

Appendix B

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

Risk ID 175 Risk Title Freedom of Information and Subject Access Requests Risk Level Corporate	IF we repeatedly fail to respond to FOIs and SARs and requests for erasure of personal data within the statutory timescales THEN we risk the number of overdue requests leading to an Enforcement Notice from the ICO requiring us to deal with the backlog and improve performance.	Medium	High	Red	Tracey Meredith / Kim Collis	> FOI and other information requests are all logged centrally and dispersed to a network of FOI officers embedded in different service units across the authority. Every service unit has an FOI officer. The workflow process for information requests is manual but will be automated. GOSS software has been purchased. Further improvements to the process are listed in 'Progress to Date' >Purchase and implement new workflow process software				>Internal audit of FOI / SAR / EIS on rolling audit cycle				Service Specific Assurance / Cross Cutting
--	--	--------	------	-----	------------------------------	--	--	--	--	---	--	--	--	--

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

<p>Risk ID 222</p> <p>Risk Title Digital, data and digital security</p> <p>Risk Level Corporate</p>	<p>If the council does not have robust cyber, data and digital security measures and behaviours in place, embedded and working as best as they can be then it will not be protected from cyber threats, disruption to service delivery, possible loss of information including confidential information and associated fines and reputational damage.</p>	Very High	Medium	Red	Sarah Lackenby / Jo Harley	<ul style="list-style-type: none"> >Communication to users to keep up awareness >Constant monitoring and surveillance of cyber risks by Security Office using system and tools in place. Situation reported monthly to Digital Services Board and Information Governance Board chaired by SIRO >DR test training completed for Digital Services team. >Simulated test of a cyber attack. Training to be provided to HoS and CMT >Simulated cyber-attacks on staff carried out periodically to measure their actions, identify weaknesses and improve knowledge >Cyber security guidance and cyber scams staffnet page >Cyber security strategy in place >Digital services continually working with internal audit and emergency planning to further improve the ICT disaster recovery plan >LRF Cyber exercise >SIRO training 			<ul style="list-style-type: none"> >Member of the Cyber Security Information Sharing Partnership which is a joint industry and government initiative to exchange cyber threat information >Part of Wales Warning Advice and Reporting Point to share cyber threats and defences with other public bodies >New regional multi-agency cyber cell meetings being attended to share intelligence and actions >PSN Certification Achieved >Cyber essential accreditation achieved >Member of Wales WARP & CISP sharing knowledge of threats. 	<ul style="list-style-type: none"> >Various IT / System audits in Audit Plan. >GDPR audits. 	<ul style="list-style-type: none"> >Public Services Network (PSN) compliance certificate – tested annually. 	<ul style="list-style-type: none"> >WAO review undertake an IT audit each year as part of reviewing financial accounts >WAO undertook an all Wales review last year and the findings were shared in closed sessions with G&AC and Cabinet / CMT 	<ul style="list-style-type: none"> >Range of IT audits in the plan to be completed as part of the rolling audit schedule. 	<ul style="list-style-type: none"> >IT audits included in the 2024/25 plan as per the rolling programme and additional ICT reviews as a result of the annual consultation exercise and review of risk registers. 	Service Specific – Digital & Customer Services and IT Audits – Transformation and Future Council
--	---	-----------	--------	-----	----------------------------	---	--	--	---	---	---	---	---	--	--

Appendix B

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

					<p>>Comms. Issued to staff and members detailing impact of cyber attack at other councils.</p> <p>>Software purchased to protect against malware attacks</p> <p>>More use of secure cloud storage.</p>			<p>>Discussed at IG Board – standing agenda item</p>						
--	--	--	--	--	---	--	--	---	--	--	--	--	--	--

