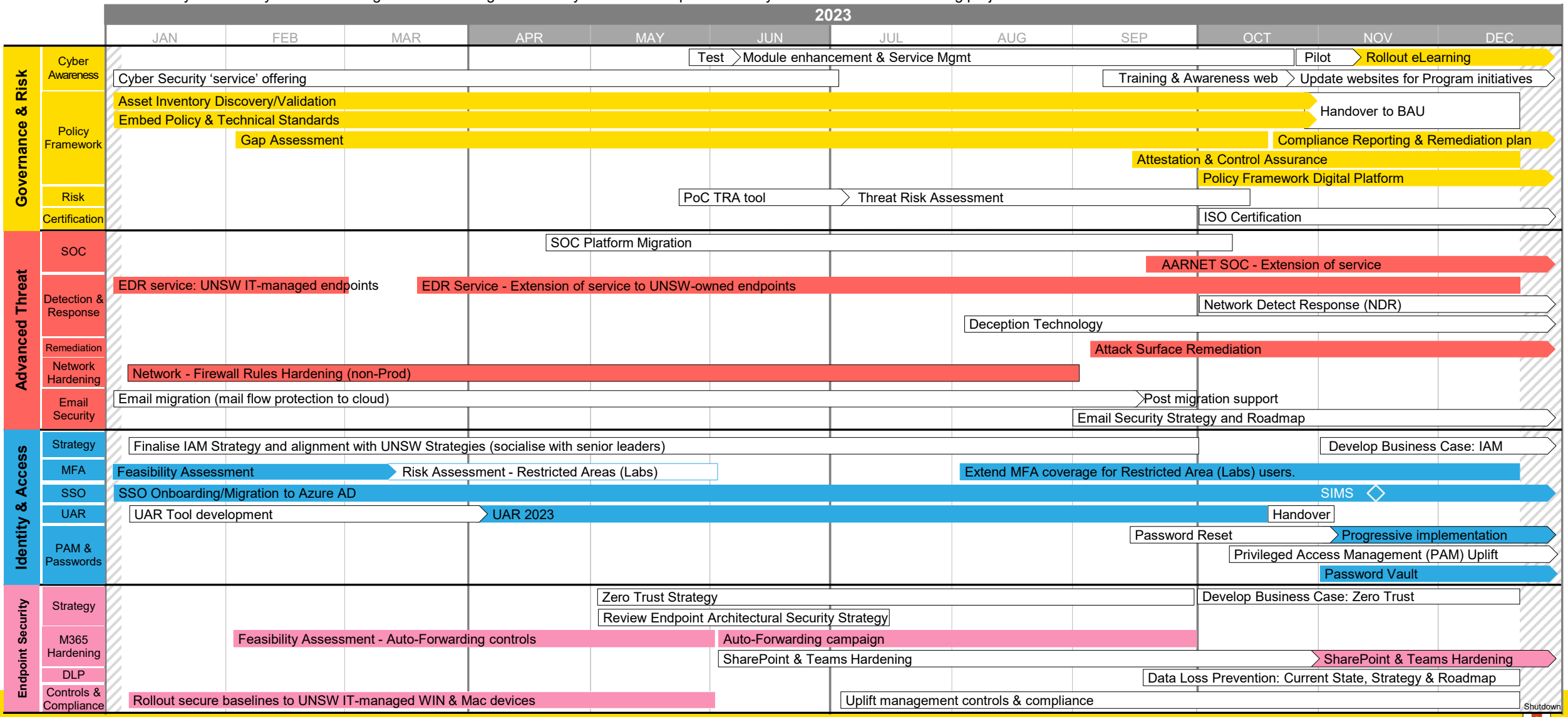
Cyber Security Resilience Program timeline 2023

UNSW IT Cyber Security Resilience Program is continuing to reduce cyber risk and improve security for UNSW with the following projects:

High-level **impacts key:**

- White cell = Impacts UNSW IT only.
- Coloured cell = Impacts staff.
- Coloured cell + boarder = Impacts staff and students.



