Isle of Wight Council

Isle of Wight Council CYBER SECURITY STRATEGY 2023 - 2030

26th October 2023 / Draft v0.3

1 Document information

Title:	IWC Cyber Security Strategy 2023 - 2030
Status:	Draft
Current version:	0.3
Author:	Roger Brown, Strategic Manager - ICT & Digital Services (SIRO) ICT, Customer Services roger.brown@iow.gov.uk 07813 998618
Sponsor:	Wendy Perera, Chief Executive wendy.perera@iow.gov.uk (01983) 821000
Consultation:	Legal Department Corporate Information Unit ICT Management Information Security Group Learning and Development Chief Executive Officer Corporate Management Team Portfolio Holder
Approved by:	Councillor Karen Lucioni
Approval date:	19th December 2023

1.1 Version history

Version	Date	Description
0.1	9th June 2023	For consultation
0.2	28h September 2023	For consultation – following LGA Cyber 360
0.3	26th October 2023	For consultation – following CMT Feedback

Document Status

This is a controlled document. While this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

2 Contents

3 Context

3.1 Importance of cyber security

In 2022 the council approved its Digital Strategy which set out four priorities for digital improvement (Digital Island, Digital Citizen, Digital Council and Digital Intelligence). To enable these priorities to be achieved and the principle maintained, whilst protecting the digital information held, it is crucial that the council has an appropriate approach to cyber security. The Digital Strategy also included the principle that the council will be “Secure by design” and this strategy expands on the statements made in that principle:

- Whether it be the coding of our website or the architecture of our internal and external facing services, they must be secure by design.
- We will take a risk-based approach in meeting the customer end to end service delivery requirements and the information security and cyber security measures that are necessary to protect the council’s information assets.
- These must unite, acting to provide a proportionate and multi-layered umbrella of security.

It is vital, that in this ever-changing landscape of cyber threats, the council considers its protection of the information it holds and does this through appropriate risk-based investments in cyber security.

3.2 Challenges and opportunities for the council

Having worked with the Local Government Association (LGA) Cyber team and the Department for Levelling Up, Housing & Communities (DLUHC) Cyber team it has been established that there continues to be a gap between where the council needs to be and where we are now with regards to cyber security. The importance of bridging this gap is highlighted by the significant increase in the volume of cyber-attacks seen against UK government and educational establishments over the past few years.

40% of all incidents managed by the National Cyber Security Centre (NCSC) between September 2020 and August 2021 had some level of impact on the public sector in the UK. For the 12-month period of 2022 the NCSC estimated that, across all UK businesses, there were approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud as a result of cyber crime.

Following consultation with the NCSC, the DLUHC cyber team and advice from the LGA cyber team the council has completed several cyber security based technical enhancements over the last three years. The council continues to invest in systems and solutions to close the technical gaps identified and reduce the attack surface of the organisation.

In early 2023, the council completed a cyber security culture review, and this has shown that there remain opportunities for enhancements in our cyber defences through greater awareness and culture change both within the council and in our partnership arrangements with other organisations including suppliers.

In June 2023, the council completed a Cyber 360 engagement with the LGA, and the report received included 39 recommendations across leadership and governance, risk, asset management, supply chain, policy and process, identity and access, data and systems, resilience, people management, response and recovery and learning and development. Those recommendations helped shape this strategy.

4 Approach

4.1 Vision and aim

The council approach is to follow the vision and aim of the 2022-2030 UK government Cyber Security Strategy:

Vision: To ensure that core government functions - from the delivery of public services to the operation of National Security apparatus – are resilient to cyber-attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

Aim: To achieve its vision the strategy pursues a central aim - for government's critical functions to be significantly hardened to cyber-attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

The council's aim should meet the target of "being resilient to known vulnerabilities and attack methods no later than 2030".

4.2 Pillars

To focus resources, manage risk and achieve this aim the council is basing its Cyber Security strategy on the same two complementary strategic pillars and five underlying objectives. Although these pillars and objectives are set by the government at a national level, they are still applicable to the council and its own cyber security at a local level.

4.2.a To build a strong foundation of organisational cyber security resilience; as an organisation sharing the responsibility, the council will use governance structures, mechanisms, tools, and support to manage our cyber security risks.

4.2.b To ‘Defend as one;’ the council will work with partners and suppliers to ensure we can “present a defensive force disproportionately more powerful than the sum of its parts.”

4.3 Objectives

These objectives and statements are taken from the UK ‘Government Cyber Security Strategy 2022 – 2030’. They are provided as advisable dimensions for what needs to be considered with regards to a public bodies’ cyber resilience, this strategy will map out the Isle of Wight councils approach to each of these objectives.

4.3.a Manage cyber security risk:
Effective cyber security risk management processes, governance and accountability enable the identification, assessment, and management of cyber security risks - at both the organisational and cross-government level.

4.3.b Protect against cyberattack:
Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.

4.3.c Detect cyber security events:
Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.

4.3.d Minimise the impact of cyber security incidents:
Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.

4.3.e Develop the right cyber security skills, knowledge, and culture:
Sufficient, skilled, and knowledgeable professionals fulfil all required cyber security needs - extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - all underpinned by a cyber security culture that promotes sustainable change.

5 Objective 1 - Managing Cyber Risk

The basic principle of this strategy is the management of risk. While there can never be guarantees with cyber security, appropriately focused risk management activities would enable mitigating actions to be completed and risks reduced.