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

Risk ID 235	If we do not have sufficient emergency planning, resilience and business continuity arrangements in place, then we will not be able to respond effectively in an emergency, provide the necessary civic leadership or continue to run vital services and ensure compliance with the legal requirements of the Civic Contingencies Act 2004 as a Category 1 Responder, which may lead to reputational damage, a loss of political and community confidence, increased potential for loss of life, prolonged	Medium	Medium	Amber	Ness Young / Craig Gimblett	As a Category 1 responder under the Civil Contingencies Act, Swansea Council has a legal requirement to plan for and respond to emergencies, to do this the following will be maintained and monitored by the CHSEMWS manager, with any gap or area of concern escalated to the CX. >The authorities Major Incident Plan will be reviewed annually, and tested on a 3 yearly basis unless activated, after which a review of the response will be provided to CMT, including any areas for improvement or additional resources needed to ensure we meet all legal obligations and can effectively respond to an emergency. >An annual delivery plan which clearly identifies priorities to address any gaps, or coming statutory needs, will be developed and delivered by the Emergency Management Service,	>EMS Manager briefs leader/cabinet as required. >CMT receives regular updates on key planning and agreement as required from EMS manager. >EMS manager meets monthly with the portfolio holder for political oversight and visibility. EMS Manager represents Swansea Council at Strategic level within SWLRF and Pan Wales Forums.	>EMS have been called to several Scrutiny panels, with none currently in the calendar.	>Multi agency exercising and training >Internal development/ training of new officers including newly created assistants post. >Joint work programs and information sharing with Welsh Civil Contingencies managers and South Wales Resilience Team. >Service Manager part of the National and Regional PSPG group and CONTEST Group with local PSPG arrangements in-place. >EMS is embedded within the SWLRF at Executive, Strategic and Tactical levels BC plans in-place with each HoS.	>EMS were audited in Nov 22 with an outcome of High assurance rating.	>EMS have been part of the consultation group for Welsh Governments Civil Contingencies review this will lead to independent external audit of Civil Contingencies when final structures are established in 2023. > The Protect Act, which places responsibility for CT planning based on organisational risk, as part of this a new Regulator will be appointed to enforce compliance/breaches and audit	>Independent external Audits will be conducted through Welsh Government and the new regulator appointed to enforce the Protect Duty in 2023/24 to establish maturity and mitigation.	>Standard audits in the plan cover this area on rolling basis.	>Audits in the plan to be completed in as part of the rolling programme include disaster recovery & Business Continuity, Emergency Planning & Business Continuity	Service Specific Audits – Communications / ICT / Council wide assurance
-----------------------	--	--------	--------	--------------	------------------------------------	--	--	--	---	---	--	--	--	---	---

Appendix B

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

	recovery following a major/business continuity incident which will deny service to the public and increase operating costs.				to ensure compliance and maintenance of our ability to effectively respond and protect the organisation and communities . >Maintain and review on an annual basis all subordinate plans, including Mass Fatalities, Flood, Offsite COMAH Plan, Rest Centre Plan. with exercising as appropriate >Deliver a duty officer rota to effectively respond to emergencies available 24 hours per day, 365 days per year, this will be shared with all key external and internal partners including CMT to ensure a timely response can be achieved. >Annually review all identified risks, with relevant partner agencies that are present within the borders of Swansea Council to ensure control measures remain relevant and proportionate. >Ensure that all HoS review their business			>Plans and Action cards reviewed annually and EMS audited in 2022. >Collaborative working with SWP on call out protocols in-place and reviewed. >ACT App and free training promoted across Authority. Local Partner CT comms strategy and alerts system established.		arrangements.			
--	---	--	--	--	--	--	--	--	--	---------------	--	--	--

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

Risk ID 236	If the Authority does not have a robust framework of Health & Safety Policies and procedures that are reviewed regularly, or in the event of significant change, it may lead to legal non-compliance, the realisation of adverse events including reputational damage, injury, financial loss and litigation by regulators.	High	Low	Amber	Ness Young / Craig Gimblett	To ensure the Authority meets it's legal responsibilities the following will be implemented and monitored. >Review the statutory Corporate H&S Policy and arrangements under full consultation with the organisation and TU's on a 3 yearly cycle, or when there is significant statute change or on the appointment of a new CX or Leader. Communicate changes to the Corporate H&S Policy to the organisation via H&S Alert and published on Staffnet. >HR to provide a copy of the Corporate H&S Policy to all new starters prior to commencement of employment, and be covered during induction, and completion of Mandatory H&S training to meet legal compliance, clarify roles and responsibilities and avoid accidents, ill health, reputational damage and the potential for legal/financial penalties.	>H&S Manager provides regular updates, reports, presentations, and statistics. to CMT. >H&S Manager meets monthly with portfolio holder to provide briefing and political oversight and awareness. >Accident Statistics and investigations finding provided to all H&S Committees' and sub groups.	>H&S Manager has provided updates to numerous scrutiny panels, none currently in diary. >Service has been fully audited internally in 2019.	>Member of British Association of Counsellors and Psychotherapists (Bacp). >Directors H&S Committees & Sub Safety Groups >Increased accessibility to H&S training via teams and online. >Policy development and review plan in-place under full consultation. >Officer representation at trade union meetings. >Additional resources placed in Occupational Health (31/03/230 & Stress Management and Counselling, with extension of Psychological Support project until 31/03/23	>H&S Audit Plan	> H&S Manager represents Swansea on a Pan Wales/regional basis as part of the Managers forum to share best practise and coproduce where appropriate.	>Standard audits in the plan already cover this area.	>Health, Safety & Wellbeing audit completed in 22/23 on the rolling programme	Service Specific Audits – Communications / ICT / Council wide assurance
-----------------------	---	------	-----	--------------	------------------------------------	--	--	--	--	-----------------	--	---	---	---

