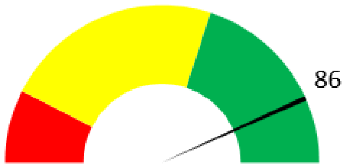
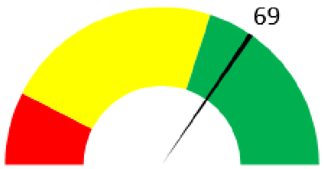
Appendix 2: 10 Steps to Cyber Security: Deep Dive - Dashboard & Breakdown

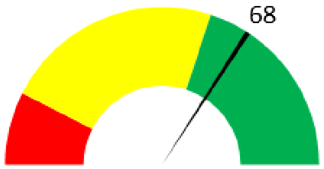
1. Information Risk Management



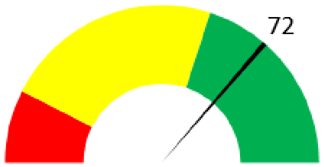
2. Network Security



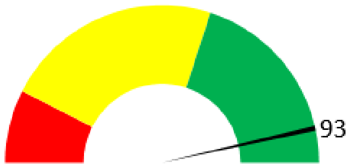
3. Malware Prevention



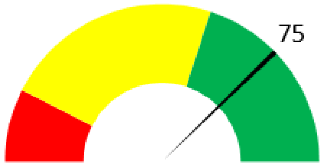
4. Monitoring



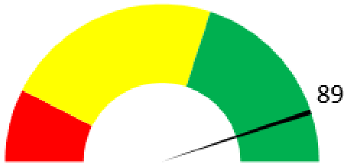
5. Incident Management



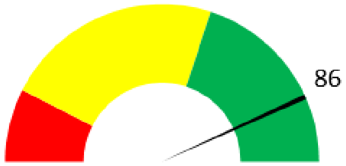
6. Managing User Privileges



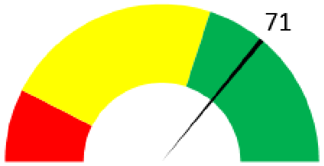
7. Removable Media Controls



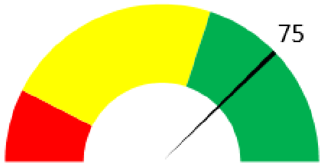
8. Secure Configuration



9. Home and Mobile Working



10. User Education and Awareness



1 – Information Risk Management

Taking risk is a necessary part of doing business in order to create opportunities and help deliver business objectives. For the City Corporation to operate successfully it needs to address risk and respond proportionately and appropriately to a level which is consistent with what risks it is willing, or not, to tolerate. If we do not identify and manage risk it can lead to business failure.

The lack of an effective risk management and governance structure may lead to the following:

- **Exposure to risk:** Without effective governance processes the Board will be unlikely to understand and manage the overall risk exposure of the organisation.
- **Missed business opportunities:** Risk decisions taken within a dedicated security function, rather than organisationally, will be motivated by achieving high levels of security. This may promote an overly cautious approach to risk leading to missed business opportunities or additional cost.
- **Ineffective policy implementation:** The board has overall ownership of the corporate security policy. Without effective risk management and governance processes the Board won't have confidence that its stated policies are being consistently applied across the business as a whole.

Control Measures:

	% Complete	Target Score	Actual Score
Information Risk Management	**86%**	**4**	**4**
Establish a governance framework	100%	4	4
Determine the organisation’s risk appetite	25%	4	2
Maintain the Board’s engagement with information risk	100%	4	4
Produce supporting policies	100%	4	4
Adopt a lifecycle approach to information risk management	100%	4	4
Apply recognised standards	100%	4	4
Make use of endorsed assurance schemes	100%	4	4
Educate users and maintain their awareness	75%	4	3
Promote a risk management culture	75%	4	3

2 - Network Security

Networks need to be protected against both internal and external threats. If the City Corporation fails to protect the networks appropriately we could be subject to a number of risks, including:

