FRONTIER AI: ORGANISATIONS MUST ACT NOW

National Cyber Security Centre

Frontier AI is collapsing exploit timelines from days to hours. Lock down the fundamentals now.

N-days → N-hours
Vulnerability Discovery to Exploitation

	01	02	03	04	05	06
STRATEGY	**Secure** **Horizon: Short-term** Systems are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced.	**Reduce** **Horizon: Short-term** Vulnerabilities in systems are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.	**Replace** **Horizon: Short-term** Systems that are not capable of meeting cyber security requirements are managed using compensating controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or replaced.	**Prepare** **Horizon: Medium-term** Systems are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced.	**Adopt** **Horizon: Medium-term** Artificial intelligence is used for cyber defence and is secure, controllable, human supervised and used in an ethical and accountable manner.	**Modernise** **Horizon: Longer-term** Systems are planned, designed, developed, tested, deployed, maintained and decommissioned according to business criticality ratings and security and resilience requirements using Secure by Design and Secure by Default principles and practices.
ACTIONS	**Reduced attack surface** ▪ Define and deploy approved configuration baselines. ▪ Disable or remove insecure or unnecessary services, settings and communication protocols. ▪ Detect and respond to configuration drift from approved configuration baselines through automation or continuous security assessments.	**Secure software vulnerabilities** ▪ Identify software vulnerabilities and weaknesses through continuous security assessment activities. ▪ Apply security patches, updates or vendor mitigation within risk-based timeframes or, where operational impact is low, automatically.	**Replace legacy information technology** ▪ Establish and maintain a process for identifying, assessing and managing the cyber security risk associated with legacy systems. ▪ Replace or isolate legacy systems where operationally possible.	**Prepare for cyber security incidents** ▪ Review cyber security incident response, business continuity and disaster recovery plans to ensure they remain fit for purpose. ▪ Regularly exercise cyber security incident response, business continuity and disaster recovery plans.	**Adopt AI for cyber defence purposes** ▪ Deploy AI models for augmenting software development activities, such as identifying and remediating software flaws and weaknesses. ▪ Deploy AI models for augmenting system assurance activities, such as performing vulnerability scanning and vulnerability assessments. ▪ Deploy AI models for augmenting system monitoring.	**Modernise for the future** ▪ Design systems to enforce authorised access and minimise default and required privileges. ▪ Design systems to protect data. ▪ Design systems to provide visibility.

FRONTIER AI: ORGANISATIONS MUST ACT NOW

National Cyber Security Centre

ACTIONS	DESCRIPTION	GUIDANCE
1. Approved configuration baselines	Define and deploy approved configuration baselines.	ISM Control: 3287, 3389, 4895, 4896
2. Software configuration hardening	Disable or remove insecure or unnecessary services, settings and communication protocols.	ISM Control: 1162, 1163, 1149, 7554, 1878
3. Approved configuration drift	Detect and respond to configuration drift from approved configuration baselines through automation or continuous security assessment.	ISM Control: nil
4. Continuous security assessments	Identify software vulnerabilities and weaknesses through continuous security assessment activities.	ISM Control: 4909,
5. Patching Processes	Apply security patches, updates or vendor mitigations within risk-based timeframes or, where operational impact is low, automatically.	ISM Control: 3451, 3452, 3453
6. Legacy ICT management	Establish and maintain a process for identifying, assessing and managing the cyber security risk associated with legacy systems	ISM Control: 3465
7. Legacy ICT decommissioning	Replace or isolate legacy systems where operationally possible	ISM Control: 3465
8. Incident response planning	Review cyber security incident response, business continuity and disaster recovery plans to ensure they remain fit for purpose	ISM Control: 1260, 1154
9. Incident response exercising	Regularly exercise cyber security incident response, business continuity and disaster recovery plans.	ISM Control: 709
10. AI software test	Deploy AI models for augmenting software development activities, such as identifying and remediating software flaws and weaknesses.	ISM Control: nil
11. AI security assessments	Deploy AI models for augmenting system assurance activities, such as performing vulnerability scanning and vulnerability assessments.	ISM Control: nil
12. AI security monitoring	Deploy AI models for augmenting system monitoring activities, such as identifying and triaging cyber security events.	ISM Control: nil
13. System authentication security	Design systems to enforce authorised access and minimise default and required privileges.	ISM Control: 1480, 1149, 7541, 1829, 1945
14. System data security	Design systems to protect data.	ISM Control: 865, 4849, 1123, 1892
15. System visibility provision	Design systems to provide visibility.	ISM Control: 2013, 6860, 2006, 6861, 2022, 2018, 2001, 2017, 7560, 7561, 2031, 2029, 4444, 4445, 2009, 2012, 3637, 3640, 1593