UNSW IT Cyber Security Resilience Program

W: Cyber Security Resilience Program | Cyber Security | UNSW Sydney

E: cybersecurityresilienceprogram@unsw.edu.au

27 September 2023

Program – overview of projects 2023

UNSW IT Cyber Security Resilience Program is continuing to reduce cyber risk and improve security for UNSW with the following projects:

Key:
OCM Organisational Change Management
BAU Business As Usual
PoC Proof of Concept
SME Subject Matter Expert

Governance and Risk Management (GRM)

These projects focus on embedding frameworks and security controls within the University and uplifting the compliance, awareness and understanding of cyber security.

Cyber Awareness

Cyber Security eLearning

In 2023, UNSW will introduce a new **Cyber Security Awareness eLearning module** mandatory for all staff, with annual refreshers to keep knowledge current. This awareness module will be included in staff inductions as part of HR compliance requirements.

This project will:
- Develop a self-paced, interactive Cyber Security Awareness module that will contain an assessment component and will be accessible via Moodle.
- Develop dashboards and reports for compliance tracking.
- Uplift the Cyber Security Training and Awareness website.

Impacts:
- All staff (incl. affiliate, casual, etc)
- HR support teams.
- UNSW IT & HR support teams.

→Learn more

OCM: Shirley Ndelaphi

Cyber channels

In 2022, the Program created an external facing Cyber Security website and five intranet pages to build cyber awareness.

This project will:
- Profile cyber BAU services by team.
- Uplift pages relating to inflight projects and where required transition to a BAU maintenance and ownership model.

Impacts:
- UNSW IT support teams.

→Learn more

OCM: Zoe Lukic

Policy Framework

In 2022, all Cyber Security Policies and Standards were updated to uplift the maturity of Cyber Security at UNSW. The Policy Framework project will:

- Conduct an **Asset Inventory** validation & discovery of all UNSW IT Managed and UNSW managed systems.
- Develop a **transition plan** to an agreed BAU maintenance and ownership model in line with the IT Asset Management Strategy.
- Embed **Cyber Security Policies and Standards** across the University and inform key roles responsible
- Assist key roles to conduct a **Gap Assessment**
- Support key roles to develop **Remediation** (risk treatment) **Plans** and exemption documentation
- **Compliance Reporting.**

Impacts:
- Roles outlined in Cyber Security Policies and Standards: Business Owners/ IT Service Owners.
- Technical SMEs.
- UNSW IT support teams.

→Learn more

- Assist senior managers with their **Attestation and Assurance** responsibility.

Out-of-scope:
- *Implementation of Control Assurance Program.*
- *Report of Attestation outcomes/gaps.*

Impacts:
- Senior Manager level: DVC, VP, Dean, Rector and Director.

- Assist the Cyber Security Strategy & Governance team to establish a Cyber Security Community of Practice to support the embedding of the Framework.
- **Handover** Policy Framework to BAU support.

Impacts:
- Cyber Security Strategy & Governance team.

- Implement a Policy Framework **Digital Platform** to assist with ongoing compliance to the framework.
- Engage a third-party vendor to develop/ implement the platform, operating model & user manual.

Impacts:
- All roles involved in Policy Framework.

OCM: Taylor Gorman

Risk

In 2022 a new Governance Risk & Compliance (GRC) tool was developed to manage security risks.

This project will:
- Engage a service to undertake a control maturity and threat **Risk Assessment**.
- Report to contain current state assessment, and recommendations for risk treatment.

Impacts:
- UNSW IT Support teams.

Certification

Certification against ISO 27001 to formally recognise UNSW's Information Security Management System (ISMS) compliance.
- With Cyber Strategy & Governance team, the program will undertake a gap analysis, risk assessment, documentation and audit accreditation.

