ANNEX B: CORPORATE RISK MANAGEMENT GUIDANCE

Corporate Risk 3: Information and Cyber Security

OVERVIEW

This guidance note has been created using an example (Information and Cyber Security) to describe the key components of the register.

SECTION 1 – RISK OVERVIEW

This section provides an overview of the risk, identifying the owner and the impact on the Council's ability to meet the national well-being goals. The section also introduces and documents the risk from each of the four categories of risk used by the Council.

1.1: RISK DEFINITON – This provides a succinct definition of the risk, using language such as 'Failure to…'

1 – Risk Overview	
1.1 Risk Definition	Information and Cyber Security involves the practice of preventing the unauthorised use, access, disclosure, disruption, modification, inspection, recording or destruction of information. There is a risk of the Council not having appropriate arrangements in place to prevent this from occurring. This applies regardless of the form data/information may take i.e. electronic or physical.
1.2 Risk Owner	**Director of Corporate Resources**
1.3 Supporting Governance	**Corporate IT risk and governance processes** **Information Governance Team** **Information Governance Board chaired by the Senior Information Risk Owner (SIRO).**

1.3: SUPPORTING GOVERNANCE – Highlight any supporting governance arrangements that manage the risk.

1.4 Impact on our contribution to the Wellbeing Objectives			
To work with and for our communities	**To support learning, employment, and sustainable economic growth**	**To support people at home and in their community**	**To respect, enhance and enjoy our environment**
Yes	Yes	Yes	Yes

1.4: WELL-BEING OBJECTIVES IMPACT: This section aligns the Corporate Risk to the Well-being Objectives of the Council's Corporate Plan to indicate the potential impact this risk could have on our ability to deliver/meet the Well-being Objectives.

1.5: RISK CATEGORIES: Due to the nature of corporate risks, there will always be several aspects to them. To help analyse and evaluate the various aspects of the risk, the Council uses four categories which provide different perspectives on the risk. These are Political & Legislative, Resources, Service Delivery & Well-being and Reputation. These categories have been identified as they are the key considerations for our organisation that have a significant influence/effect over how we define and describe each corporate risk. They are a consolidation of the previous categories of risk used and represent a simplification of the way in which risks are categorised. As a risk is identified, we look to define it from each of the four categories as they apply. For example, any changes in the legislative environment such as the introduction of a new Act will place more duties on us to meet requirements of the new legislation. Therefore, when thinking about the risk from the perspective of "political and legislative" then we will describe the repercussions of us not meeting our new legislative requirements and the impact this has on the Corporate Risk overall. In addition, there must be consideration of the risk appetite that we as an organisation take towards the risk categories. The risk appetite level statements are outlined in the risk management policy.

1.5 Risk Categories (inc. consideration of risk appetite)		
Categories	**Yes/No**	**Definition**
Political & Legislative	Yes	Political and legislative impact of failing to comply with legislation including Data Protection Act 2018, Computer Misuse Act 1990, and the General Data Protection Regulation (UK GDPR). Failure to put effective information security and cyber security controls in place leading to the disclosure, unauthorised alteration or loss of authorised access to personal, sensitive or confidential information. Potentially leading to political instability, undermining confidence in local government. ***There is no appetite for failing to meet our statutory and legal obligations.*** ***The Council has an opposed stance to non-compliance with legislative, regulatory and safeguarding risks.***
Resources	Yes	Financial impact of fines from the Information Commissioner's Office for data breaches. Increased insurance and other costs following data breaches or cyber-attacks. Financial impact of correcting and resolving data breaches, including potential compensation to data subjects. Financial impact of recovering from a cyber attack and restoring services, including costs of third-party specialists, in house staff, and the loss of ability to generate revenue. Increased pressure on our financial resources and annually shrinking real-terms budgets impacting our ability to invest in assets and programmes of work consistent with a robust and resilient cyber security posture. Limited funding to address legacy systems, leading to threat actors (hackers, criminals, unfriendly nation states) exploiting vulnerabilities and attacking the council successfully. Budget constraints limiting our access to the necessary skills, resources, tools, software, systems, backups, business continuity and disaster recovery capabilities to either remediate a successful attack on the council or prevent one from happening in the first place. ***There is a mixed risk appetite to resources. The council takes an opposed stance to information management and cyber security risks. However, there is a need to make the best use of financial and human resources to manage information and cyber risk. The council takes a mindful to eager stance on technology and people to deliver strong controls to mitigate these risks.***
Service Delivery and Wellbeing	Yes	Failure to manage the information and cyber security risks effectively could severely impact the council's ability to deliver services and safeguard council and residents' information. This could have a serious impact on the wellbeing of residents, staff and other stakeholders.

