

West Suffolk Council Cyber Security Strategy 2026 to 2028

Defending our digital services, protecting our data

This version published: April 2026

Next review date: January 2028

www.westsuffolk.gov.uk

Email: cyber.security@westsuffolk.gov.uk

Telephone: 01284 767007

West Suffolk House, Western Way, Bury St Edmunds, Suffolk, IP33 3YU

Contents

Foreword	1
Overview	2
Vision.....	2
Current context and threat landscape.....	3
Statistics	4
Threats	4
Vulnerabilities.....	5
Risk management	5
Implementation	6
Objectives.....	6
Principles.....	6
Goals and actions.....	7
Measuring success	12
Appendix: Roles and responsibilities.....	14
Glossary	15

Foreword

Digital systems have become critical to the delivery of council services to local residents and businesses. As public bodies, local councils have increasingly been the target of high-profile cyber-attacks, many of which have left systems offline for months, cost millions to recover from and adversely impacted residents. The council's cyber security strategy's primary objective is to ensure the smooth and uninterrupted delivery of our services while keeping customer data safe and secure.

West Suffolk Council has always taken a proactive approach to cyber security, meeting or exceeding government best practice and standards. This strategy seeks to build on our approach, delivering modern and effective cyber security controls that support the continued adoption of new technology to benefit all our stakeholders.

Overview

This document lays out West Suffolk Council's high-level approach to cyber security until March 2028, with an expectation that its successor council will want to adopt the same or a similar approach but will need to review this as the new council comes into being. The aim is to keep pace with cyber threats that are increasing in volume and sophistication. The strategy aims to align with the Ministry for Housing, Communities and Local Government's (MHCLG) Cyber Assessment Framework (CAF) for local government and, most importantly, protect us from real world threats. The cyber security strategy provides appropriate controls to protect personal data as required under the General Data Protection Regulation (GDPR).

The purpose of cyber security is to ensure the confidentiality, integrity and availability (CIA) of the data stored within our digital systems. This model is called the CIA triad. The following details how cyber-attacks can compromise these properties.

- **Confidentiality** – a cyber-attack where organisational data are accessed by an unauthorised third party. Almost all types of cyber-attack compromise confidentiality. In the most severe cases, a ransom is requested to avoid stolen data being published online.
- **Integrity** – a cyber-attack could manipulate financial data such as payment details, leading to a financial loss and trust in data sets that have been accessed and potentially modified.
- **Availability** – a distributed denial of service (DDoS) attack could take our public-facing digital systems, such as our website, offline.

With more and more customer data being processed, and the expectation from residents that they can transact digitally with the council, it is more important than ever that our cyber security processes are both comprehensive and robust.

A successful cyber-attack against a council would have devastating effects on the most vulnerable people we serve and erode public trust in using our digital services.

Cyber security is inherently technical. This document aims to provide a clear overview. It does, however, include various terms specific to cyber security. We have, therefore, created a comprehensive glossary at the end of the document to explain these terms.

Vision

Our high-level vision is to minimise both the likelihood and impact of any cyber-attack that targets the council and, in doing so, protect our customer data and availability of our services. Management of risk is the core principle of our approach to cyber security.

- **Minimising our attack surface** – we aim to achieve this by minimising the different technology products and suppliers we use and adopting a secure-by-default or zero trust methodology for any new technologies, limiting access and functionality to business need.
- **Identification of threats and vulnerabilities** – for the attack surface that remains, we adopt a proactive and comprehensive approach to threat hunting and vulnerability discovery, increasingly focusing on real world threats that fall out of scope of traditional compliance-led security testing. This includes both

technical vulnerabilities and those relating to process that could allow exploitation using social engineering of our people.

- **Remediation of risk** – where risks posed by threats and vulnerabilities are identified, we prioritise, track and resolve. We do this through patching, configuration hardening and encouraging a positive cyber security culture that promotes early reporting of suspicious activity.

