Isle of Wight Council

Isle of Wight Council CYBER SECURITY STRATEGY 2023 - 2030

19th December 2023 / Final v1.0

1 Document information

Title:	IWC Cyber Security Strategy 2023 - 2030
Status:	Final
Current version:	1.0
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
0.4	15th November 2023	For consultation – following Scrutiny Committee
1.0	19th December 2023	Final

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).

For these priorities to be successfully delivered, in an ever-changing landscape of cyber security threats   it is vital that the council has an appropriate approach to cyber security for the protection of all its information assets.

A key principle of the Digital Strategy is for all technological developments to be “Secure by design” (an approach that seeks to protect people and businesses from cyber-attack). This strategy will enhance how this principle can be achieved. Central to this strategy will be that:

- Whether it be the coding of our website or design of internal and external technology-based customer service systems, they must be secure by design.
- We will take a risk-based approach in meeting the identified business need and the information security and cyber security measures that are necessary to protect the council’s information assets.
- There will be a proportionate and multi-layered approach to cyber security measures put in place.

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 closely with the Local Government Association (LGA) and the Department for Levelling Up, Housing & Communities (DLUHC) Cyber teams, there is a need to have a clear strategy for continuous improvement with regards to cyber security. This is further 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 because of cyber-crime.

In conjunction with the NCSC, DLUHC and LGA cyber security teams the council has undertaken cyber security based technical enhancements over the last three years. The council continues to invest in systems and solutions that seek to reduce the potential number of possible points, where an unauthorized user can access a system and extract data from the organisation.

In early 2023, the council completed a cyber security culture review with its workforce. The results show that there are opportunities to secure greater awareness of the risks associated with cyber-crime and individual responsibilities for precaution and action that can bring about a robust cyber aware culture across our organisation and in our partnership arrangements with other organisations including those with suppliers.

In June 2023, the council also engaged with the LGA Cyber 360 programme to assist us in determining what strategic and practical action could be taken to further enhance the council’s approach to cyber security. The report and its recommendations, one of which was to establish a specific cyber security strategy have been incorporated into this document.

4 Approach

4.1 Vision and aim

It is our intention that this strategy will mirror the 2023 – 2030 UK government cyber security strategy which, adapted to reflect our local context is:

Vision: To ensure that the delivery of local government services on the Isle of Wight will be resilient to cyber-attack and which underpins the strengthening of the UK as a sovereign nation, cementing its authority as a democratic and responsible cyber power

Aim: For the Isle of Wight Council to meet the central government target to be significantly hardened to cyber-attack by 2025 and being resilient to known vulnerabilities and attack methods no later than 2030.

4.2 Strategy Approach

To focus resources, manage risk and achieve our stated vision and aim, the council is basing its Cyber Security strategy on the framework established by the central government which comprises of two strategic pillars for action and complemented by five underpinning objectives. Although these are set by government at a national level, they are still applicable to the council and its cyber security arrangements at a local level and serve to develop a common language with regards to cyber security.

Strategic Pillars:

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

4.2.b To 'Defend as one;' we 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

The five underpinning objectives of the central government's cyber security strategy set out what must be considered by public bodies' in securing cyber resilience. This strategy will map out the Isle of Wight council's approach to each of these objectives.

4.3.a Manage cyber security risk:
To establish effective cyber security risk management processes, governance and accountability that enables the identification, assessment, and management of cyber security risks.

4.3.b Protect against cyberattack:
Adopting proportionate security measures informed by understanding risk and mitigating risks where feasible through centrally developed security measures that give protection at scale.

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

4.3.d Minimise the impact of cyber security incidents:
Ensuring that 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: Investing in the development of skilled, and knowledgeable professionals capable of fulfilling all required cyber security needs together with a strong workplace cyber security aware culture that secures organisational ownership in driving down the risk of cyber related crime.

5 Objective 1 - Managing Cyber Risk

The basic principle of this strategy is the management of risk. The risk of cyber-attack can never be fully eradicated, but appropriately focussed risk identification, mitigation activity and management afford the best possible opportunity to minimise the risk and impact.

For effective risk management to take place, it is vital that the council understands the digital assets held, where they are located and how they are processed. Appropriate governance structures and systems with clear accountability assigned to individuals will enable the council to plan its mitigation activities and monitor progress against them.