For these risks to be evaluated and understood it is vital that the council understands the digital assets held and where and how they are processed. Appropriate governance and clear accountability will enable the council to plan mitigation activities and monitor progress towards achieving the risk reduction goals effectively and efficiently.

5.1 Governance and accountability

Cyber risk is seen within the council to be an integral part of our risk management processes. Strategic level risks such as:

- Maintaining compliance with the Public Services Network Code of Connection (PSN CoCo)
- Risk of Cyberattack
- Loss of ability to process card payments due to lack of Payment Card Industry Data Security Standard (PCI-DSS) compliance.

These are shown on the corporate risk register with mitigating actions and associated sub risks for individual detailed activities.

In addition to the strategic risks being presented within the corporate risk register, the Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO) will submit an annual report to Corporate Management Team (CMT) followed by Corporate Leadership Team (CLT) (heading of this report are included in Appendix A). The focus of these reports will be specific identified risks and proposed mitigation measures and progress against them.

The council will review, update, and monitor risk management progression. These reviews must aim to ensure that risks are scored uniformly and that all departmental risk registers identify and manage specific cyber risks for their own services.

CMT will continue to monitor the cyber security culture ensuring management, teams and services are engaged in the process of understanding and owning their own cyber security risks. CMT acknowledges that Cyber Security is not a set of processes and activities solely owned and managed by the ICT and Digital Services teams.

5.1.a Identified roles and responsibilities:

These are the roles that help protect our information from various threats. The SIRO will maintain a section on the Intranet that provides information about the staff members who currently hold these roles, and their responsibilities in the area of Information Security and Cyber Security.

- Data Protection Officer (DPO) and deputy DPO's.
- Senior Information Risk Owner (SIRO) and an identified deputy SIRO.
- Caldicott Guardian.
- Information Asset Owners (IAO); this role is a senior position held by a Strategic Manager or above and will be identified for every service.
- Information Governance Lead (IGL); this management role will be identified for every service.
- Information Asset Administrators (IAA); this role will be identified within every service to support the role of the IAO and IGL.

5.1.b Governance meetings

The Intranet section on Information Governance and Cyber Security will also provide all the terms of reference for the following groups:

- Internal Information Governance Group (IIGG) – the DPO is the chair of the IIGG.
- The IIGG meetings are to be held on a bi-monthly basis. IGL or nominated deputy must represent their services and IAO's at the IIGG meetings.
- Information Security Group (ISG) – the SIRO is the chair of the ISG
  The ISG meetings are to be held on a bi-monthly basis.

5.1.c Governance reporting

- The DPO and SIRO will prepare annual update reports for CMT, managers and CLT. These reports will include information on the investments made, their impact on reducing risk and the ongoing threats that are being monitored with future action plans.
- The report for CMT / CLT will be presented along with the budget management process to ensure that the risk reduction measures are properly planned and integrated into the council's budget.
- Cyber security will be a regular item on the agenda of the DMT meetings / service boards of all Directors, under the section of risk management.
- The Caldicot Guardian will report any concerns or issues to CMT/CLT.

5.2 Assets and vulnerabilities

The SIRO will make sure the council has an automated asset management system and vulnerability assessment system in place to ensure that there is a comprehensive picture of the cyber security risks within the council. This picture will enable the appropriate risk analysis to be completed and remedial action plans to be created.

The SIRO will make sure that vulnerabilities are discovered on a constant basis and the solutions employed must provide a prioritised list to ensure that the limited resources are focused on remediating the higher risk vulnerabilities. Ensuring that the appropriate ICT technical teams can rapidly assess, manage, and resolve them in a robust manner.

To ensure that it has information about critical vulnerabilities shared across government the council's ICT service will be an active participant within the South East Government Warning, Advisory and Reporting Point (SEGWARP) and maintain close contact engaging whenever appropriate with the National Cyber Security Centre (NCSC), Local Gov Digital Cyber team and the LGA Cyber team.

5.3 Data assets

There is a significant range of data held by the council, some of it publicly available, some personal sensitive information and some classified. The council will ensure it maintains an ISO27001 conformant Information Security Management System (ISMS) and it will also maintain Information Asset Registers (IARs) to ensure it has a comprehensive record of all data assets.

The IAR's will ensure that the council can adequately assess risk to each data asset and ensure that sufficient protections put in place will be proportional to the sensitivity of the data being protected and ensure compliance with all data protection legislation.

Through a process of internal evaluation, independent assessment, and certification the council will maintain compliance with PCI-DSS incorporating any additional requirements required as versions change over time. E.g. the upgrading of the council compliance regime to comply with the replacement of v3.2.1 with v4 by March 31, 2024 at the latest.

5.4 Supply Chain Risk

The council utilises a significant number of commercial products and services in the delivery of its services to our customers. As our supply chain becomes more interconnected and information exchange automated for enhanced services delivery and cost reduction, it is critical that the council considers all areas of the supply chain for cyber security risk.

The cyber security risks associated with supply chain could be direct though interconnected systems or indirect through loss of services or supply of goods through the cybercriminal taking down our suppliers' systems instead of ours. This action can still have significant impact on the council's ability to deliver its services.

Through improved understanding by all services of their supply chains and the points in them that could be risks to service delivery mitigation, through contractual controls and contract governance of both direct suppliers and subcontractors will support the reduction of identified risks.