This strategy builds on our established practical approach to cyber, providing a secure infrastructure that can deliver current and future digital systems in a safe and secure way.

In line with the Cyber Assessment Framework (CAF), the strategy highlights the need for understanding and ownership of cyber security risk within the council's Leadership Team (board) and wider organisation. Cyber security is no longer something an IT team can deliver alone, specifically with an increasing number of our line of business systems provided as Software as a Service (SaaS) solutions, entirely managed within the software vendor's cloud infrastructure.

The strategy is informed by lessons learnt from cyber-attacks on both the public and private sectors which have increased year on year, as well as learning from our own simulated attacks.

This strategy is supported by the [West Suffolk Council – West Suffolk Council Information Security Policy](#) and our compliance with the National Cyber Security Centre's (NCSC) Cyber Essentials: Requirements for IT infrastructure v3.2.

The council has already completed the MHCLG's 'Get CAF ready' scheme and its third-party assessment of our work against CAF objectives A and D. The council aims to complete assurance of the final CAF objectives B and C with MHCLG in 2026.

Current context and threat landscape

Recent years have seen an increase in significant cyber incidents, with NCSC's Annual Review 2025 citing 'highly significant incidents' increasing by 50 per cent in the past year – the third successive year that has seen an increase. Attacks on local government have proved both costly and disruptive to councils and the communities they serve.

The NCSC's annual review also states the importance of preparing for the impact of a successful attack, highlighting the need for leaders to have plans in place and regularly conduct business continuity exercises to rehearse the response to a successful cyber-attack. The following sections provide key statistics on how the threat levels are increasing and describes common cyber threat and vulnerability types.

- Criminal ransomware gangs have splintered into smaller, less coherent groups, making it harder for law enforcement. Forthcoming legislation is expected to introduce a ban on the payment of ransoms across the public sector. Advances in technology must be assessed at speed, and risks captured and addressed, to ensure the council can realise the benefits of new and emerging technologies in a safe and secure way. For example, recent breakthroughs within the field of quantum computing highlight the need to implement Post Quantum Cryptography (PQC) as it is made available by technology suppliers. Artificial intelligence (AI) has the potential to deliver increased efficiencies for the council

as it matures, but is already being used to increase the scale and sophistication of attacks, as well as containing new vulnerabilities to be exploited. Increasingly, operational technology (OT) such as building management systems and environmental sensors are all Internet-connected and require protection and segmentation from the wider council IT environment.

- Finally, with an industry-wide shift to Software as a Service (SaaS) provided via the software vendors cloud, the need for expanded third party and supply chain risk management is vital. This should include standards for assessing and securing how these systems interconnect via application programming interfaces (APIs).

Statistics

Increase in the number of highly significant cyber-attacks	Increased by 50 per cent in 2025. (Source: NCSC annual report)
Cost of cyber-attacks	"The average cost of a significant cyber-attack for an individual business in the UK is estimated in this study to be £194,729." "the modelling estimates a total cost to businesses at the UK economy level of £14.7 billion." "representing 0.5 per cent of the UK's annual Gross Domestic Product (GDP)." (Source: GOV.UK – KPMG economic modelling)
Decreasing time to exploit unpatched systems	The average time to exploit unpatched vulnerabilities has reduced to five days, down from 32 days in 2022. This highlights an ever-decreasing window for critical updates and fixes to be installed. (Source: Mandiant)
Phishing	90 per cent of cyber-attacks start with phishing. (Source: Microsoft)
Increase in identity-based attacks	In the past year, voice impersonation attacks rose by 442 per cent. Many of the most serious incidents started with threat actors calling service desks and impersonating staff or contractors asking for password resets. (Source: CrowdStrike)

Threats

Threat actors are malicious groups who target vulnerabilities in our systems, processes and people. These are categorised based on motivation below.