Impacts:
- UNSW IT Support teams.

Program – overview of projects 2023

UNSW IT Cyber Security Resilience Program is continuing to reduce cyber risk and improve security for UNSW with the following projects:

Key:
OCM Organisational Change Management
BAU Business As Usual
PoC Proof of Concept
SME Subject Matter Expert

Advanced Threat Management (ATM)

These projects focus on uplifting controls to improve the University's endpoint detection and response, managed security service, network and firewall rules in line with Cyber Security Policies and Standards.

Security Operations Centre (SOC)

In 2022 a new 24/7 Managed Cyber Security Operations Centre (SOC) was established to uplift the UNSW capability to detect, monitor and respond to security events. This project will:

- Migrate off AARNET LogRhythm Security Information and Event Management (SIEM) to Falcon LogScale.

Impacts:
- UNSW IT support teams.

- Establish an AARNET SOC service request for servers and workstation assets not previously known to IT, in accordance with Cyber Security Policies and Standards.

Impacts:
- Business Owners.
- IT Service Owners.
- UNSW IT support teams.

Detection & Response

In 2022 a strategic MDR service was procured, and the implementation of an **Endpoint Detection and Response (EDR) Service** commenced to provide UNSW with 24/7 advanced threat notifications on all endpoints. This project will:

- Complete the implementation of EDR technology on **UNSW IT-managed endpoints**.
- Operationalise the EDR/MDR Service.

Impacts:
- Staff with IT-managed devices.
- UNSW IT support teams.

→Learn more

- **Extend EDR/MDR services** to agreed state.
- **Establish an EDR Service request process** for UNSW-owned (non-UNSW IT-managed) endpoints.
- Embed the end-to-end EDR service.
- Migrate off FireEye HX, SEP and MS Defender as needed.

Impacts:
- Business Owners.
- Staff with UNSW-owned devices.
- UNSW IT support teams.

→Learn more

Implement **Deception Technologies** to provide active defence to improve proactive intelligence, detection and response. This project will:
- Define project scope and outcomes.
- Develop future state high-level solution options
- Conduct market analysis and product selection.
- Implementation and operationalisation of the service.

Implement **Network Detect Response (NDR)** solutions to enhance visibility and provide early network level threat detection against sophisticated attackers. This project will:
- Define UNSW NDR requirements.
- Conduct current state/gap analysis and market analysis.
- Conduct PoC and provide recommendation to proceed with procurement.

Out-of-scope:
- *Implementation of NDR solution.*

Impacts:
- UNSW IT support teams.

Remediation

Remediate high priority vulnerabilities identified from an external attack surface assessment.

This project will:
- Identify application/asset owners of the prioritised issues and vulnerability findings (1090 IP addresses and 76 domains) and provide remediation recommendations.
- Drive remediation activities undertaken by owners.
- Explore opportunities of augmenting resources of the most impacted findings area to assist with remediation.

Out-of-scope:
- *Remediation of operational vulnerabilities by the program.*

Impacts:
- UNSW website owners and technical support staff.
- Indirectly, website users.
- IT support teams.
- UNSW IT support teams.

Network Hardening

Assessing UNSW's network landscape and planning the implementation of high priority activities to uplift the Network Security posture.

This project will:
- Audit, review and harden firewall policies and network infrastructure in the **non-Production (Test) environment** to address all agreed critical to medium vulnerabilities.
- Review and update support model (as required).

Impacts:
- Non-production firewall owners.
- UNSW IT support teams.

→Learn more

Email Security

The migration from an on-premise Email Security platform to a Cisco Secure Email Cloud service will improve email traffic, simplify deployment and lower ongoing operational costs.

This project will:
- Migrate to a Cisco Email Cloud service.
- Agree on items for inclusion in future project scope (H2 2023+).

Impacts:
- UNSW IT support teams.

→Learn more

Leveraging the 2022 assessment and email security control architecture blueprint.

