining its Cyber Essential PLUS status for a further year.

3.2 Scottish Public Sector Supplier Cyber Security - Guidance Note

3.2.1 In January 2020 the Scottish Government issued the Scottish Public Sector Supplier Cyber Security - Guidance Note. The key aims of the guidance is:

- To support Scottish public sector organisations to put in place consistent, proportionate, risk-based policies that effectively reduce the risk of Scottish public services being damaged or disrupted by cyber threats as a result of supplier cyber security issues; and

- to minimise any necessary additional burdens on Scottish public sector organisations (as purchasers) and private and third sector organisations (as suppliers), whilst ensuring the presence of proportionate cyber security controls in the public sector supply chain. This includes a requirement to avoid discouraging SMEs, in particular, from bidding for public sector contracts.

3.2.2 The guidance provides organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence, through the continued adoption of good practice.

3.2.3 Furthermore, Scottish public sector organisations are encouraged to take a proportionate approach to the application of security controls in line with the guidance note. Where a cyber risk has been identified, any decisions about minimum cyber security requirements should be risk-based and proportionate to an organisation’s risk appetite. This is to avoid an overly prescriptive approach to cyber security.

3.2.4 Whilst SEStran holds limited data, Officers will carry out a review of the partnership’s supplier chain cyber security and implement the principles, where appropriate, in line with the guidance and supporting toolkits, using a proportionate and risk-based approach.

3.2.5 Once this exercise is concluded, any significant actions identified will be included in the partnership’s risk register, which is regularly presented to the Performance and Audit Committee.

4. RECOMMENDATIONS

4.1 The Committee are asked to note the contents of this report.

Angela Chambers
Business Manager
March 2020

Policy Implications	As outlined in the report
Financial Implications	Cost of reassessment at £1500
Equalities Implications	None
Climate Change Implications	None