Organised crime	Criminal gangs motivated by financial gain.
-----------------	---

Hostile nation states	These groups target critical national infrastructure, public bodies and key sectors of the economy with the aim of destabilising the UK.
Politically motivated (Hacktivists)	These groups target sectors for a specific political cause – for example, anti-war or anti oil protest groups.
Insider threat	Insider threats can be malicious individuals who have infiltrated the organisation, or those who inadvertently disclose information.

All threat actors use a range of tactic techniques and procedures (TTP) to achieve their aims. As shown in the statistics section, they have increasingly opted to use social engineering techniques such as phishing emails and impersonating staff and suppliers when calling IT Service desks for password and multi factor authentication (MFA) resets. These techniques in particular have been magnified with the adoption of AI powered video and audio deep fakes.

We monitor threats through analysis of indicators of compromise (IOCs), which are static values seen in attacks by threat actors. These could be the IP addresses the attack comes from, web addresses that malware communicates with or identifiers of malicious files they deploy. In addition, we monitor anomalous behaviour based on known techniques, tactics and procedures (TTP)

Vulnerabilities

Vulnerabilities are weaknesses in our digital systems or supporting processes that threat actors can exploit. Vulnerabilities fall into many categories.

Poor system setup and configuration	Systems that are not installed or configured correctly in line with manufacturer guidance – for example, with excessive access, default passwords or unneeded components.
Missing updates	Critical updates that are not installed in a timely manner or legacy software where the manufacturer no longer provides updates.
Lack of training and skills	Staff who have not received appropriate awareness training, or where processes that staff follow are not robust enough.

Risk management

The council manages the cyber risks posed by threat actors and vulnerabilities across three levels as shown within the table below.

Strategic	At a strategic level, cyber risk is highlighted on the council's corporate risk register.
Operational	The council has a cyber risk register which is maintained by the council's Cyber Security Manager and reviewed by the council's Information Governance Working Group (IGWG) on a quarterly basis.
Technical	Technical cyber risk is managed on a day-to-day basis by the council's Cyber Security Manager, through analysis of vulnerability scans, threat intelligence and simulated attacks.

The council has achieved and maintained the following cyber security accreditations, which provide third party assurance on our cyber security practices:

- Public Services Network (PSN) – held since 2010
- NCSC Cyber Essential Plus (CE+) – held since 2018
- NHS Data Security and Protection Toolkit – held since 2020.

Implementation

Objectives

This strategy is broken down into four categories which are mapped to the Cyber Assessment Framework (CAF) objectives as follows.

Identify	Links to CAF objective A
Protect	Links to CAF objective B
Detect	Links to CAF objective C
Respond and recover	Links to CAF objective D

Principles



- A. Managing security risk
Principles:
 - A1. Governance
 - A2. Risk management
 - A3. Asset management
 - A4. Supply chain
- B. Protecting against cyber attack
Principles:
 - B1. Service protection policies and procedures
 - B2. Identify and access control
 - B3. Data security
 - B4. System security
 - B5. Resilient networks and systems
 - B6. Staff awareness and training
- C. Detecting cyber security events
Principles:
 - C1. Security monitoring
 - C3. Threat hunting which replaces proactive security even discovery
- D. Minimising the impact of incidents
Principles:
 - D1. Response and recovery planning
 - D2. Lessons learned

These principles are common across many cyber security frameworks such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0).

Goals and actions

a. Identify

Goal: Identify governance structures and risk management processes.
Identify physical assets, data, apps, suppliers, threats and vulnerabilities.

