ENSURING DATA INTEGRITY AND CONFIDENTIALITY:
CLOUD SECURITY BEST PRACTICES FOR AUSTRALIA'S PUBLIC SECTOR

Intermedium White Paper Sponsored by Kinetic IT

kinetic IT

EXECUTIVE SUMMARY

Greater threats, increased regulation, retaining citizen trust, questions of integrity: Australian government agencies face myriad risks while navigating the relatively unchartered territory that is the cloud.

The Australian public sector's transition into the cloud – whether public or hybrid - marks a major milestone in Australia's technology history. Spend on public cloud solutions is estimated to top **$23 billion** this year alone, while the government's **Data and Digital Government Strategy** puts the public sector on a pathway to leverage cloud solutions to achieve greater citizen engagement and satisfaction. But with this revolution comes added and unique complexities as agencies aim to manage data responsibly and securely. At the same time, cyber threats are escalating, budgets are being cut but the expectation that the public service maintains contemporary and rapid response approaches to risk while managing these complexities has skyrocketed.

This is where proactively selecting a secure by design, robust and sovereign solution from the get-go will make a significant difference: You must start as you mean to go along. Ensuring Data Integrity and Confidentiality: Cloud Security Best Practices for Australia's Public Sector, prepared by Intermedium and sponsored by Kinetic IT, is dedicated to exploring essential strategies and best practices tailored specifically to address the unique challenges faced by Australian government agencies.

Aligned with the **Australian Cyber Security Strategy 2023-2030**, this white paper outlines key problems and trusted best practice solutions to deliver the Australian Public Sector a comprehensive roadmap to cloud security, and therefore a more cyber resilient nation. It introduces eight best practices distilled from both governmental and industry standards, designed to enhance data security in diverse cloud environments.

Highlighted within this report is the key role of secure cloud technologies in delivering scalable, adaptive, and citizen-centric services, and how government can best manage the increased volume of sensitive data it now holds as part of Australia's rapid digitisation of citizen services. It delves into the critical issue of data integrity and confidentiality in the cloud era and how it is incumbent on the public sector to proactively respond with best practice approaches to ensure data integrity and confidentiality is upheld. The report also provides guidance within the context of the escalating frequency and sophistication of cyber-attacks that Australia has faced in recent years.

Addressing the intersection of technological innovation, regulatory compliance with operational imperatives, Kinetic IT's white paper equips government leaders with actionable insights to navigate the complexities of cloudsecurity. In engaging with this white paper, those in the public sector can ensure confidence and integrity in its management of citizen data while advancing Australia's digital transformation agenda.

BACK TO TOP

INTRODUCTION

Data is the lifeblood of agency operations, but managing it can be a major source of risk for government executives. This is where cloud products and services can provide upfront, robust security measures – better than internal IT teams.

The digitisation of citizen services, to improve the customer experience and optimise the use of resources, has led to agencies amassing an unprecedented volume of data, including highly sensitive personal information. Criminal and nation-state actors are using a variety of malicious methods to gain access to this data, resulting in a rising number of data breaches.

> **19% increase in data breach reports from January-June to July-December 2023 – Office of the Australian Information Commissioner, *Notifiable Data Breaches Report* [1]**

Data breaches have major consequences. They can jeopardise citizen privacy, reduce trust in government, and tarnish an agency's reputation.[2] They can impact citizen safety by exposing a private address, lead to identity theft and financial loss, derail government work, and undermine professional relationships.[3]

> **"Harm to individuals as a result of a data breach can be physical, financial, emotional or reputational." – Office of the Victorian Information Commissioner, *Managing the Privacy Impacts of a Data Breach*[4]**

Agency executives face several challenges when managing the threat of data breach or manipulation to safeguard data integrity and confidentiality. They must oversee increasingly complicated information technology environments, deal with skills shortages and resource constraints, and constantly remind staff about the need for cyber hygiene.

BACK TO TOP

Cloud products and services allow agencies to overcome some of these challenges and benefit from the cloud's rapid infrastructure provisioning, flexibility and reliability.[5] Cloud-based services can also provide security benefits.