5.1 Governance and accountability

Cyber risk is an integral part of our risk management processes. Current strategic level risks included on the corporate risk register with associated mitigating actions are:

- Maintaining compliance with the Public Services Network Code of Connection (PSN CoCo) (necessary to transfer information between local authorities and central government and other public bodies)
- Risk of Cyberattack
- Loss of ability to process card payments due to lack of Payment Card Industry Data Security Standard (PCI-DSS) compliance.

An additional strategic risk of cyber security culture will be added to develop organisational awareness and ownership of the action required to minimise attack. These risks are managed in accordance with the council’s risk management policy and are regularly reviewed by the council’s corporate management team and through the cabinet’s quarterly performance report. The Audit and Governance committee under its terms of reference also affords oversight of the effectiveness of the council’s arrangements for risk management.

In addition, the Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO) submits an annual report to senior managers who form the Corporate

Management Team (CMT) and Corporate Leadership Team (CLT) which comprises of senior managers and cabinet members. The report content is provided in Appendix A.

Each service of the council is also required to identify service specific cyber security risks, including potential operational business process failures, upskilling and awareness raising of staff. These are to be recorded on the council's risk management system and regularly reviewed at directorate management team meetings alongside other risk management discussions.

5.1.a Identified roles and responsibilities:

There are several key roles assigned to cyber security, designed to help protect our information assets from various threats. These are:

- Data Protection Officer (DPO) (the person responsible for monitoring and advising on the council's compliance with data protection legislation) and nominated deputy DPO's.
- Senior Information Risk Owner (SIRO) (the person responsible for managing and overseeing organisational information asset risks) and nominated deputy SIRO.
- Caldicott Guardian (the person responsible for protecting the confidentiality of people's health and care information).
- Information Asset Owners (IAO); (these are nominated senior officers who are responsible for providing assurance to the SIRO on the security and use of business information assets in each of the council's service areas).
- Information Governance Lead (IGL); (these are nominated staff responsible for dealing with information governance and compliance matters within each service).
- Information Asset Administrators (IAA); (these are nominated staff who provide support to the IGL in making sure that information governance policies and procedures are followed)

The SIRO will maintain a section on the council's Intranet that provides information about the staff members who currently hold these roles, and their responsibilities for Information Security and Cyber Security.

5.1.b Governance meetings

There is an Internal Information Governance Group (IIGG) (chaired by the DPO) and Information Security Group (ISG) (chaired by the SIRO) who meet bi-monthly to oversee, monitor organisational practices, and compliance with corporate and legislative requirements. The SIRO will maintain a section on the council's intranet for these operational groups and their associated terms of reference.

5.1.c Governance reporting

- The DPO and SIRO will prepare an annual information governance and cyber security update report for senior managers and cabinet members. 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 will be presented alongside the annual budget setting process to ensure that the risk reduction measures are appropriately planned for and integrated into the council's budget.
- Cyber security will be a regular item on the agenda of directorate management team meetings and/or service boards.
- The Caldicot Guardian will report any concerns or issues to the corporate management team and cabinet as necessary on an on-going basis.

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 central repository of cyber security risks within the council. This will enable a co-ordinated approach to risk analysis to be undertaken with comprehensive remedial action plans created.

The SIRO will be responsible for proactive measures to detect vulnerabilities, prioritisation of available resources to remediation of those determined to be substantial risk and ensuring that ICT technical teams are capable of rapid assessment, management and resolution of threats.

To ensure that it has information about critical vulnerabilities that is 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 engage 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 ICT department will on behalf of the council, will maintain an ISO27001 conformant Information Security Management System (ISMS).

The production of Information Asset Registers (IAR’s) is a mechanism for understanding what information assets the organisation has and the risks associated with them. They ensure that risks can be adequately assessed for each data asset; that sufficient protections are put in place, proportionate to the sensitivity of the data and is capable of providing assurance of compliance with data protection legislation. The Corporate Information unit maintains a central record of all completed IARs so that there is a comprehensive record of all data assets.

The council will maintain compliance with the Payment Card Industry Data Security Standard (PCI-DSS) incorporating any additional change requirements to the standard over time.

5.4 Supply Chain Risk

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

Cyber security risks associated with supply chains 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.

Through improved understanding by all services of their supply chains and the points of potential vulnerability in them, mitigating actions can be established and embedded into contractual controls with suppliers and/or their subcontractors. This will support the reduction of identified risks.