The procurement team will ensure that it incorporates a cyber security supply chain risk management question into the Procurement Initiation Form (PIF). This will ensure that, every procurement whether it is directly managed by the service or ICT will have a common approach to cyber security through the advice and guidance given at the time of tendering.

When appropriate, Invitation to Tender documents will incorporate the councils Supply Chain Security Statement of Applicability questionnaire. Through discussion between ICT, procurement, and the services procuring their solutions, the questionnaire will be assessed in a proportionate and appropriate level. Therefore, in the future there will be suitable cyber security requirements incorporated into all contracts signed.

Central government has stated in the national cyber security strategy that:

"Cyber security requirements in government procurement frameworks and contracts will be strengthened, ensuring that commercial arrangements are risk based and consistent with robust clauses relating to the identification and management of subcontractors."

The council's services regularly utilise government frameworks for procurement and so this new process instigated by central government will aid the council in delivery of this supply chain risk reduction process.

5.5 Threat information

The seamless collation and dissemination of threat information is crucial to enabling appropriate defence mechanisms to be created, utilised, and reviewed. The ICT cyber security team and Information Security Manager will work with SEGWARP, the NCSC, Local Gov Digital Cyber team and the LGA Cyber team to ensure that it they have the required strategic, tactical, technical, and operational detail needed to predict and defend against attacks. Any information appropriate for dissemination to councillors, staff and partners will be sent out from the cyber security team.

Threat information updates will also come from our suppliers and specialist cyber defence systems that are designed to highlight threats through integrated threat feeds and prioritise risks and provide step-by-step directions to ICT services for efficient and focused remediation activities.

5.6 Cyber security data

It is vital that the council's cyber security team have access to relevant and actionable cyber security data. The ICT service will continue to use the current sources of cyber security information:

- South East Government Warning, Advisory and Reporting Point (SEGWARP)
- National Cyber Security Centre
- Local Gov Digital Cyber team
- LGA Cyber team

In 2022 the government announced the creation of a new Government Cyber Coordination Centre (GCCC) with the aim of "ensuring that targeted cyber security data is shared across government - in a way that is appropriate to its classification and legal status". The Information Security Manager will ensure that the council is included in the outputs of this centre to local authorities.

5.7 Government cyber security measures

Historically the council has maintained compliance with the Public Services Network Code of connection (PSN CoCo). In 2022 government announced that this process would be changing in the future, and a version of the Cyber Assessment Framework (CAF) would be created for local government organisations.

The published aim of the CAF is: "Focusing on an organisation's most important functions, including critical infrastructure, it will provide an objective way of assessing whether an organisation's cyber security assessment and management of cyber security risk is proportionate and within accepted risk tolerances."

The PSN CoCo has required the council to conduct regular (at least annually) penetration tests, it is expected that a potential LA CAF will continue to require these activities but additionally extend requirements to real world testing and exercises. These exercises are not to be just managed by ICT teams but are such that services are essential in their completion. The focus of these activities and the associated assessment framework documentation is to provide confidence that the cyber security risks are being managed sufficiently by all stakeholders.

The council's Information Security manager is involved in the development of the potential LA CAF by assisting the consultancy company that have been employed by central government in identifying all existing compliance regimes and related MOU's and data sharing agreements (50+). This is to ensure that whenever possible the potential LA CAF simplified the compliance regime in the future.

The council has always prioritised activities around compliance to PSN CoCo, the NHS Data Security and Protection Toolkit (NHS DSPT) and will continue to prioritise compliance to the CAF when published.

5.8 Private sector and partnerships

The council relies on partnerships with other councils and the private sector to deliver its cyber security services. It is crucial to the protection of the information processed on behalf of our customers that the SIRO works closely with our partners and suppliers to ensure that our cyber security challenges are tackled collaboratively.

6 Objective 2 - Protecting against Cyber Risk

The process of protecting against cyber-attack is dependent upon the council's collective understanding of risk. The cooperative response between ICT, councillors, and services in risk mitigation activities will ensure that our attack surface is greatly reduced by increasingly hardening our overall security posture.

6.1 Secure technology and digital services

The council uses a range of technologies to deliver its services, these are a mixture of both in house created and bought in solutions, these can all present areas of attack surface. All systems will be based on the 'secure by design' framework published by UK government.

The ability for the council to protect its information assets against evolving vulnerabilities and the constantly moving threat landscape can be constrained by any presence of legacy and potentially vulnerable ICT systems. The SIRO will ensure that the ICT service continues to manage, upgrade or remove such ICT systems and put the necessary safeguards and ongoing investment in place to ensure ICT systems are sufficiently secure throughout their lifecycle.

The SIRO will annually review roles and responsibilities around patch management within hardware and all applications and ensure that where contracts and system administration are managed outside of ICT, there is clear visibility of the nature and security status of applications. All contracts for applications will incorporate patch management requirements to ensure that all parties are clear on where responsibilities lie for cyber security.

The ICT service will maintain a set of design principles and guides for the development and procurement of all systems. This approach will be used to ensure that there is a consistent use of appropriate cloud services (private/hybrid/public) and security standards. The approach will be proportionate to the risk and importance of the system and enable the building of highly resilient and available solutions whilst delivering value for money for investments made.