Action	Responsible	Timeframe
Ensure cyber security risks are identified, captured on a cyber security risk register and discussed at Information Governance Working Group (IGWG) meetings.	IT Infrastructure and Cyber Security Manager	Ongoing (quarterly)
Provide regular briefings to the council's Leadership Team on cyber security, to ensure they can make effective decisions in the event of major incidents.	IT Infrastructure and Cyber Security Manager	Ongoing (six- to 12-monthly)
Ensure cyber roles are identified and understood.	Information Governance Working Group	Ongoing
Identify the council's risk appetite as defined in the government's 'orange book'.	Information Governance Working Group	Initial identification Quarter 3 2026, then ongoing

Action	Responsible	Timeframe
Conduct regular network and vulnerability scans of the council's internal network to identify new devices on the network and associated risk levels.	IT Infrastructure and Cyber Security Manager	Ongoing (weekly)
Conduct regular real world attack simulations against the council's IT systems and processes. These will be run by an accredited third-party Red Team provider and linked closely to real world threats.	IT Infrastructure and Cyber Security Manager	Ongoing (six per year)
Identify users and appropriate cyber security training based on their job roles.	Information Governance Working Group	Ongoing
Ensure physical devices (servers, laptops) are subject to appropriate asset management throughout the lifecycle from initial purchase to secure disposal of data they contain.	IT Infrastructure and Cyber Security Manager	Ongoing (monthly audit)
Identify 'shadow IT' apps that contain West Suffolk Council organisational or customer data. These are apps not sourced through the council's IT service or programme.	IT Infrastructure and Cyber Security Manager Service Manager, Change and Digital	Ongoing
Identify and assess third party providers in the council's supply chain. Ensure they are assessed at contract award and periodically throughout the term of the contract.	IT Infrastructure and Cyber Security Manager Service Manager, Change and Digital	Ongoing (process review six-monthly)
Adhere to vendor support lifecycles, ensuring legacy technology (technology for which the vendor no longer provides security updates) is not run.	IT Infrastructure and Cyber Security Manager	Ongoing
Create a third-party risk register of suppliers who are critical for the delivery of council services.	IT Infrastructure and Cyber Security Manager	Quarter 4 2026
Ensure vendors provide a Software Bill of Materials (SBOM) for systems identified a critical system under the Cyber Assessment Framework (CAF).	IT Infrastructure and Cyber Security Manager Service Manager, Change and Digital	Added to vendor questions Quarter 2 2026, then ongoing collection

b. Protect

Goal: Protect our systems, data and user identities through appropriate controls – for example, through technical restrictions, policies and appropriate training and processes.

Action	Responsible	Timeframe
Protect data stored in cloud systems through strong identity and access management (IAM), including single sign on (SSO) using the council's centrally	IT Infrastructure and Cyber Security Manager	Ongoing (passkeys available in

Action	Responsible	Timeframe
managed identity provider or phishing resistant MFA such as device bound passkeys.		Microsoft 365 Quarter 2 2026)
Enforce identity-based micro segmentation across the cloud and internal network, building on strong network access control (NAC) already in place.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure all users have modern MFA enabled on their accounts, such as authenticator apps, rather than one-time codes sent by email or text message.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure privileged users (those with IT admin rights) are subject to stronger controls, MFA, limits on which devices can be used and greater logging and alerting on the use of these accounts.	IT Infrastructure and Cyber Security Manager	Ongoing
Continue to provide robust perimeter protection on the council's network through firewalls and intrusion prevention systems.	IT Infrastructure and Cyber Security Manager	Ongoing
Replace all technology before its end of support date when critical security patches are no longer available.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure reliable and resilient Internet connectivity to protect against distributed denial of service (DDoS) attacks.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure all staff and elected members undergo annual cyber security awareness training appropriate to their roles.	Information Governance Working Group	Ongoing
Ensure all staff and elected members are aware of cyber risks as part of the induction programme.	IT Infrastructure and Cyber Security Manager Monitoring Officer	Ongoing
Maintain regular programme of cyber security information articles on the staff and councillor intranet.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure IT processes are robust and regularly tested by an external Red Team for resistance to social engineering attacks.	IT Infrastructure and Cyber Security Manager	Ongoing
Maintain NCSC Cyber Essentials Plus accreditation.	IT Infrastructure and Cyber Security Manager	Ongoing (annual audit)
Ensure the council has a comprehensive Information Security Policy that is regularly updated to reflect changing technologies and threats.	Information Governance Working Group	Ongoing (reviewed and agreed annually)
Ensure processes are in place to onboard and offboard new users in a secure way, with staff identity checked by HR team before IT officers set up accounts.	IT Infrastructure and Cyber Security Manager HR and Payroll	Ongoing

