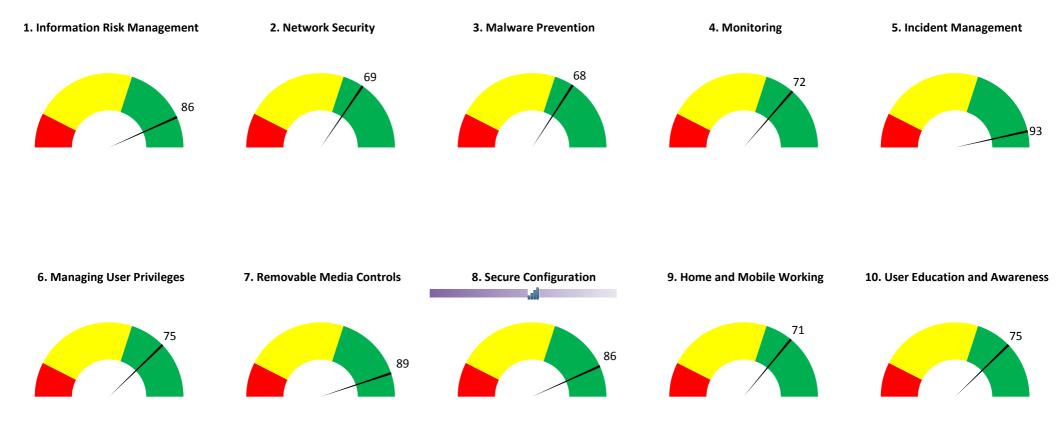


City of London Corporation

10 Steps Maturity Assessment

01 June 2019

10 Steps to Cyber Security: Dashboard



City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 01 June 2019

	% Complete	Target Score	Actual Score		% Complete	Target Score	Actual Score		% Complete	Target Score	Actual Score
Information Risk Management	86%	4	4	Network Security	69%	4	3	Malware Prevention	68%	4	3
Establish a governance framework	100%	4	4	Police the network perimeter	75%	4	3	Develop and implement anti-malware policies	75%	4	3
Determine the organisation's risk appetite	25%	4	2	Install firewalls	100%	4	4	Manage all data import and export	75%	4	3
Maintain the Board's engagement with information risk	100%	4	4	Prevent malicious content	75%	4	3	Blacklist malicious web sites	100%	4	4
Produce supporting policies	100%	4	4	Protect the internal network	80%	4	3	Provide detailed media scanning machines	25%	4	1
Adopt a lifecycle approach to information risk management	100%	4	4	Segregate network as sets	25%	4	1	Establish malware defences	75%	4	3
Apply recognised standards	100%	4	4	Secure wireless devices	100%	4	4	End user device protection	50%	4	2
Make use of endorsed assurance schemes	100%	4	4	Protect internal IP addresses	25%	4	1	User education and awareness	75%	4	3
Educate users and maintain their awareness	75%	4	3	Enable secure administration	25%	4	2		73/0	4	3
Promote a risk management culture		4	3	Configure the exception handling process		4	Δ				
riumue a iisk iiiaiiagamen culture	75%	4	3	Monitor the network	100%	4	-				
				Assurance process	50%	4	2				
				Assurance process	100%	4	4				
Monitoring	72%	4	3	Incident Management	93%	4	4	Managing User Privileges	75%	4	3
Establish a monitoring strategy and supporting policies	50%	4	2	Obtain senior management approval	100%	4	4	Establish effective account management processes	100%	4	4
Monitor all ICT systems	75%	4	3	Provide specialist training	100%	Δ	Δ	Establish policy and standards for user identification and access	75%	Δ	3
Monitor network traffic			-	Define the considered refer and consequently little		-		control		-	
	75%	4	3	Define the required roles and responsibilities	100%	4	4	Limit user privileges	75%	4	3
Monitor all user activity	75%	4	3	Establish a data recovery capability	100%	4	4	Limit the number and use of privileged accounts	75%	4	3
Fine-tune monitoring systems	50%	4	2	Test the incident management plan	100%	4	4	Monitor	75%	4	3
Establish a centralised collection and analysis capability	75%	4	3	Decide what information will be shared and with whom	75%	4	3	Limit access to the audit system and the system activity logs	50%	4	2
Provide resilient and synchronised timing	100%	4	4	Collect and analyse post-incident evidence	75%	Δ	3	Educate users and maintain their awareness	75%	4	3
Align the incident management policies	75%	4	3	Conduct a lessons learned review	100%	4	4		73/0	4	3
Conduct a lessons learned review		4	3	Educate users and maintain their awareness		4	· ·				
Conduct a lessons learned review	75%	4	3	Report criminal incidents to law enforcement	75% 100%	4	3 4				
					100%	4	4				
Removable Media Controls	89%	4	4	Secure Configuration	86%	4	3	Home and Mobile Working	71%	4	3
Removable Media Controls Produce corporate policies	89% 50%	4 4	4 2	Secure Configuration Use supported software	86% 80%	4 4	3	Home and Mobile Working Asses the risks and create a mobile working security policy	71% 75%	4 4	3
		•	•	Use supported software Develop and implement corporate policies to		•				•	
Produce corporate policies	50% 100%	4	•	Use supported software	80% 100%	4	3	Asses the risks and create a mobile working security policy Educate users and maintain their awareness	75% 75%	4	3
Produce corporate policies Limit the use of removable media Scan all media for malware	50%	4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories	80%	4	3	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline	75%	4	3
Produce corporate policies Limit the use of removable media	50% 100%	4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software	80% 100%	4	3	Asses the risks and create a mobile working security policy Educate users and maintain their awareness	75% 75%	4	3
Produce corporate policies Limit the use of removable media Scan all media for malware	50% 100% 100% 100%	4 4 4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories	80% 100% 80% 100%	4 4 4	3 4 3 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline	75% 75% 100% 100%	4	3 3 4