6.2 Cyber Security Controls

The council will deploy cyber security controls that are proportional with the risk profile of compromise for all ICT systems. The SIRO will continue to work with the LGA Cyber Team, DLUHC Cyber Team and SEGWARP to ensure that it is able to assess risk and establish the appropriate profile of threats. This will enable the resulting security approach to be one that mitigates risk to a suitable level whilst limiting impact to the business where possible.

The Strategic Manager for ICT and Digital Services will conduct access recertification activities to ensure that the system-based security controls are appropriate. It is the responsibility of all staff and councillors to engage with ICT during reviews to ensure that access controls provided are required and used appropriately to limit the attack surface to cybercriminals.

Control changes within applications will be moved away from cloning existing user privileges and the council will develop a Role Based Access Control (RBAC) model based on an officer's job title and role. Using RBAC within Identity and Access Management (IAM) for all staff and councillors and Privilege Access Management (PAM) for administration accounts the council will reduce the risk of account compromise.

A risk-based approach will be documented for access to all systems. The council will use Active Directory Federated Services (ADFS) based Single Sign On (SSO) with Multi-Factor Authentication (MFA) wherever practical and risk-appropriate for authentication independent of where an application is hosted.

6.3 Secure Configuration

The councils' systems will require appropriate architecture configuration to ensure that standard profiles for common technologies are used. The SIRO will ensure that both Hardware and Software Policies are maintained and reviewed annually to ensure that architectures are developed and updated to meet current needs and mitigate threats. Updated versions will be approved through the Information Security Group.

By regularly reviewing our architecture profiles and our adoption of the secure by design approach published by government the council will address some of the inherent risks in ICT systems. It is the responsibility of all the designers, administrators and ultimately the end users of any ICT systems to contribute to the continued compliance to security requirements.

6.4 Shared capabilities

The council will ensure that whenever possible common aspects of its ICT architecture will be utilised to ensure that protection is shared beyond our own resources.

By using the tools provided by government bodies, partner local authorities and suppliers across common areas to reduce unnecessary individuality the ICT Service teams will work on proactively mitigating against specialist distinct threat profiles to help prevent known and emerging attack trends.

The ICT Service teams will develop training, policy, and processes for the management of access to systems that can be applied and followed both by teams within ICT who manage access to applications and by systems administrators within services who locally manage applications.

6.5 Information and Data Security

The council has a responsibility to ensure that all data held by the council must be appropriately protected, the basis for the protection of information will be the backup and restore technologies and processes in use. The ICT Service and the customer service lead will develop and agree clear Service Level Agreements (SLA) on a per application basis for the entire architecture.

These SLA’s will be based on existent Recovery Point Objectives (RPO) from the backup frequency and Recovery Time Objectives (RTO) which will be based on established restore times from the systems in use.

The service lead and Emergency Management team will maintain Business Continuity Plans (BCP) to ensure expectations are known, processes are developed, and service staff are trained in enactment and delivery of these processes.

To ensure this can be done effectively the corporate information unit (CIU) will maintain a Protective Marking Policy. This policy will be reviewed at a minimum of every two years to ensure that it is aligned with national government guidance.

The Policy will ensure that all staff and councillors have the information to appropriately classify all information. Through classification the council will ensure that information is handled, shared, stored, and processed commensurately with the risk the information presents.

The councils Digital Strategy incorporates a priority of Digital Intelligence that explains our approach to unlocking the value of data through analysis to improve service delivery and evidence-based decision making and utilising business intelligence tools to understand the needs of our residents, customers, businesses, and visitors. Service leads will ensure that information and data security is kept at the heart of these processes.

ICT Service team leads will review the data retention capabilities of its internally developed systems and develop a remediation plan to rectify any issues. It will enhance its internal design standards to ensure all future internally developed solutions have the needed capabilities around data security, retention, and protection.

Service Leads will review how its data retention policies are being applied to the unstructured information stores to ensure that appropriate controls for retention, access control, protective and destruction marking are in place.

7 Objective 3 - Detecting Cyber Security Events

Despite the council using a robust and risk-based approach to cyber security and information protection the inherent unknown vulnerabilities hidden in ICT systems mean that cyber-attacks will still occur. The council will use comprehensive vulnerability tools and processes to identify and prioritise emerging risks to assist in effective management of them.

7.1 Detection within the Council

The councils' networks, systems, applications, and all end points will be constantly monitored with proportionality appropriate detection and protection capabilities. The systems will generate and offload log data to assist in the detection of Cyber threats.

Threat detection monitoring will not be provided by a single solution that can in itself have vulnerabilities but rather by multiple solutions all focusing on different views of the threat landscape. This approach is designed to ensure that we appropriately limit the areas where new patterns of compromise are available to cybercriminals whilst still maintaining accessible systems for business and service delivery.

The council's Procurement and ICT Service teams will work with its supply chain to exchange appropriate information on threats and activities monitored that may indicate compromise of any ICT systems.

7.2 Partner detention and alerting

The council will ensure that all appropriate information regarding cyber incidents is shared between partners in a timely and appropriate manner. Partners will be informed of the IWC expectations through the distribution of the Partners Cyber

Incident Response Procedure. The ICT Service team leads will create a partnership cyber response network utilising the collaboration features of Microsoft Teams.

This sharing of incident information will enable all parties to ensure that information and data security can be maintained by one partner in the event another partner is compromised. The aim is that, whenever possible, information and potentially resources are shared to ensure risk mitigation of further compromise amongst a wider set of organisations.