Action	Responsible	Timeframe
Ensure appropriate patching policies are in place and reflect current threat levels, specifically the decreasing mean time to exploit.	IT Infrastructure and Cyber Security Manager	Ongoing
Encrypt data at rest and in transit to the latest government and manufacturer standards. Specifically, ensure our systems are using quantum resistant encryption within the next three years, as it is launched by vendors such as Microsoft in the latest releases of their products.	IT Infrastructure and Cyber Security Manager	Ongoing
Adopt a secure by design approach. All systems implemented should be well understood by IT and configured in line with manufacturer and government guidance.	IT Infrastructure and Cyber Security Manager	Ongoing
Segmentation between systems should be in place wherever practical to limit lateral movement and escalation by threat actors.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure backups are air gapped from the main network and at least three copies exist, with at least one copy being immutable.	IT Infrastructure and Cyber Security Manager	Ongoing
Create a standard for secure application programming interface (API) configuration required by our suppliers of cloud-based systems, including strong certificate-based authentication and appropriate encryption.	IT Infrastructure and Cyber Security Manager Service Manager, Change and Digital	Added to vendor questions Quarter 2 2026, then ongoing collection

c. Defend

Goal: Ensure appropriate security monitoring and proactive threat hunting in line with current threat levels.

Action	Responsible	Timeframe
Continuously monitor logs for indicators of compromise (IOCs). These are static indicators of threat actors targeting our systems and include their IP addresses, website address and file signatures.	IT Infrastructure and Cyber Security Manager	Ongoing (daily)
Consume and share threat intelligence with the Local Government Warning Advice and Reporting Points (WARPs).	IT Infrastructure and Cyber Security Manager	Ongoing
Proactively hunt for tactics, techniques and procedures (TTPs). Unlike static matching for threats known to have attacked other organisations, these show behaviours seen in other attacks. The council will search for known TPPs.	IT Infrastructure and Cyber Security Manager	Ongoing (daily)

Action	Responsible	Timeframe
Ensure logs are collated centrally within a security information and event management (SIEM) and are immutable.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure alerts are tuned to minimise false positives and reviewed in close to real time.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure logs identify activity throughout the lifecycle of an attack by conducting regular simulations and correlating Red Team activity to alerts.	IT Infrastructure and Cyber Security Manager	Ongoing
Ensure automated response capabilities within our environment are enabled, configured and tested, utilising AI where appropriate to respond at machine speed.	IT Infrastructure and Cyber Security Manager	Ongoing
Review augmenting current automations and staff with managed detection and response (MDR) services.	IT Infrastructure and Cyber Security Manager	Initial review Quarter 4 2026, then ongoing

d. Respond and recover

Goal: Respond to security events and incidents, plan and rehearse our response to a successful cyber-attack. Incorporate lessons learnt from business continuity (BC) exercises and attack simulations into our plans and procedures.

Action	Responsible	Timeframe
Conduct annual cyber-attack tabletop exercises led by the Suffolk Joint Emergency Planning Unit with the council's Leadership team.	Emergency Planning Officer IT Infrastructure and Cyber Security Manager	Ongoing (annual)
Ensure lessons learned from business continuity (BC) exercises are captured and incorporated into future versions of our threat cards and service area plans.	Emergency Planning Officer IT Infrastructure and Cyber Security Manager	Ongoing (annual)
Ensure cyber-attack threat cards and service area business continuity plans detail how prioritised activities can be maintained if some or all IT systems go offline.	Emergency Planning Officer IT Infrastructure and Cyber Security Manager	Ongoing (annual or when services change)
Ensure the response plans contain timely actions to limit the impact of any cyber-attack.	Emergency Planning Officer IT Infrastructure and Cyber Security Manager	Ongoing (annual)
Conduct regular attack simulations on IT staff and end users to ensure they know how to respond to a genuine incident.	IT Infrastructure and Cyber Security Manager	Ongoing (one to two per year)
Ensure IT helpdesk personnel are aware of the process for dealing with initial access	IT Infrastructure and Cyber Security Manager	Ongoing