Appendix B

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

					<p>>Each Director or their delegated HoS to ensure a minimum of a Bi-annual H&S Committee, which will receive all minutes of lower level H&S Groups, statistics and information from the CHSEMWS, including any regulatory activity from the HSE/M&WWFRS and agree actions to resolve any unaddressed risks, with an agreed timeframe for completion.</p> <p>>Review all H&S policies and guidance under full consultation every 3 years, in the case of significant change through legislation or if an adverse incident identifies the need for review. Monitor and report as part of the Corporate HSW action plan, which will be updated on-line quarterly, with reports on progress submitted to each Directors H&S committee with a formal update on an annual basis to CMT.</p> <p>>Publish a Health, Safety & Wellbeing Action plan on a rolling</p>			<p>> New CORITY OH management software management package due for implementation March 2023.</p> <p>> SEQOHS accreditation submission and assessment due March 2023.</p> <p>> Application for evaluation for Welsh Government Gold Corporate Health Standard October 2023.</p>					
--	--	--	--	--	---	--	--	---	--	--	--	--	--

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <u>Internal</u> Assurance			Other <u>Independent</u> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

					avoid accidents, ill health, reputational damage and the potential for legal/financial penalties. > Each Director or their delegated HoS is responsible for ensuring a minimum of a Bi-annual H&S Committee, this will receive all minutes of lower level H&S Groups, statistics and information from the CHSEMWS, including any regulatory activity from the HSE/M&											
Risk ID 335 Risk Title Workforce recruitment and retention Risk Level Corporate	If the Council is not able to recruit and retain the right staff, then there may be reduced workforce capacity and capability, leading to lower staff morale and productivity, poor work quality, increased staff costs and reduced staff well-being / higher sickness rates.	Medium	Low	Amber	Rachael Davies / Rachael Davies	>Review the existing recruitment policy and assess weaknesses in application processes and selection processes for improvement by April 2023, to ensure the most appropriate application and selection techniques are being used to hire talent into the organisation. >Quarterly reporting provided to Directorates for PFM to highlight areas of concern and consider targeted approaches accordingly	>Cabinet Member briefings, Cabinet reports where applicable	>Regular reporting to Scrutiny Working Group - Regular reporting to Organisational Development CDC	>Quarterly reporting provided to Directorates for PFM to highlight areas of concern and consider targeted approaches accordingly. Quarterly reporting to Workforce Transformation Programme Board	>Internal audit of recruitment procedures			>Standard rolling audit schedule, repeated based on audit risk score.	>Audits included on rolling programme in HR & OD / Service Centre. Includes Recruitment and Staff Contracts		Service Specific Audits – HR & OD, Service Centre /

Appendix B

Business Risk	Current Impact	Current Likelihood	Overall RAG Status	Risk Owner / Updater	Level and Source of Assurance						Internal Audit Needs	Planned Internal Audit Work	Audit Plan Area	
					Level 1	Level 2			Level 3					
					Management Assurance	Other <i>Internal</i> Assurance			Other <i>Independent</i> Assurance					
Council/ Cabinet	Scrutiny	Other	Internal Audit	Other Bodies		External Audit								

Risk ID 336	If the Council does not implement, monitor and ensure the completion of mandatory training, then the Council may not fulfil its statutory and regulatory obligations or ensure the safe and effective operation and delivery of services.	Low	Low	Amber	Ness Young / Rachael Davies	>Regular Quarterly and annual reports to CMT on compliance levels by Directorate.	>Cabinet Member briefings, Cabinet reports where applicable	>Scrutiny Panels in place to scrutinise Social Services Work and Performance, of which safeguarding training is included; Scrutiny Working Group – Workforce in place	>Mandatory Corporate Training available for all Staff and Members. Reports to CMT on progress and actions required	>Internal Audit of mandatory training compliance Governance and Audit Committee reporting	>HSE where applicable CIW/EWC where applicable	>Standard rolling audit schedule, repeated based on audit risk score.	>Safeguarding cross cutting audit is included in rolling programme >Corporate Learning & Development team audit due for 2024/25 following Fusion implementation linked to training records	Service Specific Audits – HR & OD, Service Centre /
-----------------------	---	-----	-----	--------------	-----------------------------	---	---	---	--	---	--	---	---	---