1.5 Risk Categories (inc. consideration of risk appetite)		
Categories	**Yes/No**	**Definition**
		The council holds large volumes of sensitive data and loss of such data could have a severe impact on some of our most vulnerable service users. ***The council aims to innovate and create new service delivery models to help residents and stakeholders achieve their goals, taking an eager approach to some risks. It is cautious with risks related to statutory obligations. The council recognises certain risks as intolerable, particularly those that threaten health, safety, well-being, and the council's future operations. It firmly opposes any risks that would impact service delivery to our most vulnerable service users.***
Reputation	Yes	Cyber security and data loss incidents can have a serious negative impact on staff and service users, undermining confidence in the council and having the potential to greatly impact the reputation of the council. Leading to loss of trust from the public and damage to the credibility of the council in the eyes of third-party partners, regulators and service users. ***The Council has a cautious appetite to reputational risk.***

SECTION 2 – RISK EVALUATION

This is the second section of the risk register. It is where we consider the risk in different stages:

i. "The inherent risk" – i.e. before we consider what arrangements we've got in place to manage the risk, we think about the impact and likelihood of the risk occurring.
ii. Controls – we think about the controls that are in place to manage or mitigate the risk and the impact these have in terms of reducing the likelihood of the risk occurring or the impact it would have.
iii. The "residual risk" – we evaluate how effective the controls are at managing or mitigating the risk and the result this has on the risk.

Scoring is done by the likelihood of it occurring and the impact it would have if it did occur. We use a 1-4 scoring mechanism to define the likelihood and impact of a risk. See Appendix 1 for the risk scoring matrix. The multiplication of the likelihood and impact enables us to show how the two factors combined measure the scale of a risk.

2.1– INHERENT RISK SCORING:

For each of the four risk categories we identify a likelihood and impact score and use this to calculate a total inherent risk score for each risk category (by multiplying the likelihood by impact score).

To calculate the Overall Inherent Risk Score we calculate the average score for likelihood and impact columns for each risk category separately. The average likelihood is then multiplied with the average impact score to provide the Overall Inherent Risk Score for the Corporate Risk.

Please note that the risk scores are always whole numbers and as such, anything calculated as .5 and above is rounded up and anything below .5 is rounded down to the next whole number.

2 – Risk Evaluation			
2.1 Inherent Risk Scoring			
Category	**Likelihood**	**Impact**	**Total Inherent Risk Score**
Political & Legislative	4 (Almost certain)	3 (High)	**12 (High)**
Resources	4 (Almost certain)	3 (High)	**12 (High)**
Service Delivery & Well-being	3 (Probable)	3 (High)	**9 (Medium/High)**
Reputation	3 (Probable)	4 (High)	**12 (High)**
Overall Inherent Risk Score	**4 (Almost certain)**	**3 (High)**	**12 (High)**

2.2 – CONTROLLING INHERENT RISK

In this part of the register, the risk owner identifies and defines all of the existing controls that are in place to help minimise or reduce the risk. For ease of identifying them and understanding their effectiveness, this is done for each risk category in turn. In some cases controls may align to more than one risk category.