7.3 Detection at scale - e.g., SEGWARP

The council will utilise shared information platforms with other local authorities and government bodies such as DLUHC, NCSC as well as partnership bodies such as the LGA, and SEGWARP to ensure that we and our partners gain the most benefit from the sharing of cyber security information.

The effective sharing of these detected activities enhances every organisations capabilities and assist each of them in the reduction of the active threat landscape available for attack within their own ICT systems.

8 Objective 4 - Minimising the impact of Cyber Security Incidents

Even with a well-designed and risk assessed set of security protections and detections measures in place the council will still be required to deal with cyber security incidents. It is therefore essential that the council has the ability and planning in place to deal with these incidents whenever they happen and can minimise the impact on ICT systems and the services they are used to provide.

By implementing a risk assessed set of well designed, managed and monitored systems and processes for Cyber Security for the council, we are ensuring that we are appropriately hardened and limiting where possible the attack landscape. We must still ensure that we and our partners are ready to respond to the incidents and keep as many essential services running whenever possible.

8.1 Response preparation

The council has created a Cyber Incident Response Plan (CIRP). This plan has been tested and will continue to be reviewed annually for required updates to maintain preparedness for the potential risks that have emerged since the last update.

Following the annual review and to ensure appropriate dissemination of changes, the council services, with support from the Emergency management team will complete at least one tabletop exercise for this plan annually. To ensure appropriate complexity of the exercise the scenarios will combine a cyber incident with a non-cyber incident for those services involved.

Should emerging threats require immediate and emergency updates to the plan an additional review and dissemination of changes will be performed.

The council has created a Partner Cyber Incident Response Procedure (PCIRP) and through the Local Resilience Forum (LRF) the Emergency Management team will engage with other partners inviting them to an annual tabletop exercise where these processes and procedures can be evaluated and enhanced.

The CIU will complete an annual review of the content and training that is available to officers and managers around the handling of data breaches. It must be kept up to date to ensure it supports them to take the correct steps as well as how and when to involve support from the appropriate dedicated internal team.

8.2 Incident response

The council has a Cyber Security function managed by the ICT Cyber Security and Infrastructure Manager. This team is there to provide capacity and expertise in the triage of cyber security incidents, assess their impacts and prioritise appropriate response activities.

The team are responsible for the creation and management of the playbooks for the commonly known threats the council face. These playbooks will provide support and guidance to ICT staff in other teams as well as staff and councillors when required.

The Cyber Security staff maintain connections with external experts such as the NCSC, DLUHC and LGA cyber teams to provide a channel of communications for rapid advice when new and unknown incidents occur.

The council will develop a robust approach to recovering from a cyber incident based on a clearly prioritised set of applications with an agreed recovery order that CMT has agreed via the agreement of ICT SLA and the ICT Disaster Recovery Plan (DRP).

ICT will update the ICT Service Level Agreement (SLA) and ICT Disaster Recovery Plan (DR Plan) on annual basis to ensure that the corporate management team are informed of all changes to the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) information for all applications. The Directors and services managers are responsible for ensuring that the RPO and RTO information is incorporated into services' business continuity plans.

8.3 Incident Recovery

Following the completion of incident response processes and procedures, the Cyber Incident Response Team will work with ICT colleagues, as well as any affected customers to ensure that recovery is completed and that any lessons learnt during the incident are then put into practice by all required areas.

It is critical that recover activities incorporate a risk review of all areas affected by the incident so that those risks identified as still outstanding have appropriately proportionate mitigation activities identified and planned.

8.4 Lessons Identified

The Emergency Management team in conjunction with the service leads taking part in any particular exercise will follow an agreed process of sharing experiences between business continuity exercises. Historically the exercises have been delivered in an ad-hoc manner with limited sharing of lessons learned outside of those services involved. This approach narrows the potential for improvement; to ensure that information is shared wider, updates will be provided to directors to discuss in the Directorate Management Team meetings.

To enable continued improvement of the council's defence in Cyber Security it is important that lessons learnt reports are generated for every cyber incident processed by the Cyber Security Team. Reports generated following Cyber Incident Response activities must not be based on blame but rather focused on the development of a revised risk assessment based on the completed root cause analysis.

Whenever possible the lessons learned within one service after a cyber incident will be shared widely across all services. The aim of this process is to help share learning between wider elements of the council beyond the affected service and the centre and reduce the risk of repetition of similar incidents. These post incident activities should have an appropriate amount of information so that they support better cyber security in the future.

9 Objective 5 - Developing the right skills, knowledge, and culture

With the majority of the council running services that utilise ICT systems at some stage in their service delivery model all staff and councillors can be considered part of a cyber workforce.

Achieving the vision and aims of this strategy will not be possible without skilled and knowledgeable staff and councillors. These skills and knowledge need to be appropriate for all areas including ICT technical, cross corporate policy and strategy creators, all areas of risk management processes, and council leadership.

9.1 Skill requirements

The Information Security Manager will ensure that the council continuously reviews its training programme for technical staff, staff, management, and councillors. The Information Security Manager will take guidance from expert partner organisations such as NCSC. LGA, DLUHC and SEGWARP on the breadth and depth of the training that would be appropriate for all audiences identified.

When the UK Cyber Security Council has appropriate advice and guidance and any standards applicable to Local Authorities the Information Security Manager of the council will ensure that this advice is also considered when planning training to ensure the entire cyber workforce is appropriately skilled.