According to the Digital Transformation Agency, "Cloud providers often implement and manage better IT security controls than internal IT teams as it is a core part of their business and reputation." [6]

As more data and workloads move to cloud environments, so does the focus of adversaries. Cyber security solution provider CrowdStrike observed a 75 per cent increase in cloud intrusions between 2022 and 2023 across its clients.[7]

> **75 per cent increase in cloud intrusions (2022 to 2023) – CrowdStrike *Global Threat Report 2024*[8]**

Agencies must consider the unique characteristics and risks of cloud environments in their cyber security strategy.

Even though cloud services reduce or eliminate agency infrastructure workloads, agencies continue to have responsibility for data and security in several areas under a 'shared responsibility model' between agencies and their cloud provider. These responsibilities include data management, identity and access management, and network and firewall configuration.[9]

This white paper outlines eight cloud security best practices, which if addressed, will significantly enhance citizen data safety, integrity and confidentiality.

The eight best practices are drawn from the cyber security risk reduction policies and guidance issued by governments at the Federal, State and Territory level and by industry.

Government-issued guidance referenced includes the Australian Cyber Security Centre's (ACSC's) *Cloud Computing Security for Tenants*[10] and *Information Security Manual (ISM).*[11]

BACK TO TOP

BACK TO TOP

SECURING DATA DURING A PERFECT STORM

A perfect storm of external risks and internal challenges is making data security more difficult than ever for agencies.

Fortunately, new technologies and methods to protect data assets are emerging too, allowing agencies to reduce risk with an innovative culture.

CHALLENGE	DESCRIPTION	EVIDENCE
The 'data deluge'	The volume, variety and sensitivity of data for agencies to secure is increasing with digital services.	Annual global data will double between 2022 and 2026.[14]
Increasing frequency and sophistication of cyber attacks	Typical methods used by adversaries include gaining initial access via valid accounts, conducting privilege escalation by exploiting stolen credentials or misconfigurations and moving laterally through the environment to access sensitive data.[15]	CrowdStrike observed a 3x increase in adversaries targeting cloud environments from 2021 to 2022.[16]
Widening attack surface	Agency work is often decentralised, widening the attack surface.	In 2022, 55% of Australian Public Sector employees worked from home at least partially.[17]
Poor cyber hygiene	Poor cyber hygiene among agency personnel opens opportunities for potential adversaries, including bad password practices.	Audits repeatedly show evidence of poor cyber hygiene.[18]
Resource constraints and skills shortages	Agency executives are under pressure to reduce costs. Economy-wide cyber security skills shortages further restrict access to capability.[19]	Six cyber security roles are in national shortage, according to the 2023 Australian Government Skills Priority List.[20]
Reliance on legacy systems	Agencies rely on multiple generations of technology to perform business functions.	Legacy systems may be unsupported, labour-intensive and lack basic security protections. [21]

BACK TO TOP

CLOUD SECURITY BEST PRACTICES

KEY FOCUS 1

CHALLENGE

Establish comprehensive monitoring and visibility of cloud risks across the agency

Many agencies now operate a multi-cloud environment, storing citizen data with multiple Cloud Service Providres (CSPs).. To do this safely requires an enterprise-wide view to identify and remedy cyber security risks (including misconfigured security settings) covering multiple cloud and on-prem environments.

SOLUTIONS

IDENTIFY THE 'CROWN JEWELS'

Not all systems and data are equal – agencies must identify business-critical and sensitive data (the 'crown jewels') and apply appropriate protections. The Australian Government is currently reviewing its sensitive and critical datasets to determine if its current storage and protections are risk-appropriate.[22] Agencies can identify their 'crown jewels' by considering the business, regulatory and reputational impact of system damage or data leakage.

DEVELOP ENTERPRISE-WIDE MONITORING AND VISIBILITY

Technologies including machine learning, global networks of threat intelligence telemetry and network traffic monitoring solutions can now be leveraged to establish whole-of-enterprise observability, encompassing legacy solutions. To be effective, monitoring must: operate continuously; and become aware of and take appropriate action on new cloud instances, accounts, credentials, and modifications to configuration settings.