Action	Responsible	Timeframe
attempts, such as phishing, and take timely steps to make affected users safe.		
Regularly audit and test backup and restore processes.	IT Infrastructure and Cyber Security Manager	Ongoing (bi-monthly)
Formalise cyber incident root cause analysis documentation and process and testing these with simulated attacks.	IT Infrastructure and Cyber Security Manager	Quarter 4 2026
Formally adopt a 'no-pay' posture with a focus on recovery first resilience. This positions the organisation for forthcoming legislation which is expected to enforce no-pay legislation across the public sector.	Senior Information Risk Owner (SIRO) Cabinet	Quarter 4 2026
Actively participate in knowledge sharing with the wider local government and public sector, including participation in pilot projects as part of MHCLG's 'Defend as One' initiative and the local Warning, Advisory and Reporting Points (WARPs).	IT Infrastructure and Cyber Security Manager	Ongoing (as required)

Measuring success

Third party accreditations

Accreditation	Assessment type and frequency
NCSC Cyber Essential Plus	Annual audit by an accredited assessor
NHS Data Security Protection Toolkit	12- to 18-month validity, self-assessment
Public Services Network (PSN) and Department of Work and Pensions (DWP) and Memorandum of Understanding (MoU)	Annual assessment, written submission assessed by DWP and Department for Science, Innovation and Technology (DSIT).
Alignment to Cyber Assessment Framework (CAF)	Self-assessment with optional third party assurance

Key performance indicators (KPIs)

KPI	Target
User awareness training	More than 95 per cent of staff to complete annual cyber security training
Mean time to patch (MTTP)	Less than 72 hours
Recovery time objective (RTO) for critical systems	12 to 24 hours
Recovery point objective (RPO) for critical systems	4 to 8 hours
User reporting of suspicious emails	More than 65 per cent as measured against phishing simulations

KPI	Target
Users compromised by suspicious email simulations	Less than 2 per cent as measured against phishing simulations
Coverage of device vulnerability scans	More than 90 per cent of active devices
Microsoft secure score	More than 95 per cent

Appendix: Roles and responsibilities

The current governance structure includes the following key roles. We believe these provide an appropriate structure for the current organisation in terms of its size, complexity and exposure to current cyber risks. This will, however, be kept under review as part of the Corporate Risk Register process.

- **Senior Information Risk Owner (SIRO)**
The council's SIRO holds ultimate responsibility for information risk, including cyber risk, within the council, ensuring appropriate structures and processes are in place to manage cyber risk.
- **Cabinet**
Responsible for agreeing this strategy and will regularly receive updates on its implementation.
- **Leadership Team**
Sponsors and oversees the implementation of the strategy.
- **Information Governance Working Group**
Sponsors and oversees the implementation of the strategy.
- **IT Programme Board**
Ensures cyber security is considered in relation to all new systems.
- **Cyber Security Manager**
Responsible for the day-to-day management of cyber risk and associated controls.

Appropriate levels of knowledge and skills, including Certified Information Security Systems Professional (CISSP) accreditations, are maintained within the organisation.

