Cyber Security Update

Audit & Governance Committee
24th November 2021

Mike Ibbitson, Assistant Director, ICT

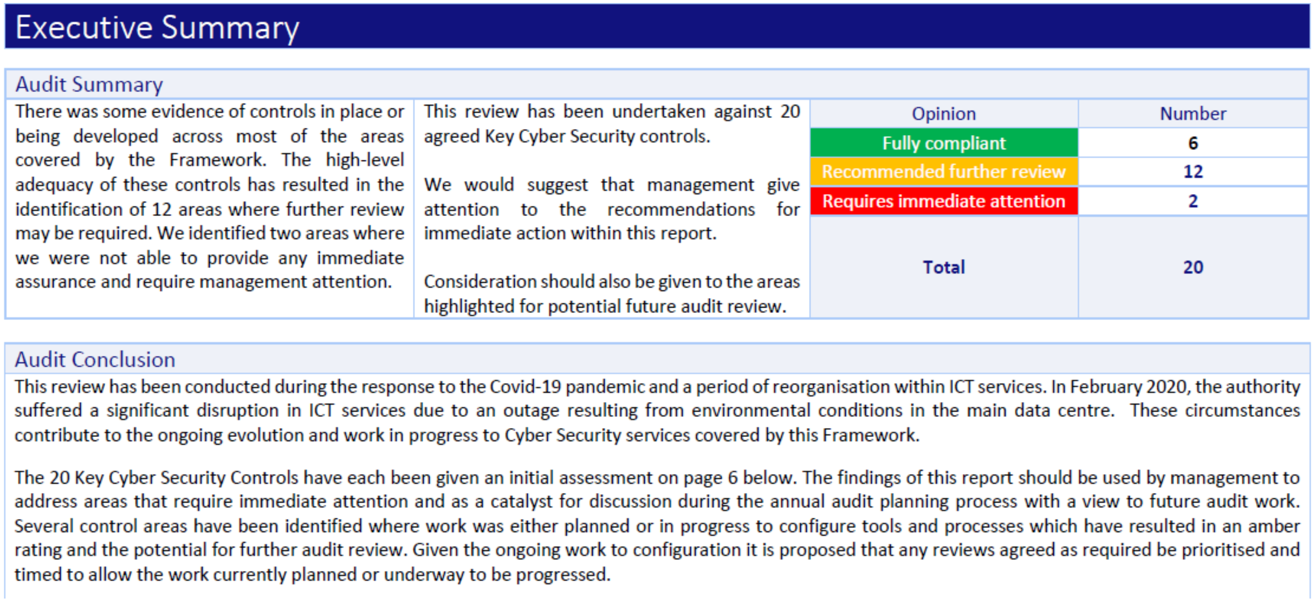
V0.6

This presentation

The Audit & Governance Committee last received an item on cyber security in April 2021 which primarily addressed the work that was underway following an internal (SWAP) audit in February 2021.

This presentation updates progress since the audit and also notes other areas of progress. Cyber Security remains an ever present threat and one which is still increasing and has directly impacted some local authorities.

SWAP Cyber Security audit; summary & findings



Executive Summary

Audit Summary

There was some evidence of controls in place or being developed across most of the areas covered by the Framework. The high-level adequacy of these controls has resulted in the identification of 12 areas where further review may be required. We identified two areas where we were not able to provide any immediate assurance and require management attention.

This review has been undertaken against 20 agreed Key Cyber Security controls.

We would suggest that management give attention to the recommendations for immediate action within this report.

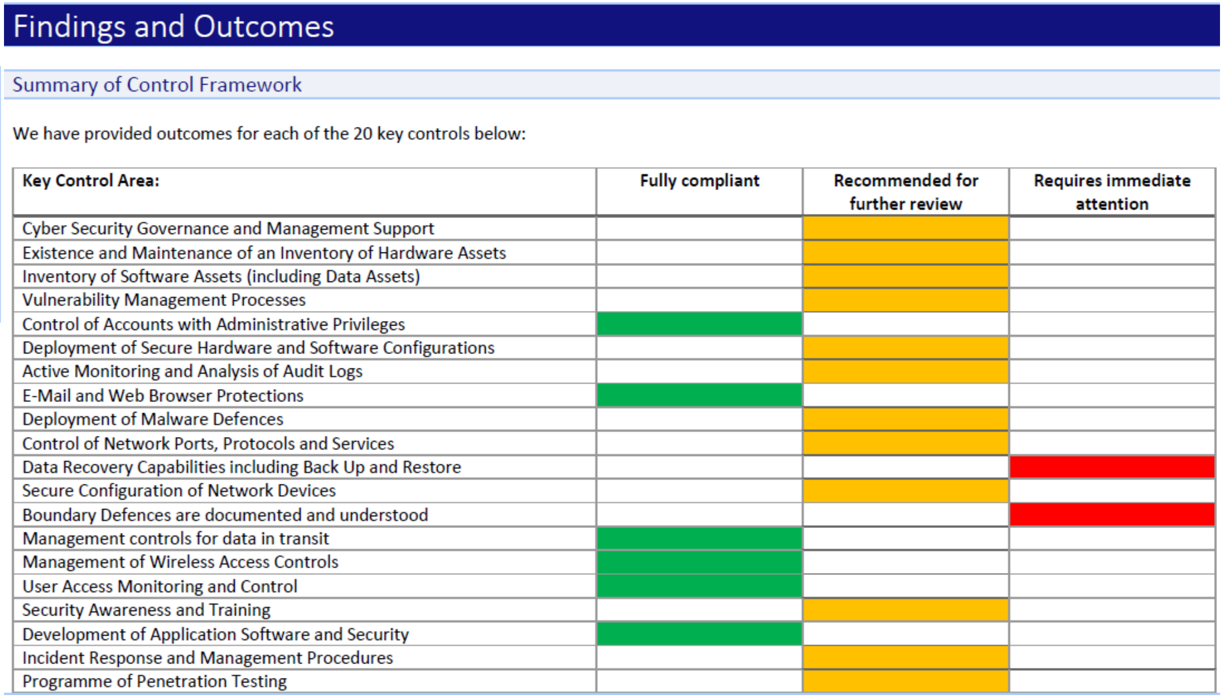
Consideration should also be given to the areas highlighted for potential future audit review.