In addition to security benefits, observability solutions can support agencies in identifying unnecessary resource usage and issues that could affect customer experience.

Agencies should also establish a register of outsourced cloud services being used by the agency, with service details, sensitivity or classification of data involved, and 24/7 contact details.[23]

DO NOT SPIN UP AND FORGET CLOUD INFRASTRUCTURE

A major advantage of the cloud is its responsiveness to agency business requirements. A new instance or service can be quickly 'spun' up. However, agency teams must remain vigilant and not neglect cloud infrastructure once it is no longer required, as neglecting ongoing security management introduces major risks, especially for Infrastructure as a Service (IaaS) arrangements where the agency may be responsible for patching. All applications and workloads must receive security management until they are decommissioned.[24]

Example KPIs

- Measure the percentage of systems subject to monitoring compared to the agency's total number of systems
- Measure the number of true positive detections of threats versus false positives and false negatives
- Measure the percentage of systems up to date with patching

BACK TO TOP

KEY FOCUS 2

CHALLENGE

Pursue a unified approach to cloud security

Government operations are often highly siloed, with agencies, business units and teams working independently.

Having a well-defined governance model is therefore vital for protecting data integrity and confidentiality in cloud environments.

SOLUTIONS

ESTABLISH DISTINCT RESPONSIBILITIES FOR DATA SECURITY

Adversaries only need a single valid account to enter a cloud-based system that holds sensitive data, so cloud security should be treated as an agency-wide effort where every employee has a role to play.

The ACSC Information Security Manual (ISM) singles out two roles vital for establishing responsibility and accountability in an agency's cyber security posture: the Chief Information Security Officer (CISO) and a system owner for each cloud-based product or service.

The CISO leads and coordinates the agency's cyber security program. This program should include applying controls, reporting, incident response, communication, business continuity planning, working with suppliers, budget management, overseeing personnel, and awareness raising.[25]

The system owner is responsible for defining the system; selecting, implementing and assessing controls; and authorising and monitoring the system.[26]

COLLABORATE WITH THE WHOLE OF GOVERNMENT (WOFG) CYBER SECURITY AGENCY

All jurisdictions fund a WofG cyber security function to help agencies improve their cyber security. These units offer guidance material, training, emergency support and technical support (e.g. vulnerability assessments, ACSC Essential Eight gap analysis, and Active Directory password reviews).

OPT FOR SHARED PLATFORMS

Across Australia, agencies are increasingly being encouraged to adopt cloud-based, shared platforms to realise the benefits of WofG architectures. Such WofG platforms will ultimately rationalise the number of systems in use to perform essentially the same function and reduce the challenge of keeping plural systems secure, particularly if these systems duplicate data.

Example KPIs

- Measure agency compliance with WofG cyber security policies, standards and guidelines (e.g. ISM, WofG architecture policies)
- Measure the percentage of common platforms used versus proprietary or bespoke systems

BACK TO TOP

KEY FOCUS 3

CHALLENGE

Ensure that cloud service providers meet security standards

Not all cloud-based systems are secure or trustworthy. In May 2022, Human Rights Watch published research stating that 90% of 164 common EdTech apps engaged in unethical data practices, including practices that put children's data at risk of breach.[27]

SOLUTIONS

Only select suppliers engaged in cloud assessment programs

Agencies can reduce security risk by selecting suppliers who understand the cyber security regulatory ecosystem in Australia and participate in government assessment programs such as the Infosec Registered Assessors Program (IRAP).

IRAP assessments demonstrate that providers have instituted processes to manage critical risks. These processes include security governance, incident response, use of cryptographic controls, security clearances, and multi-tenancy mechanisms to prevent unauthorised access.