This project will:
- Develop an **Email Security Strategy and** target state **Roadmap**.

Impacts:
- USNW IT support teams.

OCM: Sarah Shannon

OCM: Zoe Lukic

Program – overview of projects 2023

UNSW IT Cyber Security Resilience Program is continuing to reduce cyber risk and improve security for UNSW with the following projects:

Key:
OCM Organisational Change Management
BAU Business As Usual
PoC Proof of Concept
SME Subject Matter Expert

Identity and Access Management (IAM)

These projects focus on setting the strategy for, and uplifting identity and access controls in line with Cyber Security Policies, Standards and respective guidelines.

Strategy

A review of the IAM strategy was undertaken in 2022.

This project will:
- Optimise the IAM Strategy & Roadmap.
- Develop an IAM business case for prioritised roadmap initiatives.

Impacts:
- UNSW IT support teams.
- Key UNSW operational leaders.

→Learn more

MFA for Restricted Areas

In 2022, MFA was introduced for all UNSW staff and students. An MFA exemption process was put in place for users of restricted areas. A restricted area is any laboratory rated as Physical Containment level 2 or 3 where entry with mobile phones or YubiKeys is not permitted.

Restricted area users are MFA-exempt when physically on campus.

This project will:
- Facilitate a risk assessment to identify recommendations to remediate risks.
- Implement a dedicated VLAN for restricted areas to facilitate device-based MFA exemptions.

Impacts:
- (Restricted area) Lab Managers.
- Staff and students accessing restricted areas.
- UNSW IT & IT support teams.

→Learn more

Single Sign-On (SSO)

SSO functionality enables seamless login and supports modern authentication protocols such as MFA.

In 2022, 68 integrations to the Azure SSO platform were completed and a request process established for application onboarding.

This project will:
- Build Azure Application Proxy capability for critical legacy applications that do not support OIDC, OAuth, SAML.
- Discover and integrate applications with a Cyber risk rating of *High* and *Medium* as per the Cyber Security Standard - Identity and Access Management.
- Develop a transition plan to an agreed maintenance and ownership model.

Impacts:
- Business Owners.
- IT support teams.
- UNSW IT support teams.

→Learn more

UAR 2023

In 2022, an inaugural and formal review User Access Review (UAR) process, compliant with UNSW Cyber Security Policies and Standards as well as NSW Audit was implemented.

This project will:
- Develop an interim online tool MyUAR for user reviews.
- Facilitate a 2023 UAR for 61 agreed applications.
- Remediate accesses as per the UAR results.
- Publish UAR reports for audit and compliance.
- Develop a transition plan to an agreed BAU

Impacts:
- Business Owners.
- IT System Owners.
- Managers/Supervisors (of targeted staff accounts).
- Nominated delegates.

→Learn more

Privileged Access Management (PAM) & Passwords

To align with the Cyber Security Standard - Identity and Access Management the following projects will be undertaken:

A **Password Reset** is required that will:
- Require a one-off reset to meet minimum standard for passwords/ passphrases.
- Passphrases must be at least 14 characters in length and meet other password Policy conditions.
- Affect staff, students, alumni with a current staff/student role and staff admin accounts.

The project will:
- Undertake a current state assessment.
- Uplift password policy for highly critical systems.
- Develop and deliver a rollout plan for password reset.

Impacts:
- Staff & current students with a zPass.
- UNSW IT support teams.

A **Password Vault** allows technical/ administrative staff to store enterprise passwords where the password used is for an application/asset/ system where the account is not on SSO.

Out-of-scope:
- *Password Vault for Students.*

This project will:
- Undertake a current state assessment.
- Develop a strategy to implement PAM solution.
- Develop implementation and rollout plan.
- Onboard high and medium privileged accounts.
- Develop an operating and support model.

Impacts:
- Targeted IT application support teams.
- UNSW IT support teams.