The risk owner provides an indication of the effectiveness of controls on the risk in terms of how effective they are at reducing both the likelihood and impact of the risk. Controls are scored 0-4, where a zero implies a poor control of risk and a four suggest that the controls in place a highly effective. See **Appendix 1** for a more detailed breakdown of scoring definitions for effectiveness of controls.

For each of the four risk categories a likelihood and impact score are provided along with a total effectiveness of control score which is calculated by multiplying the score for likelihood by the impact score for each risk category.

To calculate the Overall Effectiveness of Controls Score we calculate the average score for likelihood and impact columns for each risk category separately. The average likelihood is then multiplied with the average impact score to provide the Overall Effectiveness of Controls Score for the Corporate Risk.

Please note that the risk scores are always whole numbers and as such, anything calculated as .5 and above is rounded up and anything below .5 is rounded down to the next whole number.

2.2 Controlling Inherent Risk				
Category	**Current Controls**	**Effectiveness of controls**		
		Likelihood Score	**Impact score**	**Total Score**
Political & Legislative	• ICT security policies in place together with Access to Information Procedures that is signed by all staff and Members.	1	2	2

2.2 Controlling Inherent Risk				
Category	**Current Controls**	**Effectiveness of controls**		
		Likelihood Score	**Impact score**	**Total Score**
	• On-line training available for DPA and introduction of Employees Information Security Responsibilities. DPA training available to all members via their induction. • Information Security & Governance Framework arrangements are in place. • The Council conducts an annual IT Health Check (independent penetration and security testing by a certified third party) as part of Public Services Network (PSN) compliance. The compliance process provides assurance and confidence in the Council's ICT security arrangements and allows connection to PSN services. • Information Governance Board ensures that changes made to working practices, support and maintain the integrity of our systems and the security of all information used by the Authority.			
Resources	• Building and Office security/access arrangements in place to control access to Council buildings for authorised staff, members, and visitors. Additional physical security controls have been approved by SLT. • Industry standard network and device security implemented. • ICT Security and Governance functions and staff. • All laptops are encrypted, and all new desktops purchased are encrypted as standard. • Nominated systems administrators and system audit trails/admin logs maintained. • Penetration testing regularly undertaken • Corporate document retention system in place and FOI/Records Management Unit established. • Independent Digital Maturity Assessments have been conducted with the relevant findings informing security and compliance strategy. • Secure information sharing tools are available and widely used.	2	2	4

2.2 Controlling Inherent Risk				
Category	**Current Controls**	**Effectiveness of controls**		
		Likelihood Score	**Impact score**	**Total Score**
	• Enterprise class secure email filtering solutions are in place. • Data Protection refresher training delivered to all relevant staff that incorporates the GDPR requirements. • The Council follows compliance frameworks with the relevant security standards, including GDPR, PCI and PSN. • IT Asset Register maintained for all equipment/devices in schools that have an SLA agreement. • As part of the Welsh Government Hwb project, the council has upgraded the infrastructure in all Vale schools to meet the Welsh Government's minimum digital standards for schools. • The Vale Council, together with the other Welsh Local Authorities, is participating in Welsh Government's CymruSOC cyber security operations centre, as part of the Cyber action plan for Wales.			
Service Delivery & Well-being	• Information Security & Governance Framework arrangements in place. • Revised the Information Management Strategy to reflect how plans to use technology will support the delivery of the Council's Corporate Plan and the expected outcomes as well as how we will manage and safeguard information that we exchange between organisations and our partners. • Implementation Plan aligned to the Strategy is in place and is being delivered. • ICT Strategy has been signed off and ICT continue to support ICT projects that fall within the Digital programme of works associated with the Digital Strategy. • Protocol to enable us to reuse information under the Open Government licence has been developed and published on our website.	2	2	4
Reputation	• We inform our customers of how we collect, record, monitor and use their personal data to ensure that we gain consent to do so.	1	1	2

2.2 Controlling Inherent Risk				
Category	**Current Controls**	**Effectiveness of controls**		
		Likelihood Score	**Impact score**	**Total Score**
	• We implement appropriate technical and organisational measures to safeguard personal and business data.			
Overall Effectiveness of Controls		**2**	**2**	**2**

2.3 – RESIDUAL RISK SCORING: This is the final part of the risk evaluation process. The Residual Risk Score shows the level of risk remaining after the effectiveness of controls have been considered. It allows us to demonstrate how the inherent risk has been managed/reduced by the effectiveness of our controls.