The ISM states that CSPs should undergo assessment every 24 months.[28]

CSPs publish regular updates on newly assessed services. For example, Amazon Web Services publishes IRAP reports every six months detailing services having undergone assessment.[29]

Data with specific security classifications (e.g. protected, secret, top secret) have different storage rules. Federal Government agencies are only permitted to store secret and top secret data on a private cloud.[30]

Specify cloud security requirements of CSPs in contracts

Agencies must ensure that data ownership, confidentiality, integrity and availability requirements are documented in their contracts with suppliers. Contracts should also permit agencies to verify compliance with these requirements.

Example KPIs

- Measure how up-to-date suppliers are with IRAP assessments
- Measure supplier compliance with contract terms (e.g. availability, incident response time (including notification of a data breach))

BACK TO TOP

KEY FOCUS 4

CHALLENGE

Deploy robust endpoint protection

Agencies struggle against low employee cyber security hygiene (poor passwords, lack of phishing awareness, etc.).[31] As remote work practices have destroyed the notion that agencies can 'secure the perimeter', training programs for cyber hygiene need to be accompanied by investments in technologies that protect the endpoint.

SOLUTIONS

Implement behavioural-based security practices

Adversaries' methods include gaining entry to environments through remote monitoring and management tools. Once in, they escalate privileges and deploy ransomware or steal data.[32] Other methods include stealing session cookies from a user's browser to authenticate and access services.[33]

Agencies must therefore ensure that endpoint protection solutions utilise behavioural-based detection and automated threat response. Behavioural-based security uses deviations from normal activity to trigger a response. For example, the system will notice that a user is attempting to gain access to the cloud environment from an atypical location or is attempting to access data that they have not been authorised to access.

Contemporary solutions can also spot and stop phishing attempts and automatically quarantine risky files while investigating a threat.

Protect against the insider (staff) threat

Insider threats, motivated by financial gain, espionage or revenge are an ongoing challenge.[34] Behavioural-based security practices should be used to identify unusual activity within an agency's cloud environment, for example, excessive copying or modifying of files, connection of devices capable of data storage, and system use outside business hours.[35]

Example KPIs

- Measure the percentage of true positive threat detections on endpoints versus false positives and false negatives
- Measure the percentage of endpoints protected
- Measure the average time to detect and resolve a threat
- Measure user satisfaction
- Measure threat intelligence, update frequency to protect against the latest threats

BACK TO TOP

KEY FOCUS 5

CHALLENGE

Apply a zero-trust approach to Identity and Access Management

Under the zero-trust approach, no user is trusted, and agencies operate as if their system may have already been breached.[36]

A zero-trust approach to Identity and Access Management involves restricting user access to the data essential to their role and requiring them to verify access at key points as they navigate the cloud system.[37]

Adversaries utilise stolen credentials, weak passwords, and overly permissive access controls to access systems and then potentially move further into business systems.

> **43% of cloud intrusions observed by CrowdStrike in 2022 involved adversaries using valid accounts. – *CrowdStrike, 2023 Cloud Risk Report*** [38]

Example KPIs

- Measure the frequency of access rights reviews
- Measure the percentage of overprivileged accounts
- Measure the percentage of users with admin privileges
- Measure the percentage of accounts that have implemented MFA

SOLUTIONS

Adopt the 'principle of least privilege'

Excessive account permissions open agencies up to data theft/destruction.[39] For example, an adversary able to secure administrator privileges may be able to review and revoke security keys and passwords, transfer ownership of files, and manage access settings for other users.

Restricting user access to only what is necessary for their work involves:

1. Identifying tasks and data needing access privileges
2. Identifying the personnel required to access that data or complete those tasks
3. Permitting access for those privileges only
4. Regularly reviewing whether the situation has changed and if so, removing privileges[40]

Under the 'principle of least privilege' even an agency secretary or chief executive will not have access to all areas of a cloud system if they do not need such access for their role.

Agencies should also incorporate risk-based conditional access into their Identity and Access Management policies, whereby a user trying to enter a cloud-based system may be given additional access procedures like multi-factor authentication if deemed high risk based on characteristics such as the device being used or the geographic location of the attempted access.