Opinion	Number
Fully compliant	6
Recommended further review	12
Requires immediate attention	2
Total	20

Audit Conclusion

This review has been conducted during the response to the Covid-19 pandemic and a period of reorganisation within ICT services. In February 2020, the authority suffered a significant disruption in ICT services due to an outage resulting from environmental conditions in the main data centre. These circumstances contribute to the ongoing evolution and work in progress to Cyber Security services covered by this Framework.

The 20 Key Cyber Security Controls have each been given an initial assessment on page 6 below. The findings of this report should be used by management to address areas that require immediate attention and as a catalyst for discussion during the annual audit planning process with a view to future audit work. Several control areas have been identified where work was either planned or in progress to configure tools and processes which have resulted in an amber rating and the potential for further audit review. Given the ongoing work to configuration it is proposed that any reviews agreed as required be prioritised and timed to allow the work currently planned or underway to be progressed.



Findings and Outcomes

Summary of Control Framework

We have provided outcomes for each of the 20 key controls below:

Key Control Area:	Fully compliant	Recommended for further review	Requires immediate attention
Cyber Security Governance and Management Support		🟧	
Existence and Maintenance of an Inventory of Hardware Assets		🟧	
Inventory of Software Assets (including Data Assets)		🟧	
Vulnerability Management Processes		🟧	
Control of Accounts with Administrative Privileges	🟩		
Deployment of Secure Hardware and Software Configurations		🟧	
Active Monitoring and Analysis of Audit Logs		🟧	
E-Mail and Web Browser Protections	🟩		
Deployment of Malware Defences		🟧	
Control of Network Ports, Protocols and Services		🟧	
Data Recovery Capabilities including Back Up and Restore			🟥
Secure Configuration of Network Devices		🟧	
Boundary Defences are documented and understood			🟥
Management controls for data in transit	🟩		
Management of Wireless Access Controls	🟩		
User Access Monitoring and Control	🟩		
Security Awareness and Training		🟧	
Development of Application Software and Security	🟩		
Incident Response and Management Procedures		🟧	
Programme of Penetration Testing		🟧	

Update on Actions from Feb ‘21 audit: all complete

- There were 20 actions from the SWAP audit report - are no outstanding actions

- RED graded actions 1.11 & 1.13 are both complete
- AMBER graded actions 1.1, 1.2, 1.3, 1.6, 1.7, 1.9, 1.10, 1.12, 1.17, 1.19 and 1.20 are complete
- GREEN areas (no actions needed) were 1.4, 1.5, 1.8, 1.14, 1.15, 1.16, 1.18

Follow on items

- Several Amber review actions were agreed as part of the audit, these are complete and we have decided on additional work to improve security (and deliver other general management targets), these include:
  - Further steps to ensure rigorous hardware asset controls via the recently adopted IT Service Management software (improves security plus cost control)
  - Building a business case for acquisition of a software asset management tool (improves security, ease of management & cost control)
  - Further updates to our network replacing some equipment and implementing a tighter regime for updates/patching
  - On going operation of the new Information Management & Governance Board (led by the SIRO & Deputy SIRO)

General items of progress & relevant action details

- The ICT restructure was completed in Autumn ‘21 & increased dedicated security staff from 1 person to 3 – now comprising a Security Manager, Senior Security Officer and Technical Security Officer. This provides much more scrutiny on security matters including policy, approach, threat assessment and day to day monitoring as well as giving annual leave cover in case of incidents.
- One aspect of this is that we have now developed a operational Cyber Security Incident Management process with clear roles and actions in this event
- Work towards the ‘Cyber Essentials Plus’ certification is underway and we expect to achieve this in Q1 of 2022 (against a new, tighter standard for 2022)
- We secured £3000 of external training funds from the LGA and were able to train 2 staff to Certified Information Systems Security Professional (CISSP) standard via a remote learning course with Salford College
- A briefing session for the Pension Fund Committee to provide a situation report and general advice has been conducted (with another update scheduled for December ‘21)

Conclusion

- The cyber threat to the security of our systems has not diminished over the past year and may have grown
- However we are in a much better position now that all 20 audit actions are done and general improvements have been made. More work is scheduled.
- We will continue to:
    - Reduce vulnerability by technology means
    - Educate users to diminish the threat
    - Maintain vigilance, manage any incidents & learn from these