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media	50% 100% 100% 100% 100%	4 4 4 4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans	80% 100% 80% 100% 75%	4 4 4 4	3 4 3 4 3	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75%	4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media	50% 100% 100% 100%	4 4 4 4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management	80% 100% 80% 100%	4 4 4 4	3 4 3 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest	75% 75% 100% 100%	4 4 4 4	3 3 4 4
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media	50% 100% 100% 100% 100%	4 4 4 4	•	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and	80% 100% 80% 100% 75%	4 4 4 4	3 4 3 4 3	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75%	4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media	50% 100% 100% 100% 100%	4 4 4 4 4	2 4 4 4 4 4	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access	80% 100% 80% 100% 75% 75% 100%	4 4 4 4 4	3 4 3 4 3 3 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75%	4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media	50% 100% 100% 100% 100%	4 4 4 4 4	2 4 4 4 4 4	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control	80% 100% 80% 100% 75% 75% 100%	4 4 4 4 4 4	3 4 3 4 3 3 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75%	4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media	50% 100% 100% 100% 100%	4 4 4 4 4	2 4 4 4 4 4	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration	80% 100% 80% 100% 75% 75% 100% 100%	4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75%	4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media	50% 100% 100% 100% 100%	4 4 4 4 4	2 4 4 4 4 4	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control	80% 100% 80% 100% 75% 75% 100%	4 4 4 4 4 4	3 4 3 4 3 3 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75% 75%	4 4 4 4 4	3 3 4 4 3 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness	50% 100% 100% 100% 100%	4 4 4 4 4	2 4 4 4 4 4	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration	80% 100% 80% 100% 75% 75% 100% 100%	4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit	75% 75% 100% 100% 75% 75%	4 4 4 4 4	3 3 4 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy	50% 100% 100% 100% 100% 100% 75%	4 4 4 4 4	2 4 4 4 4 4 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration	80% 100% 80% 100% 75% 75% 100% 100%	4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans	75% 75% 100% 100% 75% 75%	4 4 4 4 4	3 3 4 4 3 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness	50% 100% 100% 100% 100% 100% 75%	4 4 4 4	2 4 4 4 4 4 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration	80% 100% 80% 100% 75% 75% 100% 100%	4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans	75% 75% 100% 100% 75% 75%	4 4 4 4 4 4	3 3 4 4 3 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness Viser Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the	50% 100% 100% 100% 100% 100% 75%	4 4 4 4 4 4 4	2 4 4 4 4 4 3 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function	80% 100% 80% 100% 75% 75% 100% 100% 50%	4 4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security	75% 75% 100% 100% 75% 75% **Complete 86% 69%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation	50% 100% 100% 100% 100% 100% 75% 75% 75% 75%	4 4 4 4	2 4 4 4 4 4 3 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration	80% 100% 80% 100% 75% 75% 100% 100% 50%	4 4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management	75% 75% 100% 100% 75% 75% **Complete 86%	4 4 4 4 4 4 7	3 3 4 4 3 3 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness Viser Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the	50% 100% 100% 100% 100% 100% 75% 75% 75% 75%	4 4 4 4 4 4 4	2 4 4 4 4 4 3 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5	80% 100% 80% 100% 75% 75% 100% 100% 50%	4 4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security	75% 75% 100% 100% 75% 75% **Complete 86% 69%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation	50% 100% 100% 100% 100% 100% 75% 75% 75% 75% 100%	4 4 4 4 4 4 4	2 4 4 4 4 4 3 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5	80% 100% 80% 100% 75% 75% 100% 100% 50%	4 4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation Support the formal assessment of Information Assurance (IA) skills Monitor the effectiveness of security training	50% 100% 100% 100% 100% 100% 75% 75% 75% 50% 75% 50%	4 4 4 4 4 4 4 4 4	2 4 4 4 4 4 3 3 3 2 3 4 2	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5	80% 100% 80% 100% 75% 75% 100% 100% 50%	4 4 4 4 4 4 4 4	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention Monitoring Incident Management	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72% 93%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3 3 4