Enforcing session times may also reduce the damage of a successful attack by kicking an adversary out before they achieve their goal.

Agencies should also ensure that detailed logs are kept of account access, with automated alerts for suspicious activity to enable rapid threat response and containment.[41]

Implement multi-factor authentication

Multi-factor authentication (MFA) – one of the ACSC's *Essential Eight*[42] – provides additional security by requiring users to provide multiple forms of verification before gaining access. MFA protects against adversaries who have stolen just a single form of verification (e.g. password).

Agencies should use risk-based conditional access and continuous monitoring to trigger MFA or reauthentication with MFA if a suspicious activity takes place.

> **94% of user accounts in audited Victorian Government agencies did not have MFA enabled – Victorian Auditor-General's Office, 2023 cloud security audit** [43]

BACK TO TOP

BACK TO TOP

BACK TO TOP

KEY FOCUS 6

CHALLENGE

Minimise damage if an incursion occurs

Despite agency efforts to protect data and digital systems, data breaches are going to occur.

Accurate data is vital for evidence-based decision-making. Even the fear that data is compromised inhibits the government's ability to operate effectively because it ruins confidence in the integrity of data assets.

SOLUTIONS

Prioritise information management

> "Agencies… create and keep [data] in a variety of locations, onsite and cloud-based, using many formats, applications and systems." – National Archives of Australia, *Building Trust in the Public Record*[44]

Agencies suffering from data sprawl across various systems risk data duplication, prolonged retention of unnecessary data, concerns over data integrity and heightened data storage costs. The unnecessary storage of personal and other sensitive data increases the risk of breaches, potentially compromising confidentiality.

Agencies must therefore manage data according to jurisdictional information management standards[45] to improve information discovery and bolster data integrity and security. Automation tools can assist agencies in correctly classifying data to ensure that the appropriate protections are applied.

Secure data transmission with encryption

As agencies can never entirely protect against data breaches, they must reduce the value of the data for adversaries if it is leaked. 'At rest' data encryption within cloud-based systems and in transit to and from those systems can reduce the damage of data breaches if adversaries do not have encryption keys. The Australian Signals Directorate provides approved encryption algorithms for data classified as protected level and below.[46]

Agencies (like suppliers) must be aware of emerging methods to crack encrypted data – for example, adversaries using cloud computing for brute force attacks.

Implement and validate an incident response plan

Incident response plans are now WofG policy in all jurisdictions. Best practice incident response plans[47] cover roles and responsibilities, reporting and communication processes, and end-to-end incident management procedures (from planning and preparation to lessons learned).

Agencies should also take advantage of any 'playbooks' developed by the WofG cyber security entity to deal with specific response and recovery scenarios.

Incident response plans should include mechanisms to support those affected by data breaches. For example, many Australian jurisdictions now support the not-for-profit IDCARE service which helps victims of identity theft.[48]

A similar program run by the NSW Government (ID Support NSW) alerts citizens when their personal information is found on the dark web, in addition to helping citizens who have experienced the loss or theft of their government proof of identity credentials.[49]

Opt for automated backup and recovery processes

Agencies should conduct automated backups as often as business continuity requirements dictate. Access should be protected by MFA and comply with the 'principle of least privilege'. For example, only permit backup administration accounts to access, modify and delete backups.[50] Contracts with cloud providers must guarantee data can be migrated and backed up without data loss.[51]

Data analysis tools can scan backed-up data for evidence of compromise, for example by looking out for new or modified files that could suggest malware.

Example KPIs

- Measure the accuracy of data classification
- Measure agency compliance with WofG information management policies, standards and guidelines
- Measure the amount of sensitive data encrypted
- Measure how often the incident response plan is tested and revised
- Measure the average time to detect and respond to an intrusion or problem
- Measure the average time to recover after a system failure

BACK TO TOP

KEY FOCUS 7

CHALLENGE

Maximise the value of agency cyber security investments

Australian governments have significantly increased levels of funding for cyber security, especially since the start of the COVID-19 pandemic. These initiatives aim to establish or improve shared cyber security services, whether at the WofG level or within specialised 'cyber security hubs' that cater to a collection of agencies, as well as to enhance the capabilities of individual agencies.[52]

However, the threat posed by adversaries means that agencies never have 'sufficient' resources and must continually optimise the use of resources.