- **Exploitation of systems:** Ineffective network design may allow an attacker to compromise systems that perform critical functions, affecting the City Corporation's ability to deliver essential services or resulting in severe loss of customer or user confidence.
- **Compromise of information:** A poor network architecture may allow an attacker to compromise sensitive information in a number of ways. They may be able to access systems hosting sensitive information directly or perhaps allow an attacker to intercept poorly protected information whilst in transit (such as between your end user devices and a cloud service).
- **Import and export of malware:** Failure to put in place appropriate security controls could lead to the import of malware and the potential to compromise business systems. Conversely users could deliberately or accidentally release malware or other malicious content externally with associated reputational damage.
- **Denial of service:** Internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks, where access to services and resources are denied to legitimate users or customers.
- **Damage or defacement of corporate resources:** Attackers that have successfully compromised the network may be able to further damage internal and externally facing systems and information (such as defacing your organisation's websites, or posting onto your social media accounts), harming the organisation's reputation and customer confidence.

Control Measures:

	% Complete	Target Score	Actual Score
Network Security	**69%**	**4**	**3**
Police the network perimeter	75%	4	3
Install firewalls	100%	4	4
Prevent malicious content	75%	4	3
Protect the internal network	80%	4	3
Segregate network as sets	25%	4	1
Secure wireless devices	100%	4	4
Protect internal IP addresses	25%	4	1
Enable secure administration	25%	4	2
Configure the exception handling process	100%	4	4
Monitor the network	50%	4	2
Assurance process	100%	4	4

3 - Malware Prevention

Malware infections can cause material harm to our systems. This might include disruption of business services, unauthorised export of sensitive information or loss of access to critical data (eg caused by ransomware).The range, volume and source of information exchanged (as well as the technologies used) provide a range of opportunities for malware to be imported. Examples include:

- **Email:** Email still provides a primary path for internal and external information exchange. Malicious email attachments can cause their payload to be executed when the file is opened or otherwise processed. Email with malicious content may be specifically targeted at known individuals (known as spear phishing) with access to sensitive information, or at roles with elevated privileges. Alternatively malicious email may include embedded links that direct users to websites hosting malicious content.
- **Web browsing:** Users could browse (or be directed to) websites that may contain malicious content which seeks to compromise applications (such as the browser) that interact with that content
- **Web services:** User access to social media and other web based services could provide an ability for users to import a variety of data formats
- **Removable media and personally owned devices:** Malware can be transferred to a corporate system through the uncontrolled introduction of removable media or the direct connection of untrusted devices. This might include (for example) connecting a smartphone via a USB port, even if intended only to charge the device.

Control Measures:

	% Complete	Target Score	Actual Score
Malware Prevention	**68%**	**4**	**3**
Develop and implement anti-malware policies	75%	4	3
Manage all data import and export	75%	4	3
Blacklist malicious web sites	100%	4	4
Provide detailed media scanning machines	25%	4	1
Establish malware defences	75%	4	3
End user device protection	50%	4	2
User education and awareness	75%	4	3

4 - Monitoring

Monitoring provides the means to assess how systems are being used and whether they are being attacked. Without the ability to monitor your systems you may not be able to:

- **Detect attacks:** Either originating from outside the organisation or attacks as a result of deliberate or accidental user activity. Attacks may be directly targeted against technical infrastructure or against the services being run. Attacks can also seek to take advantage of legitimate business services, for example by using stolen credentials to defraud payment services.
- **React to attacks:** An effective response to an attack depends upon first being aware than an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused.
- **Account for activity:** You should have a complete understanding of how systems, services and information are being used by users. Failure to monitor systems and their use could lead to attacks going unnoticed and/or non-compliance with legal or regulatory requirements.

