Top 20 Critical Security Controls - Assessment and Mapping to NCSC 10 Steps

CSC #	Ten Steps	Control Criteria	Technical Controls in place	Technical Gaps Identified	@Investment	Status
1	Secure Configuration Monitoring	**Inventory of Authorized and Unauthorized Devices** *Actively manage (inventory,track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.*	IBM Endpoint Manager (IEM) undertakes point in time audit of connected devices.	Implementation of Network Access Control (Part of JNRP) will provide identification of unauthorised devices and report into a SIEM for remediation.	@£80k for SIEM	Awaiting connection from CoL to CoLP networks.
2	Secure Configuration Monitoring	**Inventory of Authorized and Unauthorized Software** *Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*	IEM / SCCM should provide this functionality.	Application Whitelisting	Staff Resource	Dependent on outsourcer and monitoring of assets
3	Secure Configuration	**Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** *Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*	Controlled build is in place across all device types as well as an established change management process. Microsoft InTune MDM is being deployed.	Review ITIL implementation and SIEM.	Staff Resource	In place and operating under contract with outsourcer.
4	Monitoring	**Continuous Vulnerability Assessment and Remediation** *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.*	Contractual security support.	Purchase NESSUS vulnerability assessment product and deploy in enterprise mode and feed into SIEM for alerting and reactive remediation.	@£10k	Product in place and being utilised by Infosecurity Analyst
5	Removable Media Controls Malware Protection	**Malware Defenses** *Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.*	ESET Anti-virus and Anti-Malware in place across Servers and workstations; Different AV products at gateways. However, this has proved ineffective against recent cryptoware attacks.	Consider investing in dedicated anti-malware product - MalwareBytes, proven very effective against Ransomware attacks.	@£80-100k	Requirement to invest in mobile anti-virus solution.
6	Secure Configuration	**Application Software Security** *Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.*	Change management process in place, no technical controls. Resource in place to manage process.	Deployed software will be subject to application log inspection into SIEM.		SIEM: Awaiting connection from CoL to CoLP networks.
7	Monitoring Network Security	**Wireless Access Control** *The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.*	Not currently applicable as no corporate services provided by direct wireless connection	Addressed within the netwoirk refresh project and subject to monitoring by outsourcer.		NOC in place and operating.
8	Incident Management	**Data Recovery Capability** *The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.*	Operated under managed service.	DR/BCP testing and support needed.	Significant Staff Resource Required	Requires testing.
9	User Education & Awareness	**Security Skills Assessment and Appropriate Training to Fill Gaps** *For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.*	Limited scope for awareness, training and policy enforcement	Invest in a policy and awareness product, i.e. MetaCompliance.	@£30k	Product purchased and operating.
10	Secure Configuration Network Security	**Secure Configurations for Network Devices such as Firewalls, Routers, and Switches** *Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*	Revised approach to change management process in place aligned with ITIL. No specific technical controls.	Configuration change to be tracked by SIEM.	Staff Resource	SIEM: Awaiting connection from CoL to CoLP networks.
11	Network Security	**Limitation and Control of Network Ports, Protocols, and Services** *Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.*	None	Network Access Control will provide this functionality - this is part of the network refresh delivery.		Verification of NAC outstanding with outsourcer.
12	Monitoring	**Controlled Use of Administrative Privileges** *The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*	Procedurally managed no technical montoring in place.	No automatic monitoring or alerting in place when priviledge access is granted or revoked. SIEM should be implemented to provide technical oversight as well as policy enforcement tool to ensure adherence and understanding of required standards.	£100k	Product purchased, awaiting installation by IT.

13	Home & Mobile Working
	Monitoring
	Network Security
		Boundary Defense
		Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
			Basic firewall controls, no intelligent boundary defence mechanisms in place.	Deploy an Intrusion Detection System;
				Deploy an Intrustion Prevention System;
				Data fed into SIEM.
					@£50-100k	In place and operating under contract with outsourcer.

14	Monitoring	**Maintenance, Monitoring, and Analysis of Audit Logs** *Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.*	Limited and locally managed, no centralised Syslog.	Implementation of SIEM will address this issue.		SIEM: Awaiting connection from CoL to CoLP networks.
15	Managing User Privileges Network Security	**Controlled Access Based on the Need to Know** *The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.*	Limited segregation in place.	Following identification and classification of assets the deployment of VLANS. Classification of data is linked to reducing overal cost reduction.	Staff Resource	Network refresh has introduced additional security standards for VLANS across network.
16	Managing User Privileges	**Account Monitoring and Control** *Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.*	Currently managed by outsourcer	Process driven, supported by technology.	Staff Resource	In place and operating.

Top 20 Critical Security Controls - Assessment and Mapping to NCSC 10 Steps

CSC #	Ten Steps	Control Criteria	Technical Controls in place	Technical Gaps Identified	@Investment	Status

17	Removable Media Controls	**Data Protection**
		The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
			Limited capability managed by Firewall and gateway filters.	Deploy an Intrusion Detection System;
				Deploy an Intrustion Prevention System;
				Deply DLP controls including the review of Email and Internet gateway rules;
				Pixalert - content scanner.
					@50k	Move to o365 requires review of MS security centre control set and alignment with security controls.

18	Incident Management	**Incident Response and Management** *Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*	Recorded within SupportWorks by ServiceDesk no other technical controls in place; Reactive and fragmented processes in place; Currently under review by management.	Create a single incident reporting process across the organisation for all security incident types; Audit technical capability against CESG Cyber Incident Response Scheme.	Staff Resource	In place and operating.
19	Secure Configuration	**Secure Network Engineering** *Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.*	Network refresh project is addressing Security by Design including SAVE process.	Ongoing integration into procurement processes.	Staff Resource	Established processes in place and security gateways in place for procurement processes.
20	Incident Management Monitoring Secure Configuration	**Penetration Tests and Red Team Exercises** *Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.*	Penetration test takes place against PSN;	Widen scope of Penetration tests to include all risk areas;	@£50-100k	In place and operating.