9.2 Attract and retain talent

The council will continue to utilise apprenticeships, graduate traineeships, career grades and any other appropriate programmes to ensure that it can attract and retain a diverse cyber security workforce.

The Information Security Manger will monitor the current accreditations and development programmes being used within the UK local authorities through contact in the LGA, DLUHC and SEGWARP. This information will assist in the creation of appropriate support and learning programmes especially to the senior positions outside of the main ICT department.

9.3 Develop talent

The council will keep an in-house Cyber Security Team to ensure it can control the skills development, qualifications, knowledge, and expertise of this team to provide the best provision to council services and subsequently our customers.

The council will ensure that the team has clear learning and development and support, and the skills of its officers are kept updated with recognised professional qualifications in-line with national standards such as the CISSP and CISM qualifications.

9.4 Cyber security knowledge across the council

The need for cyber security knowledge is not confined to ICT, it needs appropriate consideration across all services of the council. Whilst the degree of expertise needed will vary upon the service in question, all staff and councillors require an appropriate knowledge of cyber security and the council processes regarding it.

Learning programmes will be focused for specific audiences. Examples of such specific programmes will be CMT, DMT's, new and existing managers, Councillors, and those staff in front line service roles in high-risk areas. It is vital that all staff and councillors understand the concepts of cyber security and how to apply them within their own roles.

The council will engage with partners to better understand the requirements of the services it provides and a programme of learning and development including potentially desktop exercises for staff and councillors will be provided through aligned processes, guidance, and support.

9.5 Cyber Security culture

It is critical for effective Cyber Security that the council has a culture where all staff and councillors can learn, question and challenge; enabling all to improve and collectively enhance our cyber defences.

The council will promote a pro-active philosophy asking staff and councillors to contribute positively to a culture of open honest information sharing around practices and risk. Leadership, communications, and consistency are key to a council wide culture being developed.

The council acknowledges that each service will have its own cyber security requirements based on its information and risk assessments of that information. No one service will be enabled to bypass cyber security policies or technology for service delivery without all appropriate governance and risk assessment processes being followed.

10 Measuring success

10.1 Achieving the aims

Given the ever-changing landscape and complex nature of cyber security vulnerabilities, combined with the continuous evolution of cyber-attack tactics, techniques and procedures used by cybercriminals. The process for accounting for known vulnerabilities is difficult.

The expected Local Government CAF profile will assist the council in assessing its cyber resilience measures. By utilising a combination of penetration testing and desktop exercises, both internally and with partner agencies, we will annually review and update our policies, processes, ICT systems and playbooks.

This strategy sets out very ambitious aims for a council that has pressure on its resources, these aims, and the benefits gained from achieving them are critical to the success of the council over the life of this strategy.

The process of annual review, currently against PSN and NHS-DSPT requirements and in the future against the CAF will provide an annual statement of achievement against this aims of this strategy.

10.2 Maintaining appropriate measures of resilience

The evolving nature of cyber security and the threats posed against the council mean that the measures we must take to protect our services and the information we hold require periodic review. The ICT service teams will review their risk logs against the current CAF profiles on a quarterly basis and ensure that annually all updates to the appropriate CAF profile for a Local Authority are incorporated into our local CAF profile assessment systems.

10.3 KPI's

To ensure that the council has a complete picture of the progression in delivering against this strategy and its aims. Appropriate KPI’s will be developed, during the life of the strategy the KPI’s will change to adapt to be the most appropriate for the time. The KPI’s will be reviewed by ICT management, using industry standards for potential updates and, once the CAF profiles for local government have been evaluated relevant KPI’s will be created. All KPI’s will be based on the key principles that:

- KPI’s will place a minimum burden on services to calculate and publish.
- Data generated will be automated whenever possible and published in pre-agree formats on a set schedule.
- KPI’s will be achievable within the resource constraints of the council.
- KPI’s will be realistic against the proportional risk requirements of the council’s services and the information they store, process, share and dispose of.
- KPI’s will be linked to genuine quantifiable benefits of the cyber activities being measured.

11 Implementing the strategy

The council is not starting its Cyber defences and risk management processes from a blank canvas, some of the activities are already in production, some are in projects being implemented and some are unfunded investigations for the future. By looking towards the Vision and following the aim utilising the pillars stated, all projects instigated during the life of the strategy can be measured against it.

11.1 Transformation Proposals

1. Adopt the CAF and measure the council against the most appropriate profile published for local authorities.

2. Establish the partnership cyber response network for the council to endure greater protection through collaboration.

11.2 Implementation Plan

The implementation plan for this strategy will be a live document covering the life span of the strategy, it has been created to be approved alongside the strategy and will be shared with all stakeholders and updated on a quarterly basis with a progress report being presented to CMT and CLT as part of the Quarterly Performance Monitoring Report (QPMR).

12 Cyber Assessment Framework (CAF)

The national Cyber Assessment Framework (CAF) was developed by the NCSC - in its role as national technical authority for cyber security - to provide a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

The CAF comprises four objectives: managing security risk; protecting against cyber-attack; detecting cyber security events; and minimising the impact of cyber security incidents. These objectives are underpinned by 14 principles that are supported by 39 contributing outcomes, which specify what needs to be achieved - rather than a checklist of what needs to be done. Each contributing outcome is associated with a set of indicators of good practice (IGPs). IGPs are used to develop sector-specific CAF profiles, which provide a view of appropriate and proportionate cyber security for those organisations.