The procurement team will incorporate 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 a service or by ICT, has a common approach to the assessment of cyber security risks and their management at the time of tendering.

Where appropriate, Invitation to Tender documents will incorporate the councils Supply Chain Security Statement of Applicability questionnaire to make assessment of cyber security management a key element of contract provision and monitoring. Assessment of need will be undertaken in conjunction with the procurement and ICT information security teams. The council’s services regularly utilise government frameworks for the procurement of goods and services. Central government has made a commitment to ensuring that commercial arrangements are risk based with robust clauses for cyber security management. This will aid the council in delivery of this supply chain risk reduction process.

5.5 Threat information

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 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 (NCSC)
- Local Government Digital Cyber team
- Local Government Association (LGA) Cyber team

The council's information security manager will actively engage with the Government Cyber Co-ordination Centre (GCCC), designed to share cyber security data across government to ensure that the council has access to relevant information upon which to act.

5.7 Government cyber security measures

The council will maintain and prioritise compliance with the latest central government codes of practice, including the Public Services Network Code of Connection (PSN CoCo) and anticipated future Local Government Cyber Assessment Framework (CAF) and NHS Data Security and Protection Toolkit (NHSDSPT).

The PSN CoCo requires the council to conduct regular (at least annually) penetration tests. These tests will be supported by the implementation of real world testing and exercises. These exercises will not just be managed by ICT teams but will be undertaken in conjunction with services. The focus of these activities is to provide confidence that the cyber security risks are being managed sufficiently by all stakeholders.

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, service managers and all staff in risk mitigation activities will ensure that our risk of attack is greatly reduced.

6.1 Secure technology and digital services

The council uses a range of technology solutions to deliver its services. These are a mixture of both in house created systems as well as off the shelf purchase solutions. All can present opportunities for cyber criminals to attack. To minimise this risk, there is an expectation that any system will have been developed in accordance with the 'secure by design' framework published by UK government.

The continued use of older systems, (known as legacy systems) which may not have the same level of robustness in design security, poses an increased vulnerability risk against attack. The SIRO will ensure that the ICT service in conjunction with the service system owners, 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.

An essential element of cyber security is to ensure that any system software updates are completed (known as patch management) to protect against identified vulnerabilities. On an annual basis, the SIRO will review roles and responsibilities for the delivery of patch management ensuring appropriate support and patching activities are taking place for all hardware and software systems.

Where contracts and system administration are managed outside of the ICT service, the SIRO will also ensure there is clear visibility on the security status of the system. All contracts for purchased systems 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 internal 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 SIRO on behalf of the council will deploy cyber security controls that are proportionate to the risk profile of potential compromise for all ICT systems. The SIRO will continue to work with the LGA, and DLUHC cyber teams and SEGWARP so that there is robust risk assessment information available to afford a relevant profile of potential threats to be established for decision making purposes. This will enable the resulting recommended 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 system 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 system access controls provided are required and used appropriately to limit the attack surface to cybercriminals.

The practice of cloning user account rights of access to systems (which means an identical copy of rights assigned to one person is replicated to another) will be replaced by a Role Based Access Control (RBAC) model which will be determined by the access rights required of categories of job role. Using this new approach will reduce the risk of account compromise. Categorisation of rights of access will be recorded in the council’s Identity and Privilege Access policy framework.

The council will use Active Directory Federated Services (ADFS) (a system that allows digital identity and access rights to be shared securely across systems) to make provision for Single Sign On (SSO) (the ability to have one log-in for more than one system required for access) with Multi-Factor Authentication (MFA) (a process that requires a number of steps to be taken to log-in to a system) adopted where the risk assessment indicates it is a necessity to reduce vulnerability to cyber-attack.

6.3 Secure Configuration

The ICT Service on behalf of the council will establish and maintain an appropriate architecture configuration (a map of how systems connect and interact with each other) for all digital systems in operation. This will also allow for standard profiles to be put in place for common systems in use.

The SIRO will ensure that the policies relating to secure configuration are reviewed and updated on an annual basis, reported and approved through the Information Security Group. This, together with the adoption of the government's secure by design principles will afford greater assurance on inherent ICT security risks. There is an expectation that these standards will be adhered to by everyone.

