Questions for Scottish public sector organisations on the draft public sector action plan and draft best practice guidelines on cyber resilience

Please provide comments on the draft action plan and the draft best practice guidelines on cyber resilience in line with the following questions.

Question 1: To provide important context, please give an overview of your current arrangements for cyber security. In particular, please provide details of:

- any relevant accreditations held, or standards met, by your organisation
- current board level, governance and risk management arrangements for managing the cyber threat in your organisation
- any ongoing programmes of work on cyber security in your organisation
- the current level of resource you devote to cyber security in your organisation.

Answer to Question 1

The OU is accredited to the UK Government’s Cyber Security Essentials PLUS scheme and has been for the last two years. This government-backed cyber security certification scheme sets out a robust baseline for cyber security controls.

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) was achieved by the University in October 2016.

The University aligns, where possible, to the ISO 27001 family of standards.

Information security requirements are part of our procurement policy and processes and the Information Security Team supports Units with their procurement activity. This includes third party assessment and risk assessment.

The University has a strong commitment towards, and governance structure in respect of, information security and cyber controls. This is best demonstrated by the investment that is given to information security:

- The University has a risk management policy and framework and an aligned information security risk management policy
- The University Secretary is accountable for information security but has delegated the responsibility to the Chief Information Officer (CIO)
- The Information Security Team, consisting of a Head of Information Security and four Information Security Specialists, report directly into the CIO
- The University’s Information Security Steering Group (ISGG) is the primary focus group for information/cyber security. Meeting quarterly, the group provides leadership for the protection of the University’s information assets and technology and oversees security objectives and strategies. The ISSG has representation from Units and faculties to ensure that all University communities are represented
- The Head of Information Security presents an annual report on cyber controls to the University’s Audit Committee. The assessment responds to ‘Five Strategic Questions’, which are set by the National Audit Office to aid Audit and Risk Assurance Committees’ consideration of how ‘cyber risk’ is managed by their organisation, and the UK Government’s ‘10 Steps to Cyber Security’, to which the National Cyber Security Centre recommends organisational adherence
- Regular compliance audits take place, led by both the Information Security Team and the University’s independent audit function
- The University also has a PCI DSS Steering Group to ensure appropriate card payment control measures are in operation and that PCI DSS compliance is achieved on an annual basis.

The Information Security Team’s key activities and deliverables include:
• Strategic input - for continuous progression of the information security strategy, vision and objectives

• Policy and process - continuous development and alignment of information security policy, standards and guidelines

• The recommendation of security initiatives in order to improve the maturity of information security

• Advice and guidance - provide a focal point within the University for information security consultancy and advice

• Awareness and education - increase and improve user awareness of information security across the University through awareness campaigns, guidance, education and training

• Risk management - identification of risks through assessment and the recommendation of risk controls and treatment plans to mitigate risks in accordance with the University's risk tolerance. This also includes supporting business partners in decision-making activities.

• Incident management - support the University's incident management framework

• Testing and audit quality assurance - ensure that University information assets and technology remain secure through regular test and audit activity.

• Ensuring that the design of services and solutions meet information security policy and standard

• Work closely with network and infrastructure teams and other technical teams to ensure appropriate technical controls are in situ.

Question 2: Please give your views on the draft public sector action plan and best practice guidelines. We would particularly welcome views on:

• Whether there are any key omissions from the plan
• Whether there is likely to be any unnecessary duplication as a result of the plan
• Whether you believe the plan, if implemented, would make a significant difference to levels of cyber resilience among Scotland’s public bodies.

Answer to Question 2

We believe the plan could yield a significant improvement to levels of cyber resilience among public sector organisations. However this would depend on measures taken to monitor adherence to the plan.

The other factor to consider is that some public sector organisations may not have a dedicated information security/cyber security resource. Implementation of the plan would encourage organisations to ensure they have a commitment to information/cyber security.

The OU, uniquely among UK universities, functions across all four nations of the UK and is a University in its own right in each. Should any of the other UK administrations choose to adopt a cyber resilience plan of their own, there would be a risk that for pan-UK bodies with responsibilities in different home nations such subsequent plans could conflict with, supersede or duplicate compliance requirements.
Question 3: Please identify any key implementation challenges for your organisation in respect of the draft public sector action plan and best practice guidelines.

**Answer to Question 3**

We do not envisage any significant implementation challenges within the University; however, we would be keen to better understand the implications for suppliers and therefore for procurement processes.

As noted in response to question 2, The OU operates across the UK. Should any of the other UK administrations choose to adopt a cyber resilience plan of their own, there would be a risk that for pan-UK bodies with responsibilities in different home nations such subsequent plans could conflict with, supersede or duplicate compliance requirements.

Question 4: If you are a public sector organisation that is not subject to the Scottish Public Finance Manual, please indicate whether you would be in favour of adopting the recommendations set out in the draft action plan and best practice guidelines to ensure alignment with other public sector organisations.

**Answer to Question 4**

Given the University's role as a service provider of online educational resources, cyber security controls are of paramount importance. Therefore we would tend to be in favour of adopting the recommendations which are set out in the draft action plan.

We believe both public and private sector organisations have an obligation to invest in information security to keep pace with the current threat landscape, and the introduction of public standards and guidelines may help organisations to avoid complacency.

Question 5: Please indicate whether you would be willing in principle for your organisation to become a public sector cyber catalyst, in line with the description set out in the draft action plan at Key Actions 6 and 7. (Please note: due to practical considerations, not all organisations volunteering are likely to be selected as cyber catalyst organisations)

**Answer to Question 5**

The University is open to further discussion on this front.