Control Measures:

	% Complete	Target Score	Actual Score
Monitoring	**72%**	**4**	**3**
Establish a monitoring strategy and supporting policies	50%	4	2
Monitor all ICT systems	75%	4	3
Monitor network traffic	75%	4	3
Monitor all user activity	75%	4	3
Fine-tune monitoring systems	50%	4	2
Establish a centralised collection and analysis capability	75%	4	3
Provide resilient and synchronised timing	100%	4	4
Align the incident management policies	75%	4	3
Conduct a lessons learned review	75%	4	3

5 - Incident Management

Security incidents will inevitably happen and they will vary in their level of impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking the City Corporation's business continuity or disaster recovery plans. Some incidents can, on further analysis, be indicative of more severe underlying problems.

If the City Corporation fails to implement an incident management capability to detect, manage and analyse security incidents the following risks could be realised:

- **Managing business harm:** Failure to realise that an incident is happening or has occurred limits your ability to manage it effectively. This may lead to a much greater overall business impact, such as significant system outage, serious financial loss or erosion of public confidence.
- **Continual disruption:** An organisation that fails to address the root cause of incidents (such as poor technology or weaknesses in the corporate security approach) could be exposed to repeated or continual compromise or disruption.
- **Failure to comply with legal and regulatory reporting requirements:** An incident resulting in the compromise of sensitive information covered by mandatory reporting requirements could lead to legal or regulatory penalties.

The City Corporation's business role determines the type and nature of incidents that could occur and the impact they might have, so a risk-based approach is being used to shape incident management plans.

Control Measures:

	% Complete	Target Score	Actual Score
Incident Management	**93%**	**4**	**4**
Obtain senior management approval	100%	4	4
Provide specialist training	100%	4	4
Define the required roles and responsibilities	100%	4	4
Establish a data recovery capability	100%	4	4
Test the incident management plan	100%	4	4
Decide what information will be shared and with whom	75%	4	3
Collect and analyse post-incident evidence	75%	4	3
Conduct a lessons learned review	100%	4	4
Educate users and maintain their awareness	75%	4	3
Report criminal incidents to law enforcement	100%	4	4

6 - Managing User Privileges

The City Corporation needs to understand what level of access employees need to information, services and resources in order to do their job otherwise it won't be possible to manage rights appropriately. Failure to effectively manage user privileges could result in the following risks being realised:

- **Misuse of privileges:** Users could either accidentally or deliberately misuse the privileges assigned to them. This may result in unauthorised access to information to either the user or a third party or to unauthorised system changes having a direct security or operational impact.
- **Increased attacker capability:** Attackers may use redundant or compromised user accounts to carry out attacks and, if able, they may return to reuse the compromised account or possibly sell access to others. The system privileges provided to the original user of the compromised account will be available to the attacker to use which is why they particularly seek to gain access to highly privileged or administrative accounts.
- **Negating established security controls:** Where attackers have privileged system access they may make changes to security controls to enable further or future attack or might attempt to cover their tracks by making changing or audit logs.

Control Measures:

	% Complete	Target Score	Actual Score
Managing User Privileges	**75%**	**4**	**3**
Establish effective account management processes	100%	4	4
Establish policy and standards for user identification and access control	75%	4	3
Limit user privileges	75%	4	3
Limit the number and use of privileged accounts	75%	4	3
Monitor	75%	4	3
Limit access to the audit system and the system activity logs	50%	4	1
Educate users and maintain their awareness	75%	4	3

7 - Removable Media Controls

Removable media introduces the capability to transfer and store huge volumes of sensitive information as well as the ability to import malicious content. The failure to manage the import and export of information using removable media could expose the City Corporation to the following risks:

- **Loss of information:** Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information stored on it. Some media types will retain information even after user deletion, placing information at risk where the media is used between systems (or when the media is disposed of)
- **Introduction of malware:** The uncontrolled use of removable media can increase the risk of introducing malware to systems.
- **Reputational damage:** The loss of media can result in significant reputational damage, even if there is no evidence of any specific data loss.