12.1 Local Government Cyber Assessment Framework (LGCAF)

At the time of writing this strategy, DLUHC have not completed the work to publish the LGCAF which will have LA specific IGPs, this strategy has been written with the intention that the council will work towards compliance of the LGCAF once published. This will be achieved by following the advice of NCSC, DLUHC and the LGA in ensuring whenever possible best practice is followed for the 14 principles of the CAF.

There is a possibility that in the future the LGCAF will replace the PSN CoCo and/or the NHS DPST.

12.2 NHS Data Security and Protection Toolkit (DSPT)

The NHS DSPT is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security, and that personal information is handled correctly.

The council must comply with the toolkit to maintain out access to NHS systems. The council completes our submission annually.

12.3 Public Services Network (PSN) Code of Connection (CoCo)

The PSN is a network operated by several suppliers for government that provides a trusted, reliable, cost-effective solution to departments, agencies, local authorities, and other bodies that work in the public sector, which need to share information between themselves.

The PSN Coco outlines conditions that we need to meet and the information that we need to provide. This information is used to assess whether we may connect/continue to connect to PSN.

The Cabinet Office PSN team may also need to conduct an on-site assessment if they deem it necessary.

The council must comply with the PSN CoCo to maintain out access to the PSN systems. The council completes our submission annually.

13 Glossary / IWC Cyber Lexicon

Active Cyber Defence (ACD):
An NCSC programme which seeks to reduce the harm from commodity cyber-attacks, consisting of a number of interventions or services that help an organisation to find and fix vulnerabilities, manage incidents or automate the disruption of cyber-attacks. Some services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability.

Arm's-length bodies:
A commonly used term covering a wide range of public bodies, including non-ministerial departments, non-departmental public bodies, executive agencies and other bodies, such as public corporations.

Artificial Intelligence (AI):
A technology in which a computing system is coded to 'think for itself', adapting and operating autonomously. AI is increasingly used in more complex tasks, such as medical diagnosis, drug discovery, and predictive maintenance.

Automated asset management system
An automated asset management system is a software solution that helps the council to monitor and track both physical and digital assets. It can help to reduce costs, improve efficiency, enhance security, and ensure compliance.

Backup Frequency
Backup frequency is the term used to describe how often the council should back up data to prevent data loss in case of a disaster, failure, or disruption.

Blue teaming:
A team responsible for defending an organisation's information systems by maintaining its security posture against mock attackers (the Red Team).

CAF profile:
The articulation of required outcomes corresponding to the Cyber Assessment Framework that reflect an organisation's 'threat profile'.

Central government:
Central government comprises all the organisations that are controlled directly or indirectly by government ministers.

Critical National Infrastructure (CNI):
Those critical elements of infrastructure (namely assets, facilities, systems, networks

or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a. major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
b. significant impact on national security, national defence, or the functioning of the state.

Cryptography:
The science or study of analysing and deciphering codes and ciphers; cryptanalysis.

Cyber-attack:
Deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

Cyber Assessment Framework (CAF):
An assessment framework developed by the NCSC that provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

Cyber Essentials:
A Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

Cyber incident:
An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.

Cyber power:
Cyber power is the ability to protect and promote national interests in and through cyberspace.

Cyber resilience:
The ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite cyber security events.

Cyber risk:
The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.

Cyber security:
The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

Cyber security assurance:
The verification that systems and processes meet the specified security requirements and that processes to verify ongoing compliance are in place.

Cyber security controls:
The processes and tools an organisation have in place to detect, prevent, reduce or counteract security risks.

Cyber security data:
Any data that is relevant to cyber security, including data on cyber threats and vulnerabilities.

Cyber Security Programme:
The programme of work set up to implement the Cyber Security Strategy, and deliver against its strategic outcomes.

Cyber threat:
Anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

Domains:
A domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.

GBEST:
GBEST is an intelligence-led simulated attack framework developed and managed by the Cabinet Office. It is derived from the Bank of England’s CBEST framework but is focused on building the overall cyber resilience of government.

Government:
The organisations that operate and deliver the functions that run the UK, including central government departments, arms-length bodies, agencies, local authorities and other wider public sector organisations.

Government Cyber Adversary Simulation Exercise (GCASE):
GCASE is similar to GBEST provides although provides a less in-depth level of assurance, while being faster to deploy.

Government Cyber Coordination Centre (GCCC):
Proposed joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, bringing together their respective functions and areas of expertise to better coordinate operational cyber security efforts across government, transform how cyber security data and threat intelligence is used across government and truly enhance government’s ability to ‘defend as one’.

Government Security Centre for Cyber (Cyber GSeC):
Function that delivers a broad range of capabilities and services that support government organisations to improve their cyber security posture and achieve an appropriate level of cyber resilience.

Government Security Group:
The Cabinet Office unit responsible for the oversight, coordination, and delivery of protective security within all central government departments, their agencies and arms-length bodies.

Host Based Capability (HBC):
HBC is a software agent available to government departments for the OFFICIAL devices they use. This includes laptops, desktops and servers. The agent is installed on the devices and works in the background to collect technical metadata.

Incident management:
The management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response:
The activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Integrated Review:
Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy, describes the government’s vision for the UK’s role in the world over the next decade and the action government will take to 2025.

ISO 27001:
International Standards Organisation standard which covers requirements for an information security management system.