A **PAM uplift** for Service, Privileged and generic/shared accounts.

Out-of-scope:
- *Procurement of an alternative PAM solution.*

OCM: Zoe Lukic | OCM: Sarah Shannon | OCM: Zoe Lukic

Program – overview of projects 2023

UNSW IT Cyber Security Resilience Program is continuing to reduce cyber risk and improve security for UNSW with the following projects:

Key:
OCM Organisational Change Management
BAU Business As Usual
PoC Proof of Concept
SME Subject Matter Expert

Endpoint Security Management (ESM)

These projects will refine the strategy and implement controls and compliance for all UNSW managed endpoints (i.e., any UNSW owned device connected to the UNSW network, e.g., workstations, servers).

Strategy

A review of the **Endpoint Strategy and Roadmap** is required in line with the University Cyber Security, Acceptable Use Policy. Consideration will also be given to a strategic Zero Trust model.

This project will:

- Review and develop an Endpoint Architectural Strategy and Roadmap.
- Develop a Zero Trust model.
- Obtain IT Management endorsements.

Impacts:

- UNSW IT support teams.

→Learn more

OCM: Taylor Gorman

M365 Hardening

In 2022 this project started the process of strengthening the Microsoft 365 environment by introducing additional technical controls across the M365 collaboration platforms in line with the updated Cyber Security Policies and Standards. In 2023 this project will focus on:

- An awareness campaign discouraging staff from **Auto-Forwarding UNSW email** to external (non-trusted) domains as this exposes sensitive University data to potential security risks.
- Educating staff to directly check their staff email inbox regularly for important University updates in the Outlook app or on Outlook on the web.

Impacts:

- Staff who currently auto-forward UNSW email to private/insecure email accounts.
- UNSW IT support teams.

→Learn more

- Investigating options to **Harden Microsoft Teams and SharePoint** by assessing and improving current controls/configurations.
- Changing default settings in Teams/SharePoint/One Drive to minimise security risks, inadvertent data leaks and oversharing with unintended recipients.
- Determine scope and develop implementation plan.

Impacts:

- All staff *(to be confirmed)*.
- UNSW IT support teams.

OCM: Shirley Ndelaphi

Data Loss Prevention (DLP)

In 2021 a **DLP** solution was implemented to protect sensitive data and reduce risks from inadvertent or deliberate sharing. UNSW deployed this Information Protection and DLP to a limited pilot group. A wholesale rollout of DLP was deferred until a future date.

This project will re-initiate the DLP stream and establish a platform to uplift DLP controls by:

- Undertaking a current state assessment of DLP capability including review of findings from the previous 2019 DLP pilot.
- Engaging key stakeholders to finalise objectives, requirements and define UNSW use cases and benefits for DLP.
- Developing a **DLP Strategy and Roadmap** for implementing change to enable DLP capability.

Out-of-scope:

- *Broad rollout of DLP to staff/students.*
- *Procurement of alternative DLP solution.*

Impacts:

- UPP Data Governance team.
- UNSW IT support teams.

OCM: Shirley Ndelaphi

Controls & Compliance

Secure Baseline controls will be enforced across all UNSW IT-managed endpoints to align to the Cyber Security Policies and Standards. This project will:

- Develop and approve **Endpoint Security Baselines for UNSW IT-managed devices** (Win 10/11 & MacOS workstations).
- Implement the approved baselines for Win 10/11 & MacOS workstations using ICT Intune and JamF management tools.
- Develop a Service Management Plan to operationalise and embed this service.
- Develop an exemption request process.

Impacts:

- Staff with UNSW IT-managed devices.
- UNSW IT support teams.

→Learn more

- **Uplift management controls and compliance** by defining, with Cyber Security Governance & Risk, current requirements for metrics and compliance, and formalise regular reports under the current BAU capabilities utilising existing Intune and JAMF platforms.

Impacts:

- UNSW IT support teams.

OCM: Taylor Gorman