Control Measures:

	% Complete	Target Score	Actual Score
Removable Media Controls	**89%**	**4**	**4**
Produce corporate policies	50%	4	2
Limit the use of removable media	100%	4	4
Scan all media for malware	100%	4	4
Formally issue media to users	100%	4	4
Encrypt the information held on media	100%	4	4
Actively manage the reuse and disposal of removable media	100%	4	4
Educate users and maintain their awareness	75%	4	3

8 - Secure Configuration

Establishing and actively maintaining the secure configuration of systems should be seen as a key security control. Systems that are not effectively managed will be vulnerable to attacks that may have been preventable. Failure to implement good configuration and patch management can lead to the following risks:

- **Unauthorised changes to systems:** The protections you believe you have in-place may be changed by unauthorised individuals, either internal or external, leaving information at risk.
- **Exploitation of software bugs:** Attackers will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patches have been issued but not applied.
- **Exploitation of insecure system configuration:** An attacker could exploit a system that has been poorly configured by:
    - gaining access to information they are not authorised to see
    - taking advantage of unnecessary user rights or system privilege
    - exploiting unnecessary functionality that has not been removed or disabled
    - connecting unauthorised equipment that is then able to compromise information or introduce malware
    - creating a back door to use in the future for malicious purposes

Control Measures:

	% Complete	**Target Score**	**Actual Score**
Secure Configuration	**86%**	**4**	**3**
Use supported software	80%	4	3
Develop and implement corporate policies to update and patch systems	100%	4	4
Create and maintain hardware and software inventories	80%	4	3
Manage your operating systems and software	100%	4	4
Conduct regular vulnerability scans	75%	4	3
Establish configuration control and management	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

9 - Home and Mobile Working

Mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft/loss of devices. If the City Corporation does not establish sound mobile working and remote access practices we might be vulnerable to the following risks:

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.
- **Being overlooked:** Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.
- **Loss of credentials:** If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.
- **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

Control Measures:

	% Complete	Target Score	Actual Score
Home and Mobile Working	**71%**	**4**	**3**
Asses the risks and create a mobile working security policy	75%	4	3
Educate users and maintain their awareness	75%	4	3
Apply the security baseline	100%	4	4
Protect data at rest	100%	4	4
Protect data in transit	75%	4	3
Review the corporate incident management plans	75%	4	3

10 - User Education and Awareness

Users have a critical role to play in helping to keep the City Corporation secure, but they must also be able to effectively do their jobs. If we do not effectively support employees with the right tools and awareness we are vulnerable to the following risks:

- **Removable media and personally owned devices:** Without clearly defined and usable policies on the use of removable media and personally owned devices, staff may connect devices to the corporate infrastructure that might lead to the inadvertent import of malware or compromise of sensitive information
- **Legal and regulatory sanction:** If users are not aware and supported in how they handle particular classes of sensitive information, the City Corporation may be subject to legal and regulatory sanction
- **Incident reporting culture:** Without an effective reporting culture there will be poor dialogue between users and the security team. This is essential to uncovering near misses and areas where technology and processes can be improved, as well as reporting actual incidents.
- **Security Operating Procedures:** If security operating procedures are not balanced to support how users perform their duties, security can be seen as a blocker and possibly ignored entirely. Alternatively, if users follow the procedures carefully this might damage legitimate business activity.
- **External attack:** Since users have legitimate system accesses and rights, they can be a primary focus for external attackers. Attacks such as phishing or social engineering attempts rely on taking advantage of legitimate user capabilities and functions.
- **Insider threat:** Changes over time in an employee's personal situation could make them vulnerable to coercion, and they may release personal or sensitive commercial information to others. Dissatisfied employees may try to abuse their system level privileges or coerce other employees to gain access to information or systems to which they are not authorised. Equally, they may attempt to steal or physically deface computer resources.

Control Measures:

	% Complete	Target Score	Actual Score
User Education and Awareness	**75%**	**4**	**3**
Produce a user security policy	75%	4	3
Establish a staff induction process	50%	4	2
Maintain user awareness of the cyber risks faced by the organisation	75%	4	3
Support the formal assessment of Information Assurance (IA) skills	100%	4	4
Monitor the effectiveness of security training	50%	4	2
Promote an incident reporting culture	75%	4	3
Establish a formal disciplinary process	100%	4	4