Legacy:
Systems, services or any components that are ineffectively maintained or supported by internal teams, contractors, suppliers or vendors.

Macro cyber posture:
An assessment of the overall cyber security resilience of the organisations under the purview of a lead government department.

Minimum Cyber Security Standards:
Minimum set of cyber security standards introduced in 2018 that government expects departments to adhere to and exceed wherever possible.

National Cyber Security Centre (NCSC):
The UK's technical authority for cyber threats, providing a unified national response to cyber incidents to minimise harm, helping with recovery and learning lessons for the future.

Network:
A collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Network and Information Systems regulations (NIS):
UK regulations that provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services

National Institute of Standards and Technology (NIST) Cyber Security Framework:
A set of guidelines published by the US National Institute of Standards and Technology for organisations to better manage and reduce cybersecurity risk, as well as foster risk and cybersecurity management communications.

Offensive cyber:
Adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect. Offensive cyber operations often exploit technical vulnerabilities, use systems or networks in ways that their owners and operators would not intend or condone, and may rely on deception or misrepresentation.

OFFICIAL:
The lowest level in the Government Security Classifications system, which defines the level of confidentiality needed to protect an asset, covering the majority of government work. The information held by the council is typically OFFICIAL or OFFICIAL-SENSITIVE

Operators of essential services:
Organisations within vital sectors which rely heavily on information networks, for example utilities, healthcare, transport, and digital infrastructure sectors as identified by the criteria in the Network and Information Systems (NIS) Regulations 2018.

Penetration testing:
Activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.

Public sector:
The portion of the economy composed of all levels of government and government-controlled enterprises.

Purple teaming:
A cyber security testing exercise in which a team takes on the role of both red and blue team.

Ransomware:
Malicious software that denies the user access to their files, computer or device until a ransom is paid.

Recovery Point Objective (RPO)
A recovery point objective is a measure of how much data a service can afford to lose in the event of a disaster, failure, or disruption. It is expressed as a time interval, such as minutes, hours, or days. The RPO determines how frequently the council needs to back up the data to ensure that it can be restored to an acceptable position in time after a recovery e.g. last night's backup etc.

Recovery Time Objective (RTO)
A recovery time objective is the maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or disruption takes place. The RTO defines the point in time after a failure or disaster at which not having the application, computer, network, or system back up and running becomes unacceptable. The RTO helps determine how quickly the council needs to restore its operations and services to avoid significant damage to the business and customers

Red teaming:
A penetration testing team which takes on an offensive role, attacking computer systems to explore the ways in which a genuine aggressor would carry out an attack.

Restore times
Restore times are the durations that it takes to recover a system, service, or data after a failure, disruption, or disaster.

Service level agreement (SLA)
A service level agreement (SLA) is an agreement that defines the expectations and responsibilities between a service provider and a customer. In the case of disaster recovery, ICT is the service provider and the service with the application, computer, network, or system down, is the customer.

Secure by Design:
The discipline of embedding cyber security into digital systems and services at every step of their lifecycle - from the planning of a service, to the procurement and configuration of technology and its decommissioning at the end of its operational life.

Secure configuration:
Security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.

Supply Chain Security Statement of Applicability questionnaire
The council's supply chain security statement of applicability questionnaire, is used to obtain a detailed statement from all vendors, specifying what cyber security safeguards they have in place for the protection of council information for the duration of contracts awarded.

Threat hunting:
Cyber threat hunting is the process of proactively searching across networks and endpoints to identify threats that evade security controls.

Threat model:
An engineering technique to identify threats, attacks, vulnerabilities, and countermeasures that could affect an IT system.

Threat profile:
An articulation of the threat to an organisation and its assets, which informs the designated CAF profile under government's proposed assurance process.

User:
A person, organisation entity, or automated process, that accesses a system, whether authorised or not.

Vulnerability:
Security flaws in software programs that have the potential to be exploited by attackers.

Vulnerability assessment systems
A vulnerability assessment system is a tool that helps to identify and prioritise

security weaknesses in the council's ICT infrastructure. It scans laptops, PCs, systems, networks, and applications, and reports the vulnerabilities that are found.

Vulnerability reporting service:
A mechanism through which an organisation can be alerted to security flaws before they are exploited by attackers.

14 APPENDIX A

14.1 SIRO and DPO Report

14.1.a Summary of data breaches (to include reportable to ICO and non reportable)

14.1.b Near miss data breaches

14.1.c SARs: volume and how many completed within 1 month timeframe compliance

14.1.d Access Controls: Leavers (access removed), movers (access updated), leavers (access removal), long term off work (maternity, sick leave- access suspended or restricted)

14.1.e FOI stats

14.1.f Training stats: must evidence 95% of the orgainisation is compliant against the signed off Training Needs Analysis

14.1.g Summary of DPIAs completed and any high risks identified

14.1.h Changes to Information Asset Registers (as reported by IAOs)

14.1.i Policies reviewed

14.1.j DSPT progress and outstanding actions

14.1.k Summary of audits which have Data Privacy implications

14.1.l Cyber report (any incidents/ attacks, patches, penetration testing)

14.1.m Business continuity/Disaster Recovery: any activities/issues

14.1.n Updated media statement for sign off and use in the event of a data breach

14.1.o 15. Data Processor update: any issues, contractual updates on compliance with GDPR

14.1.p 16. Data Destruction: IT kit, shredding – any issues