6.4 Shared capabilities

The ICT service will, wherever possible, share with others who may benefit from knowledge of the common aspects of our system architecture to secure wider system protection across local government and partner organisations, including our suppliers.

Equally, through the use of security tools provided by central government; active engagement with cyber security experts such as the NCSC, LGA, participation in SEGWARP information sharing group it will be possible to work collectively and proactively on specialist and/or distinct threats and other emerging attack threats.

The ICT service will develop policy and procedures for the management of system access and provide relevant training in their use.

6.5 Information and Data Security

The council has a responsibility to make provision for all data held by the organisation to be appropriately protected. This is fulfilled through the provision of system back-up and restore technologies and operational processes that support them.

The ICT service in conjunction with each service system owner will determine and agree a service level agreement (SLA) on how these arrangements are to be managed effectively. SLAs will be informed by recovery point objectives (RPO) (the maximum amount of acceptable data loss within a given period of time) and recovery time objectives (RTO) (the maximum amount of acceptable time a system can be inoperable) both of which may occur as a result of system failure due an unexpected event or planned maintenance.

Each service must produce and maintain a business continuity plan (BCP) in conjunction with the council's emergency management team which details (amongst other factors) the operational plans that will be put in place should there be system failure. It is the responsibility of each service manager to ensure that staff fully understand and are adequately training in enacting these plans.

The corporate information unit (CIU) will maintain a Protective Marking Policy. This policy will assist everyone in understanding the requirements for the classification, handling, sharing, storage and processing of data. This will be reviewed every two years to ensure that it remains up to date with national guidance.

The ICT Service will be required to regularly review the data retention capabilities of its internally developed systems and develop a remediation plan to rectify any issues that emerge. 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 stored on document shares 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, there are inherent and unknown vulnerabilities within ICT systems which means that cyber-attacks will still occur. The ICT service on behalf of the council will operate comprehensive vulnerability tools and processes to assist in the identification and prioritisation of emerging risks that will lead to the effective management of them.

7.1 Detection within the Council

The councils' networks, systems, applications, and all end points (physical devices that connect to a network such as a laptop or CCTV cameras) will be constantly monitored by proportionate and appropriate detection and protection capabilities. These systems will generate and provide data reports to assist in the detection of Cyber threats.

Threat detection monitoring will be undertaken by the use of multiple technical solutions that allow for different views of the threat landscape to be to be scanned. 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 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 ICT service on behalf of the council will ensure that all appropriate information regarding cyber incidents is shared with partner organisations in a timely and appropriate manner. Partners will be informed of the council's 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 capability and process plans in place to deal with incidents whenever they happen. It is also incumbent upon us to work collaboratively with partner organisations that may be affected by an incident to ensure that they also have adequate plans and processes in place to respond.

8.1 Response preparation

The council has a Cyber Incident Response Plan (CIRP). This plan has been fully tested operationally and will be reviewed on an annual basis to ensure that it is kept up to date and reflects lessons learned from incidents, unless there is an urgent need for remedial updates to be made.

The ICT service in conjunction with services and the Emergency management team will complete at least one tabletop exercise for this plan each year as a means to test its practical operability. Scenarios used for this purpose will combine a cyber incident with a non-cyber incident to demonstrate the complexity of data security incidents.

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

The council has a Partner Cyber Incident Response Procedure (PCIRP) and through the Local Resilience Forum (LRF) (a multi-agency public service partnership), the Emergency Management team will instigate 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 staff in the handling of data breaches. It must be kept up to date to ensure it provides clear guidance on process and when it is necessary to engage with the CIU team.

8.2 Incident response

The council has a Cyber Security team. This team is there to provide capacity and expertise in the triage of cyber security incidents, assessment of their impacts and prioritise appropriate response activities.

The team are responsible for the creation and management of the playbooks (a term used to describe a set of guides that are to be operated when an incident occurs) for the commonly known threats the council face. These playbooks provide the necessary guidance to ICT staff in other teams as well as staff and councillors when required.

The Cyber Security team will maintain connections with external experts such as the NCSC, DLUHC and LGA cyber teams during incident management 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 are set out in the ICT Disaster Recovery Plan (DRP) and informed by individual service level agreements. The disaster recovery plan is refreshed on an annual basis to ensure it remains up to date. Strategic directors are responsible for ensuring that their recovery objectives are kept up to date within service level agreements.