SOLUTIONS

Harness threat intelligence for a risk management strategy

> "Organizations spend years and millions of dollars fighting ghosts and noisy alerts, never knowing the 'who, why and how' behind the [53]attacks." – CrowdStrike, *2023 Global Threat Report*

By investing in threat intelligence, agencies can target investment in high-risk areas. Adversaries frequently gain access to cloud-based systems by exploiting critical misconfigurations, often in identity and access management, according to threat intelligence.

Automate threat detection and response

Agencies can implement managed detection and response services to streamline manual processes and alleviate the burden on in-house cyber security personnel. These solutions leverage worldwide threat intelligence resources, provide round-the-clock operations, and automate processes (for example, vulnerability scanning and behavioural-based detection and response activities).

Reduce duplicated and bespoke systems

Agencies can reduce reliance on duplicated point solutions and bespoke configurations by adopting comprehensive data security offerings. Leading cyber security solutions typically support integration with core government platforms, including Security Incident and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms.

Many cloud services used by agencies today are likely to have security features that are not being used effectively. Greater collaboration with suppliers and employee training may be more effective uses of resources than adopting new systems.

Example KPIs

- Measure the percentage of manual processes that have been successfully automated
- Measure the cost savings achieved by using a common platform versus proprietary or bespoke systems

BACK TO TOP

KEY FOCUS 8

CHALLENGE

Incorporate cloud-focused training into cyber security programs

Agencies often struggle to embed cyber security awareness and comply with basic cyber hygiene obligations, according to several audit reports. Adversaries rely on exploiting these preventable exposures to access cloud systems and citizen data.

SOLUTIONS

Prioritise training for agency-specific risk

Cyber security training for all staff is an essential safeguard against evolving threats.

Penetration testing is vital for identifying vulnerabilities. It should be conducted before system deployment and at least annually as part of a continuous monitoring plan, according to the ISM[54], and should continuously inform end-user awareness training.

Some WofG cyber security agencies provide awareness training materials with real-world examples of relevance to their agency peers.

Adapt training to specific roles across the agency

In addition to general awareness training, agencies should conduct role-based training, including for executives and contractors. Cyber security training for users with privileged access is critical, given they have access to sensitive data and systems, demanding specialised knowledge and unwavering vigilance. The ISM states that privileged user training be undertaken annually.[55]

