digital.nsw

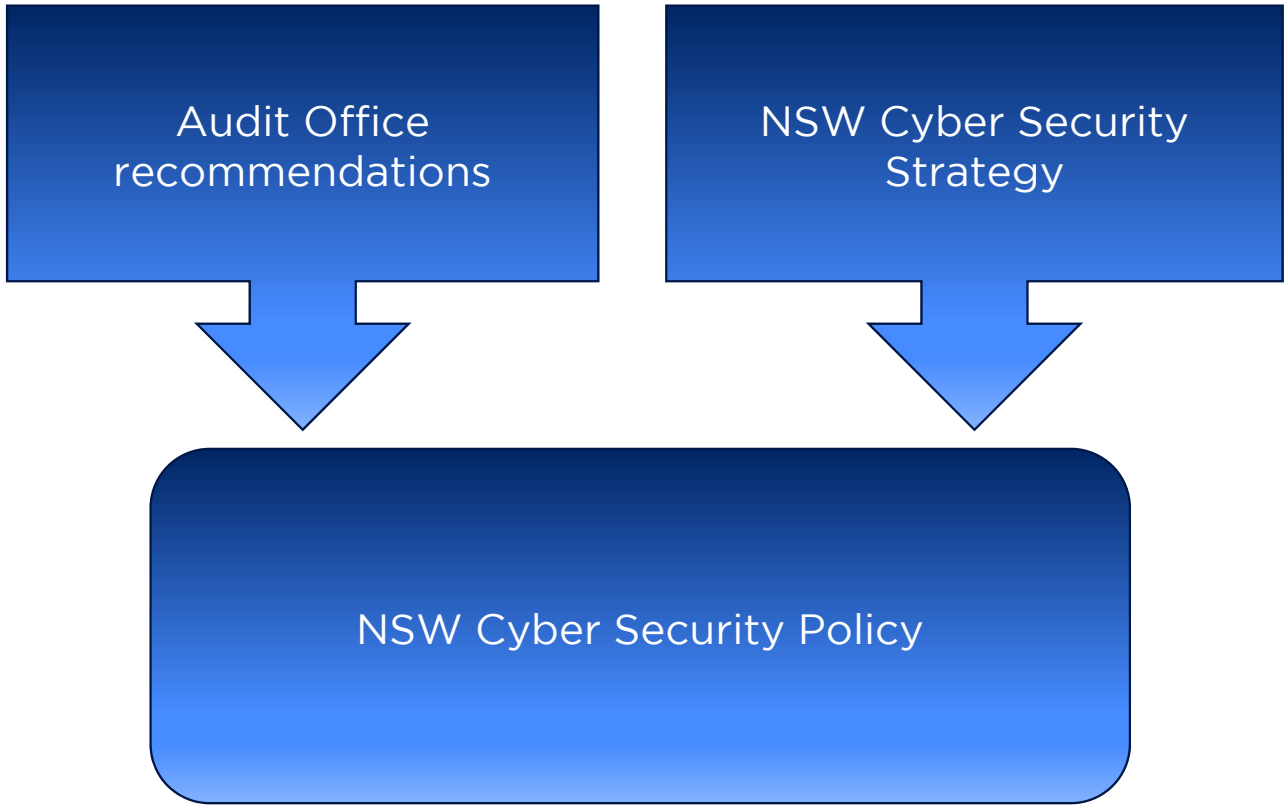
BUILDING OUR
DIGITAL FUTURE

NSW Cyber Security Policy

NSW Government Chief Information Security Officer

NSW GOVERNMENT

Cyber Security Policy: Enabling cyber uplift



NSW GOVERNMENT

An integrated approach to preventing and responding to cyber-security threats across NSW

secure • integrated • responsive • holistic.

digital.nsw
BUILDING OUR DIGITAL FUTURE

GCISO - value proposition

GCISO has four pillars, from which stem the primary functions and return on investment:

Annual Cyber Security Exercise Program

NSW Cyber Security Policy Implementation

Expanded Intelligence Capability

Cultural Uplift and Awareness Raising

NSW GOVERNMENT

An integrated approach to preventing and responding to cyber-security threats across NSW

secure • integrated • responsive • holistic.