8.3 Incident Recovery

Following the closure of an incident response, the Cyber Incident Response Team Incident Manager will meet with associated ICT staff and affected customers, to ensure that recovery is completed and that any lessons learnt during the incident are then recorded and policies and procedures duly updated.

It is critical that recovery activities includes a review of the identified risks to make sure that any that remain outstanding have appropriate and proportionate mitigating actions in place.

8.4 Lessons Identified

The Emergency Management team in conjunction with the services and the cyber security response team will capture, record and disseminate to the corporate management team, directors and service managers, the experiences and lessons learned. This will allow for increased knowledge for the effective handling of any future incidents. The preparation of any such reports must only focus on what can be done to improve and further develop prevention, detection and resilience in cyber security management.

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

The council has a wide range of ICT systems that are used by staff and councillors in the course of conducting the business of the Isle of Wight Council and in the delivery of services. Cyber security is therefore the responsibility of everyone within the organisation.

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 everyone but also recognise the specific needs of ICT technical staff, those involved in creating corporate policy and strategy those who are responsible for operating risk management processes, and those with leadership and management responsibilities.

9.1 Skill requirements

The Information Security Manager will ensure that the council has an appropriate suite of learning activities in place that meet the diverse needs of staff groups and councillors. These learning activities will be reviewed on an annual basis to ensure that they remain relevant and up to date. Guidance from expert partner organisations such as NCSC. LGA, DLUHC and SEGWARP will be sought on the breadth and depth of the training that would be appropriate for all audiences identified. There will be an expectation that the cyber security team undertake specialist training relevant to their role to ensure they have the technical knowledge and expertise to respond to and manage cyber security effectively.

When the UK Cyber Security Council has appropriate advice and guidance and any standards applicable to Local Authorities the Information Security Manager 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 to upskill other key information security roles across the council.

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 Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) qualifications.

9.4 Cyber security knowledge across the council

The need for cyber security knowledge is a responsibility of everyone. Whilst the degree of knowledge and expertise needed will vary, it is expected that everyone engage with the required learning activities that are relevant to their role and to proactively seek to keep up to date on cyber security matters.

The ICT cyber security team will engage with partner organisations to further develop programmes of learning and opportunities for practical desktop exercises that will enhance the development of knowledge and skills.

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, all of which contribute to the collective responsibility and ownership of cyber defence.

Staff will be encouraged to promote a pro-active philosophy of open and honest information sharing around practices and risk. The cyber security team will actively seek to engage with services to assist in the development of knowledge and expertise and how information sharing, discussion and other activities can be undertaken in team meetings and other forums that can contribute to a cyber aware culture.

Regular corporate channels for communication will also be utilised for the sharing of information together with tips and hints of how this can be effectively disseminated and shared.

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

There is an ever-changing landscape in cyber-attacks with increasing complexity in the nature of cyber security vulnerabilities. This combined with a continuous evolution of cyber-attack tactics, techniques and procedures used by cybercriminals the process for accounting of known vulnerabilities is difficult.

The expected local government Local Government Cyber Assessment Framework (CAF) profile will assist the council in determining its cyber resilience measures. By utilising a combination of penetration testing and desktop exercises, both internally and with partner organisations, we will annually review and update our policies, processes, ICT systems and playbooks.

This strategy sets out ambitious aims for a council that has pressure on its resources. 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 in the delivery of key actions set out in this strategy together with the achievement of annual accreditation against current standards, (PSN and NHS-DSPT) and in the future against the CAF will provide an annual statement of achievement against the 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 nature of the information we hold require periodic review. The ICT service will review their risk logs against the current CAF profiles on a quarterly basis and ensure that on an annual basis changes are incorporated into our local CAF profile assessment systems.

10.3 Key Performance Indicators (KPIs)

To ensure that the council has a complete picture of the progression in delivering against this strategy and its aims. To reflect the needs of the strategy and any given time, the KPI's will be developed and adapted 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. Embracing the CAF, its philosophy and principles and measuring the council against the national profile published for local authorities.
2. Building organisational ownership of cyber security risk management.
3. Build a proactive partnership cyber response network for the council to ensure greater protection through strong collaboration.

11.2 Implementation Plan

The SIRO will maintain a Cyber Security strategy action plan, this plan will be used as the basis for monitoring the delivery of this strategy.

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 our 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 severe 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 organisation 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