Glossary

- **Application Programming Interface (API)**
An API is a set of rules and tools that lets one application request data or services from another – for example, pulling information from a back-office system to a customer self-service portal.
- **Cyber Assessment Framework (CAF) for Local Government**
A sector security framework that details recognised best practice for the management of cyber security within local government.
- **CIA triad**
This is a model that lists the three main properties of data security we are protecting: confidentiality, integrity and availability.
- **Data exfiltration**
The malicious movement or extraction of data from systems under the council's control.
- **Distributed denial of service attack (DDoS)**
A cyber-attack that compromises availability of our systems by sending abnormally high amounts of requests to our systems, rendering them slow or unusable by genuine customers.
- **Ethical hacker**
An ethical hacker is an offensive cyber security professional who legally tests systems at the request of their owners. They use hacking techniques to identify vulnerabilities before they can be exploited by a malicious hacker so the organisation can resolve them.
- **False positive**
A security alert incorrectly triggered as malicious activity.
- **Identity and access management (IAM)**
The management of the users of IT systems (human and non-human) from onboarding to offboarding (starters and leavers processes). This includes strong authentication of identities through passwords and MFA, as well as access controls on what an identity is authorised to do once they have been granted access to the system.
- **Immutable**
IT data that is difficult or impossible to delete.
- **Indicators of compromise (IoC)**
Static evidence of malicious activity that is used to compromise systems.
- **Lateral movement**
Once an attacker has compromised a user on the system, they attempt to compromise further users at the same level, ultimately looking for a way to compromise higher privileged user accounts like IT admin accounts to gain greater control of the system.
- **Multi factor authentication (MFA)**
A password alone is single factor authentication (something you know). Multi

factor adds in one or more other factors such as something you are (facial recognition or fingerprint) or something you have (smart phone authenticator).

- **National Cyber Security Centre (NCSC)**
The defensive branch of Government Communications Headquarters (GCHQ) who provide help and advice on best practice to defend the UK from cyber-attacks.
- **Open-source intelligence (OSINT)**
Intelligence gathered during the reconnaissance phase of a cyber-attack – for example, names and IP addresses of servers used to deliver council services or usernames and other staff details found online.
- **Penetration testing**
Penetration testing, or pen testing, is the process of simulating an attack on an IT system or network. These tests are carried out by vetted ethical hackers to identify weakness that could be exploited by malicious hackers. These tests aim to ensure IT systems and networks can withstand real world attacks.
- **Red teaming**
Penetration testing or ethical hacking that closely simulates real world attacks, using more covert means than in a traditional open book penetration test.
- **Risk appetite**
Rates the organisation's high level appetite to cyber risk. The example below is taken from the government's orange book.

Risk appetite	Description
Opposed	Avoidance of risk and uncertainty is key objective.
Minimalist	Preference for safe options that have a low degree of inherent risk.
Cautious	Preference for safe options that have a low degree of residual risk.
Mindful	Willing to consider all options and choose one that is most likely to result in successful delivery.
Enterprise	Eager to be innovative and to choose options that suspend previous held assumptions and accept greater uncertainty.

- **Security information and event management (SIEM)**
A system for collating and analysing logs.
- **Shadow IT**
IT devices and systems not sourced through the council's official processes via its IT team.
- **Single sign on (SSO)**
Uses a single identity provider so that a password does not need to be stored separately on all systems.
- **Software Bill of Materials (SBOM)**
This is a comprehensive list of components of an IT system that were not directly written by the vendor of the system. This often includes open-source software and components.
- **Software as a Service (SaaS)**
This is a cloud computing service model that delivers software applications over

the Internet as an approach rather than on internal council servers. Users can access these applications through a web browser or an app, usually on a subscription basis.

- **Tactics, techniques and procedures (TTP)**
Behavioural based indicators known to be used by threat actors.
- **The principle of least privilege**
This is the principle that users of an IT system should have the rights required to carry out their role and nothing more.
- **Threat actor**
A malicious individual or group targeting an organisation with a cyber-attack.
- **Vulnerabilities**
Weaknesses in IT systems or processes that would allow a threat actor to gain unauthorised access to systems.