digital.nsw
BUILDING OUR DIGITAL FUTURE

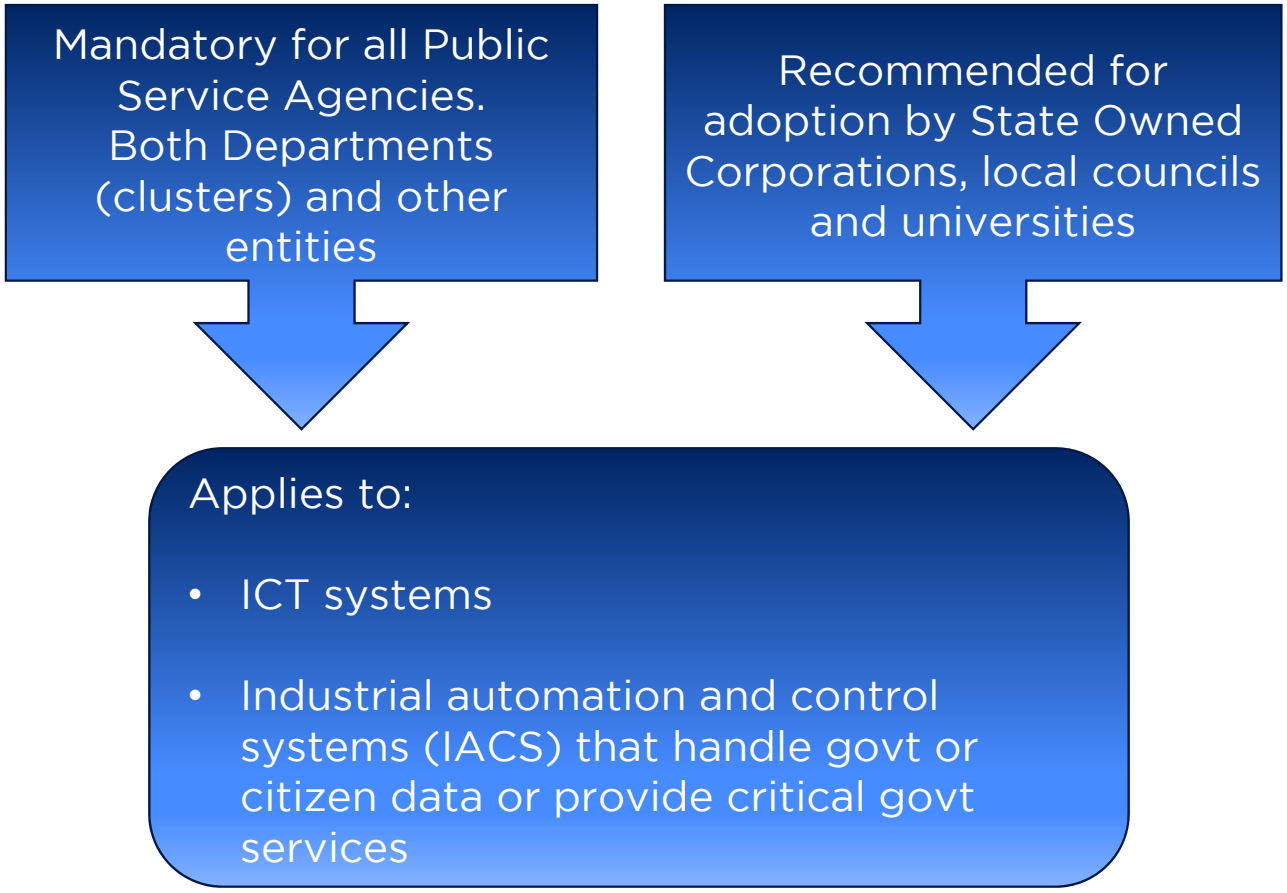
NSW Cyber Security Policy replaces the DISP

- Cyber Security Policy (2019) replaced the Digital Information Security Policy (2015).
- The CSP focuses on aligning NSW with the information requirements of the Federal *Protective Security Policy Framework.*
- The new policy calls out the need to protect Operational Technology.

