



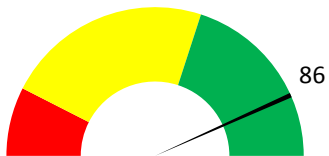
# City of London Corporation

## 10 Steps Maturity Assessment

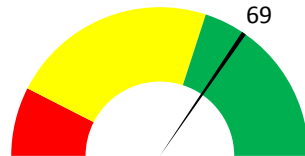
01 June 2019

# 10 Steps to Cyber Security: Dashboard

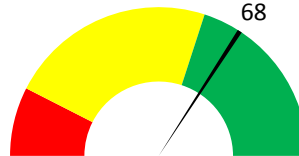
1. Information Risk Management



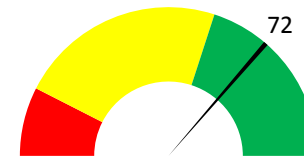
2. Network Security



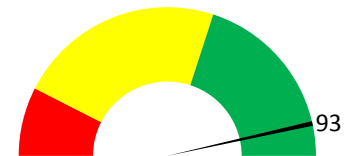
3. Malware Prevention



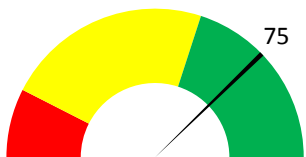
4. Monitoring



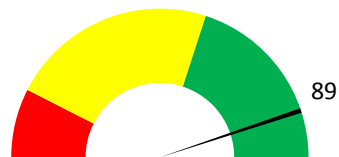
5. Incident Management



6. Managing User Privileges



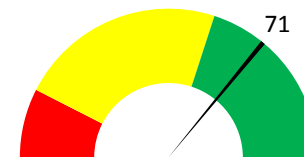
7. Removable Media Controls



8. Secure Configuration



9. Home and Mobile Working



10. User Education and Awareness



	% Complete	Target Score	Actual Score		% Complete	Target Score	Actual Score		% Complete	Target Score	Actual Score
<b>Information Risk Management</b>	<b>86%</b>	<b>4</b>	<b>4</b>	<b>Network Security</b>	<b>69%</b>	<b>4</b>	<b>3</b>	<b>Malware Prevention</b>	<b>68%</b>	<b>4</b>	<b>3</b>
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				
Promote a risk management culture	75%	4	3	Configure the exception handling process	100%	4	4				
				Monitor the network	50%	4	2				
				Assurance process	100%	4	4				
<b>Monitoring</b>	<b>72%</b>	<b>4</b>	<b>3</b>	<b>Incident Management</b>	<b>93%</b>	<b>4</b>	<b>4</b>	<b>Managing User Privileges</b>	<b>75%</b>	<b>4</b>	<b>3</b>
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%	4	4	Establish policy and standards for user identification and access control	75%	4	3
Monitor network traffic	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%	4	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				
Conduct a lessons learned review	75%	4	3	Educate users and maintain their awareness	75%	4	3				
				Report criminal incidents to law enforcement	100%	4	4				
<b>Removable Media Controls</b>	<b>89%</b>	<b>4</b>	<b>4</b>	<b>Secure Configuration</b>	<b>86%</b>	<b>4</b>	<b>3</b>	<b>Home and Mobile Working</b>	<b>71%</b>	<b>4</b>	<b>3</b>
Produce corporate policies	50%	4	2	Use supported software	80%	4	3	Asses the risks and create a mobile working security policy	75%	4	3
Limit the use of removable media	100%	4	4	Develop and implement corporate policies to update and patch systems	100%	4	4	Educate users and maintain their awareness	75%	4	3
Scan all media for malware	100%	4	4	Create and maintain hardware and software inventories	80%	4	3	Apply the security baseline	100%	4	4
Formally issue media to users	100%	4	4	Manage your operating systems and software	100%	4	4	Protect data at rest	100%	4	4
Encrypt the information held on media	100%	4	4	Conduct regular vulnerability scans	75%	4	3	Protect data in transit	75%	4	3
Actively manage the reuse and disposal of removable media	100%	4	4	Establish configuration control and management	75%	4	3	Review the corporate incident management plans	75%	4	3
Educate users and maintain their awareness	75%	4	3	Disable unnecessary peripheral devices and removable media access	100%	4	4				
				Implement white-listing and execution control	100%	4	4				
				Limit user ability to change configuration	100%	4	4				
				Limit privileged user function	50%	4	2				
<b>User Education and Awareness</b>	<b>75%</b>	<b>4</b>	<b>3</b>	<div> <p>Current status of 10 Step control areas across organisation.</p> <p>ASSESSMENT DATE: 01 June 2019</p> </div>				<b>Control Area</b>	<b>% Complete</b>	<b>Target Score</b>	<b>Actual Score</b>
Produce a user security policy	75%	4	3					<b>Information Risk Management</b>	86%	4	4
Establish a staff induction process	50%	4	2					<b>Network Security</b>	69%	4	3
Maintain user awareness of the cyber risks faced by the organisation	75%	4	3					<b>Malware Prevention</b>	68%	4	3
Support the formal assessment of Information Assurance (IA) skills	100%	4	4					<b>Monitoring</b>	72%	4	3
Monitor the effectiveness of security training	50%	4	2					<b>Incident Management</b>	93%	4	4
Promote an incident reporting culture	75%	4	3					<b>Managing User Privileges</b>	75%	4	3
Establish a formal disciplinary process	100%	4	4					<b>Removable Media Controls</b>	89%	4	4
								<b>Secure Configuration</b>	86%	4	3
								<b>Home and Mobile Working</b>	71%	4	3
								<b>User Education and Awareness</b>	75%	4	3