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation Support the formal assessment of Information Assurance (IA) skills	50% 100% 100% 100% 100% 100% 75% 75% 75% 50% 75% 100% 50% 75%	4 4 4 4 4 4 4 4 4 4	2 4 4 4 4 4 3 3 3 2 3 4 2 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5 Organ	80% 100% 80% 100% 75% 75% 100% 100% 50% Step contr	4 4 4 4 4 4 4 4 7	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention Monitoring Incident Management Managing User Privileges	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72% 93% 75%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3 3 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation Support the formal assessment of Information Assurance (IA) skills Monitor the effectiveness of security training Promote an incident reporting culture	50% 100% 100% 100% 100% 100% 75% 75% 75% 50% 75% 50%	4 4 4 4 4 4 4 4 4	2 4 4 4 4 4 3 3 3 2 3 4 2	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5	80% 100% 80% 100% 75% 75% 100% 100% 50% Step contr	4 4 4 4 4 4 4 4 7	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention Monitoring Incident Management Managing User Privileges Removable Media Controls	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72% 93% 75% 89%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3 4 3 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation Support the formal assessment of Information Assurance (IA) skills Monitor the effectiveness of security training Promote an incident reporting culture	50% 100% 100% 100% 100% 100% 75% 75% 75% 50% 75% 100% 50% 75%	4 4 4 4 4 4 4 4 4 4	2 4 4 4 4 4 3 3 3 2 3 4 2 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5 Organ	80% 100% 80% 100% 75% 75% 100% 100% 50% Step contr	4 4 4 4 4 4 4 4 7	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention Monitoring Incident Management Managing User Privileges Removable Media Controls Secure Configuration	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72% 93% 75% 89% 86%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3 4 3 4 3
Produce corporate policies Limit the use of removable media Scan all media for malware Formally issue media to users Encrypt the information held on media Actively manage the reuse and disposal of removable media Educate users and maintain their awareness User Education and Awareness Produce a user security policy Establish a staff induction process Maintain user awareness of the cyber risks faced by the organisation Support the formal assessment of Information Assurance (IA) skills Monitor the effectiveness of security training Promote an incident reporting culture	50% 100% 100% 100% 100% 100% 75% 75% 75% 50% 75% 100% 50% 75%	4 4 4 4 4 4 4 4 4 4	2 4 4 4 4 4 3 3 3 2 3 4 2 3	Use supported software Develop and implement corporate policies to update and patch systems Create and maintain hardware and software inventories Manage your operating systems and software Conduct regular vulnerability scans Establish configuration control and management Disable unnecessary peripheral devices and removable media access Implement white-listing and execution control Limit user ability to change configuration Limit privileged user function Current status of 10.5 Organ	80% 100% 80% 100% 75% 75% 100% 100% 50% Step contr	4 4 4 4 4 4 4 4 7	3 4 3 4 3 3 4 4 4 4 2	Asses the risks and create a mobile working security policy Educate users and maintain their awareness Apply the security baseline Protect data at rest Protect data in transit Review the corporate incident management plans Control Area Information Risk Management Network Security Malware Prevention Monitoring Incident Management Managing User Privileges Removable Media Controls	75% 75% 100% 100% 75% 75% **Complete 86% 69% 68% 72% 93% 75% 89%	4 4 4 4 4 4 7	3 3 4 4 3 3 3 Actual Score 4 3 3 4 3 4 3