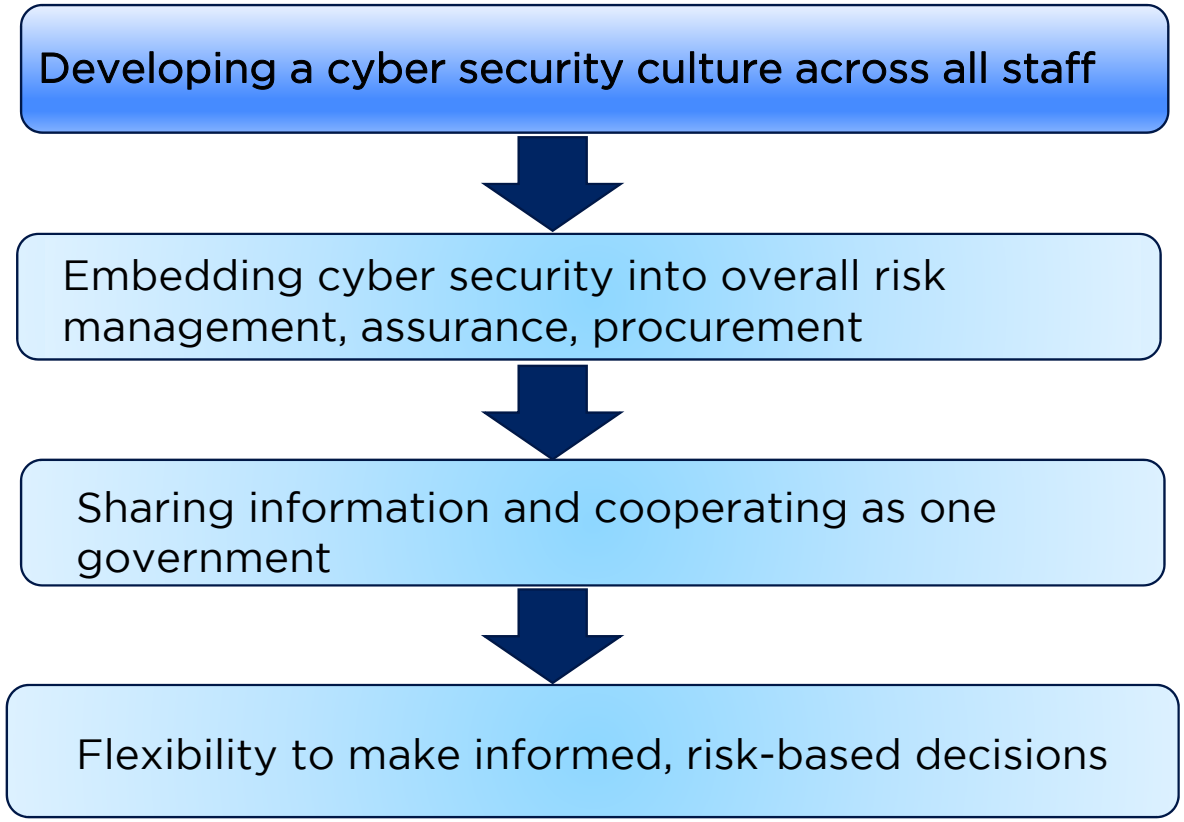
NSW Cyber Security Policy replaces the DISP

- It is now a requirement for agencies to have an approved cyber security plan integrated with BCP.
- Fosters a coordinated risk-based culture across all government agencies.
- Agencies must now identify their “crown jewels”.
- The CSP highlights that cyber security is everyone’s responsibility.