Example KPIs

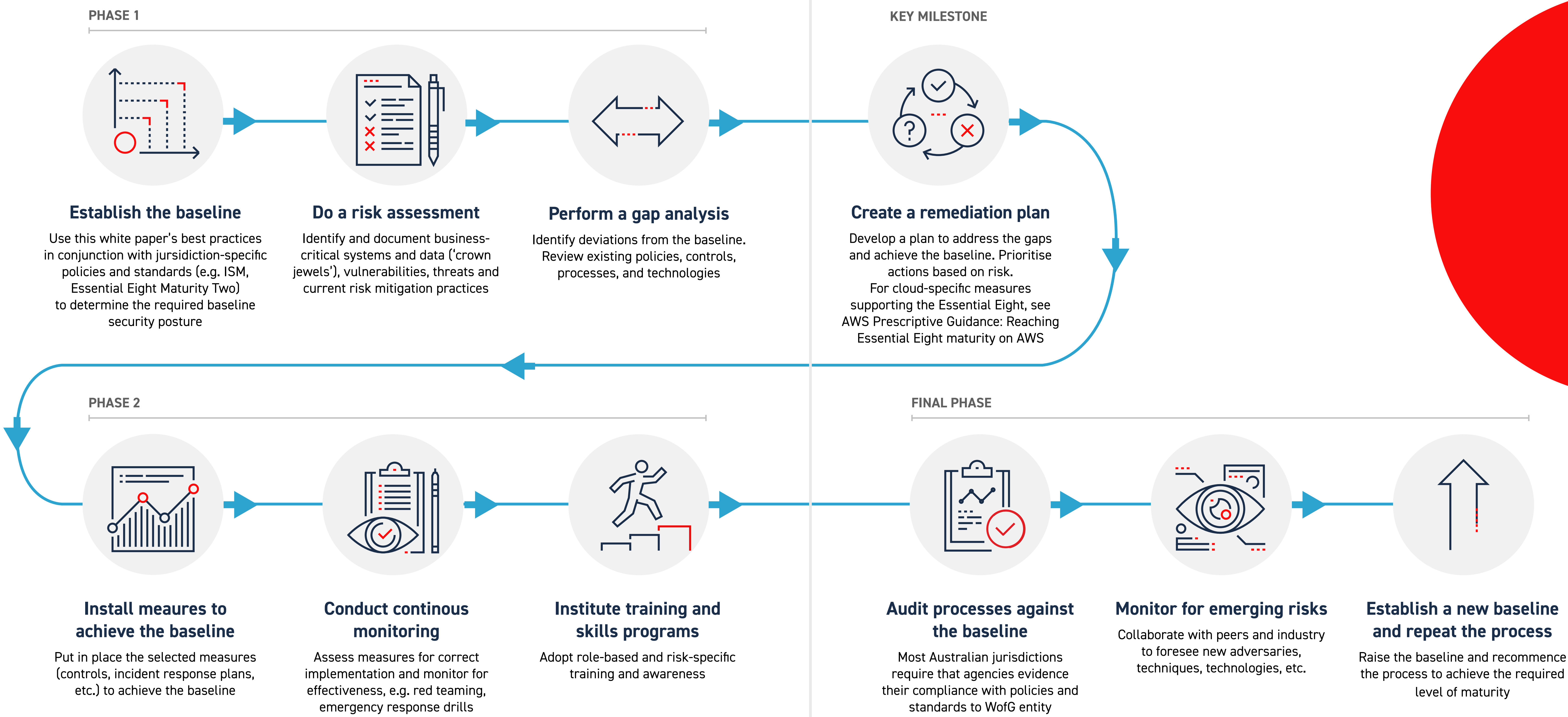
- Measure the percentage of employees who have participated in general awareness training and exercises
- Measure the percentage of employees who have participated in role-specific training (e.g. executives, privileged users)
- Measure changes in employee behaviour (e.g. click-through rates on phishing emails)

BACK TO TOP

BACK TO TOP

HOW TO IMPLEMENT CHANGE

The below steps have been synthesised and modified by Intermedium using various sources, including the NIST Risk Management Framework.[56]



PHASE 1

Establish the baseline

Use this white paper's best practices in conjunction with jursidiction-specific policies and standards (e.g. ISM, Essential Eight Maturity Two) to determine the required baseline security posture

Do a risk assessment

Identify and document business-critical systems and data ('crown jewels'), vulnerabilities, threats and current risk mitigation practices

Perform a gap analysis

Identify deviations from the baseline. Review existing policies, controls, processes, and technologies

KEY MILESTONE

Create a remediation plan

Develop a plan to address the gaps and achieve the baseline. Prioritise actions based on risk.
For cloud-specific measures supporting the Essential Eight, see AWS Prescriptive Guidance: Reaching Essential Eight maturity on AWS

PHASE 2

Install meares to achieve the baseline

Put in place the selected measures (controls, incident response plans, etc.) to achieve the baseline

Conduct continous monitoring

Assess measures for correct implementation and monitor for effectiveness, e.g. red teaming, emergency response drills

Institute training and skills programs

Adopt role-based and risk-specific training and awareness

FINAL PHASE

Audit processes against the baseline

Most Australian jurisdictions require that agencies evidence their compliance with policies and standards to WofG entity

Monitor for emerging risks

Collaborate with peers and industry to foresee new adversaries, techniques, technologies, etc.

