

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 1	Defend / Technology	Maintain firewall and scanning services.	100%	Apr-23		Jan-23	
AP - 2	Defend / Technology	Maintenance of end-point protection for devices – Anti Virus, USB Encryption and Mobile Device Management.	67%	Estimated End 2024			
AP - 3	Defend / Technology	Undertake Cyber Security Health Checks and Penetration Testing.	67%	Sep-23	Dec-24		On further investigation a wider scope assessment is to be undertaken which has increased the completion date to December 2024
AP - 4	Defend / Technology	Utilisation of the National Cyber Security Centre tools. WebCheck and Mail Check.	75%	Nov-23	Nov-23		CF to check with RF and make the change if not done already.
AP - 5	Defend / Governance	Meet compliance regimes which require good Cyber Hygiene (Public Service Network Code of Connection, Cyber Essentials).	83%	Apr-24	Mid 2025		Due to delays in other elements of work this is beginning in April 2024, and is expected to run into 2025 and will be embedded into our rolling program of infrastructure modernisation.
AP - 6	Defend / Governance	Be an active member of the public sector cyber security community. Participation in the Cyber Security Information Sharing Partnership (CISP) and Wales Local Authority Warning, Advice and Reporting Point.	100%	May-23		23-May	
	Deter / Technology	Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions.	25%	End of 2023	Dec-24		The development and management of polices has transition into business as usual work and as a result is no longer part of the Cyber Security Action Plan.

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 1	Deter / Technology	Reconcile current systems in place and last times these were reviewed.	25%	Mar-24	late 2024		Resource commitments have resulted in this being moved to late 2024.
AP - 2	Deter / Technology	Protect enterprise technology by working with specialist partners to develop model architecture.	100%	Apr-23		23-Apr	
AP - 3	Deter / Technology	Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services.	50%	Mid 2024			Resource commitments have resulted in this being moved to late 2024.
AP - 4	Deter / Governance	Embed the Secure by Design principle throughout.	100%	Apr-23		23-Oct	
AP - 5	Deter / Governance	Review vendor management to address supply chain risk.	50%	Mid 2024	late 2024		Resource commitments have resulted in this being moved to late 2024.
AP - 6	Deter / Governance	Review (update where appropriate) policies and procedures.	13%	Mid 2024	Dec-24		The development and management of polices has transition into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 7	Develop / Technology	Explore Active Cyber Defence tools and new technologies to ensure we have the best solutions to match to threats.	50%	On hold pending WG SOC review			The main pieces of work are waiting on WG. In the meantime we have started implementation of IDS/IPS and a local Security Incident and Event Monitoring system.

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 8	Develop / Technology	Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.	33%	Pending WG direction			WLGA Cyber Resilience workshop taking place on 14/03/2024. WG events waiting on further information from WG.
AP - 9	Develop / Governance	Provide relevant cyber security training for staff and elected members to help detect, deter and defend against the cyber threats.	86%	Feb-24	Apr-24		In process to be completed by end of April 2024.
AP - 10	Develop / Governance	Develop and maintain a risk management framework, internal controls and governance mechanisms. Process, procedures and controls to manage changes in cyber threat level and vulnerabilities.	25%	End of 2023	late 2024		Current Risk Management approach utilises the corporate Risk Management framework which is undergoing modification. Intention to dovetail into this for completion by end of 2024.
AP - 11	Develop / Governance	Aligned with best practice, develop a minimum requirement for all systems used, audit trails, deletion of data etc.	50%	May-23	Apr-24		With the extraordinary changes in global digital landscape (AI) and these needing to be reflected in the process, the completion will be the end of April 2024
AP - 12	Develop / Governance	Develop a communication plan in the event of an incident, which includes notifying the senior accountable individuals, the communication team, statutory notification bodies and relevant external organisation and law enforcement as applicable.	100%	Oct-23		Nov-23	
AP - 13	Develop / Governance	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.	100%	Delivered		Aug-23	

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 14	Develop - Governance	Create a cyber-specific Business Continuity Management Plan and/or review our Incident Plan to include emergency planning for cyber-attack.	100%	End of 2023		Dec-23	The development and management of business continuity plans has transitioned into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 15	Defend / Technology	Maintain firewall and scanning services.	0%	Aug-23	Pending WG direction		The main pieces of work are waiting on WG. In the meantime we have started implementation of IDS/IPS and a local Security Incident and Event Monitoring system.
AP - 16	Defend / Technology	Maintain firewall and AD scanning.	100%	Apr-24		Feb-24	The management of AD scanning has transitioned into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 17	Develop - Governance	AI Strategy - New, added April 2024	0%	Mid-Late 25 <i>(NEW)</i>			Mid-late 2025