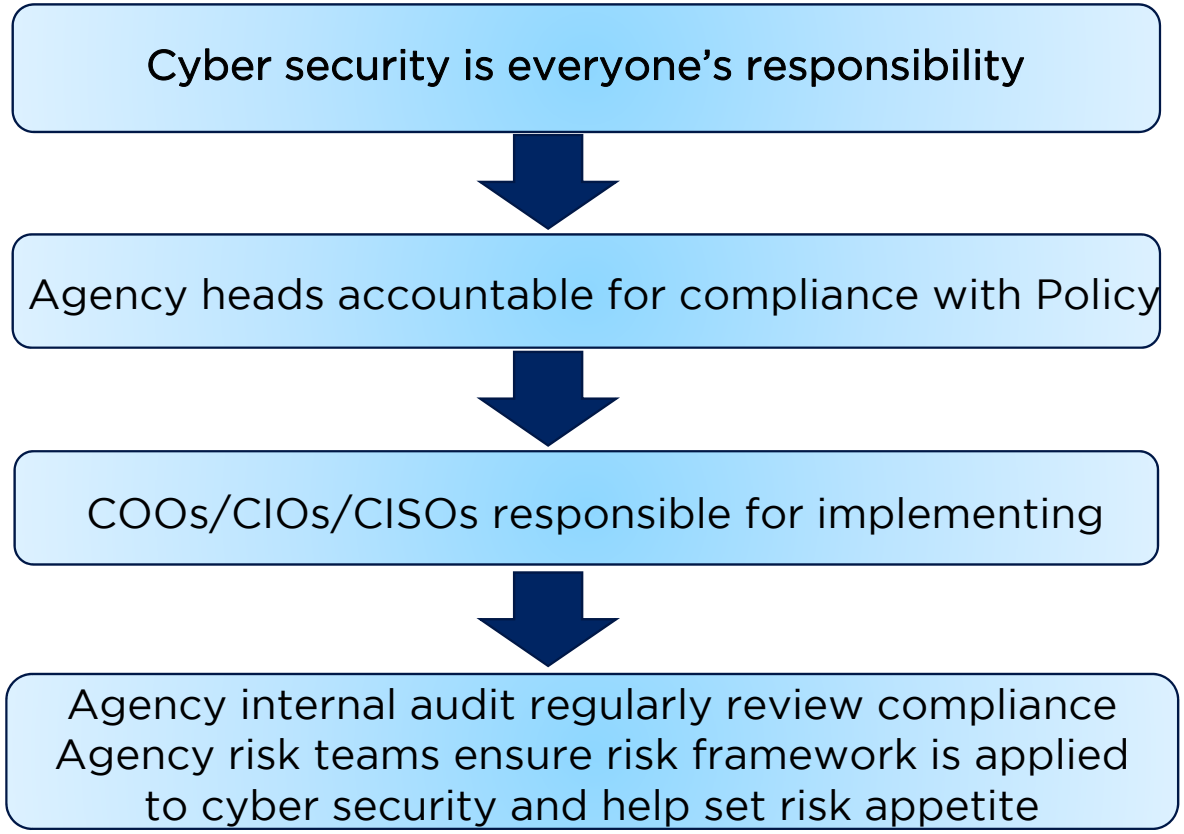
Scope of the Policy



New Emphasis on WoG Risk Management Culture



Roles and Responsibilities



digital.nsw

BUILDING OUR
DIGITAL FUTURE

Key Things to Know

New Reporting Requirements

NSW GOVERNMENT

Easy to use templates available for reporting requirements

1. 5 level **maturity assessment** against mandatory requirements
2. Maturity assessment against the ACSC Essential 8
3. List of agency crown jewels (most valuable or operationally vital systems or info)
4. List of cyber security risks with residual rating of high or extreme
5. Attestation for annual report

Scope to automate reporting in upcoming years

digital.nsw

BUILDING OUR
DIGITAL FUTURE

Mandatory Requirements

NSW GOVERNMENT

Section 1 – Planning and Governance

1. • Allocate roles and responsibilities
2. • Executive level governance committee covering cyber and including IACS
3. • Approved cyber security plan
4. • Conduct cyber security risk assessments
5. • Be accountable for cyber risks of your external service providers. Ensure they comply with policy.

Section 2 – Cyber Security Culture

1. Regular cyber security education for all staff and outsourced service providers
2. Increase awareness across all staff incl need to report. Run exercises such as simulations
3. Foster a culture where cyber security risk management is an important and valued part of decision-making
4. Access controls in place. Ensure people with access to sensitive or classified info or systems are appropriately screened
5. Share info on threats and intel with GCISO and cooperate with other agencies to manage govt-wide risk

Section 3 – Manage cyber security risks

1. Implement ISMS or CSMS compliant with ISO27001 (or ISA/IEC62443) and implement relevant controls. Annual certification, review or audit required.
2. Implement and report progress against ACSC Essential 8 (Note – no requirement to have fully achieved)
3. Classify info and systems according to their importance, assign ownership and identify crown jewels
4. Ensure cyber security requirements built into procurements and early in system development life cycle
5. Ensure new systems or enhancements include audit trails/activity logging for data integrity and internal fraud detection

Section 4 – Improved Resilience

1. Current cyber incident response plan integrated with agency incident plans and WoG cyber incident plan
2. Test cyber incident response plan annually and involve senior execs + functions + media/comms
3. Deploy monitoring tools for adequate incident identification + response
4. Report cyber security incidents to GCISO according to WoG incident response plan
5. Participate in WoG cyber security exercises as required

Section 5 – Reporting

1. Report annually to GCISO on compliance (31 August deadline)
2. Ensure cyber security risks with residual rating of high or extreme are reported to GCISO
3. Report annually to GCISO on your agency's crown jewels (most valuable or operationally vital systems/info)
4. Attest to cyber security measures in agency annual reports (and provide to GCISO)

Deadlines and Exceptions

- 31 August for all reporting requirements except annual report attestations

- **Exemptions** can be sought from GCIDO

NSW Cyber Security Policy: Next Steps

- Post-August CSP reporting deadline, review mandatory reporting process
- Develop CSP insights document and report to Secretary's Board and others on Cluster cyber maturity levels
- Input feedback and lessons-learned from reporting into revised CSP

digital.nsw

BUILDING OUR
DIGITAL FUTURE

Questions?

cybersecurity@finance.nsw.gov.au

NSW GOVERNMENT