2.3 Residual Risk Scoring & Direction of Travel

	Inherent Risk Scores			Effectiveness of Controls Scores			Residual Risk Scores			Direction of Travel	Forecast Direction of Travel
Category	**Likelihood**	**Impact**	**Total**	**Likelihood**	**Impact**	**Total**	**Likelihood**	**Impact**	**Total**		
Political & Legislative	4	3	12	1	2	2	4	2	4	Establish baseline	⟷
Resources	4	3	12	2	2	4	2	2	4	Establish baseline	↑
Service Delivery & Well-being	3	3	9	2	2	4	2	2	4	Establish baseline	↑
Reputation	3	4	12	1	1	1	3	4	12	Establish baseline	↑
Average risk score/ direction of travel	4	3	**12** A	2	2	**4** B	3	3	**9** C **(Medium/High)**	Establish baseline	⟷

SECTION 3: RISK MANAGEMENT PLAN

The final section contains a risk management plan. This plan is a summary of ongoing mitigating actions that will be taken to manage the residual risk. Where appropriate, linkages should be made to any existing action plans that will serve to mitigate the risk. The action plan is monitored quarterly. As updates are received, the Risk Owner determines whether a completed action becomes a control, and this is then included in section 2 as described above and may result in a rescoring of the effectiveness of controls (and therefore residual risk).

3. Risk Management Plan: Summary of Ongoing Mitigating Actions

Risk Owner to populate with reference to existing action plans that demonstrate ongoing mitigating actions.

OR

Risk Owner to create summary action plan to demonstrate ongoing mitigating actions.

IT Health Check Actions
Outstanding risks from the annual IT Health Check (independent security testing against compliance frameworks) are currently being managed to conclusion within Corporate IT.

Cyber Resilience Strategy
A draft Cyber Resilience Strategy for the council has been approved at the Information Governance Board and feedback incorporated into the final draft.
An associated action plan is being developed to facilitate delivery of the cyber resilience strategy.

Security Incidents and Events
Security incidents are reported to the Information Governance Board as a standing agenda item.

Red Team Exercise
A Red Team Security exercise has been carried out by an independent security specialist company and recommendations from the findings are being implemented by Corporate IT.

Senior Leadership Team Cyber Breach Workshop
A cyber breach workshop including a simulation exercise was carried out with the Senior Leadership Team and facilitated by an independent third party. Lessons learned and action points arising will be used to shape existing programmes of work and, policies and procedures.

Cyber Assessment Framework
The Welsh Government will be working with the Vale of Glamorgan Council and the other Welsh councils to pilot the National Cyber Security Centre's (NCSC's) Cyber Assessment Framework, as part of the Cyber Action Plan for Wales.

CymruSOC
The council will be onboarded into the Welsh CymruSOC Security Operations Centre in October 2024, as part of the Welsh Government's 'Defend as One' approach for public services.

RISK MATRIX:

Possible Impact or Magnitude of Risk					
	Catastrophic	4 *MEDIUM*	8 MEDIUM/HIGH	12 HIGH	16 VERY HIGH
	High	3 *MEDIUM/LOW*	*6* *MEDIUM*	9 MEDIUM/HIGH	12 HIGH
	Medium	2 LOW	4 *MEDIUM*	*6* *MEDIUM*	8 MEDIUM/HIGH
	Low	1 VERY LOW	2 LOW	3 *MEDIUM/LOW*	*4* *MEDIUM*
Low 1-2 Low/Medium 3 Medium 4-6 Medium/High 8-10 High 12-16		Very Unlikely	Possible	Probable	Almost Certain
		Likelihood/Probability of Risk Occurring			