Establish a new baseline and repeat the process

Raise the baseline and recommence the process to achieve the required level of maturity

BACK TO TOP

BACK TO TOP

CONCLUSION

As the 2023-2030 Australian Cyber Security Strategy notes, "Enduring and low levels of cyber maturity across many Australian Government entities have revealed major gaps in our security posture."[57]

> **"To uplift our collective cyber security, the Government must itself adopt cyber best practices..." – *2023-2030 Australian Cyber Security Strategy*** [58]

This white paper collated and summarised cloud security best practices from government and industry sources which, if implemented, can immediately strengthen the protection of data held by agencies, supporting data integrity and confidentiality. It also provided several key performance indicators and steps to support the journey.

The pressure to speed up cloud security action is rising as more business-critical workloads and sensitive data are processed and stored in cloud environments, while adversaries simultaneously capitalise on new technologies, exploit unaddressed vulnerabilities, and develop new methods to breach cloud-based systems.

> **"The Australian Government will deliver simple, secure and connected public services..." – Australian Government *Data and Digital Strategy* 2030 vision**[59]

Agencies cannot provide simple, secure and connected public services without prioritising cloud security, as citizens will not trust and engage with digital services if agencies are subject to frequent data breaches. Nor will agency leaders be confident in sharing data across jurisdictional boundaries to provide connected services.

Fortunately, agencies do not need to feel 'on the back foot' when it comes to cloud security. The following 'next steps' are intended to help agencies take immediate action to strengthen the protection of data and support data integrity and confidentiality.

BACK TO TOP

NEXT STEPS

1. Conduct a quick cloud security assessment

- Consider the extent to which the cloud security best practices have been instituted in your agency. See below.

Best Practice Checklist

BEST PRACTICE	CHECKLIST
Establish comprehensive monitoring and visibility of cloud risks across the agency	✓ Develop and maintain a list of the 'crown jewels' ✓ Develop enterprise-wide monitoring and visibility ✓ Monitor infrastructure so staff do not spin up and forget cloud infrastructure
Pursue a unified approach to cloud security	✓ Establish distinct responsibilities for data security ✓ Collaborate with the WofG cyber security agency ✓ Opt for shared platforms
Ensure that cloud service providers meet security standards	✓ Only select suppliers engaged in cloud assessment programs ✓ Specify cloud security requirements of CSPs in contracts
Deploy robust endpoint protection	✓ Implement behavioural-based security practices ✓ Protect against the insider (staff) threat
Apply a zero-trust approach to Identity and Access Management	✓ Adopt the 'principle of least privilege' ✓ Implement multi-factor authentication
Minimise damage if an incursion occurs	✓ Prioritise information management ✓ Secure data transmission with encryption ✓ Implement and validate an incident response plan ✓ Opt for automated backup and recovery processes
Maximise the value of agency cyber security investments	✓ Harness threat intelligence for a risk management strategy ✓ Automate threat detection and response ✓ Reduce duplicated and bespoke systems
Incorporate cloud-focused training into cyber security programs	✓ Prioritise training for agency-specific risk ✓ Adapt training to specific roles across the agency

2. Determine if external assistance is required

- Refer to the 'Steps for implementing change' section on page 18 and 19 to determine if and how external assistance is required to achieve the baseline.

3. Consult

- Consult with the WofG cyber security entity and industry leaders for support to prepare for and implement the required changes.

BACK TO TOP

KEY TAKEAWAYS

Rising Threat Landscape:

There has been a significant increase in cyber-attacks targeting cloud environments, necessitating stronger security measures.

Shared Responsibility Model:

Agencies must understand their responsibilities within the shared responsibility model of cloud security, which includes data management and Identity and Access Management.

Comprehensive Monitoring:

Establishing enterprise-wide monitoring and visibility is crucial for identifying and mitigating cyber risks across all cloud and on-premises environments.

Unified Security Approach:

A well-defined governance model and collaboration with Whole of Government (WofG) cyber security agencies are vital for effective cloud security.

Robust Endpoint Protection:

Agencies need to invest in behavioural-based security practices and technologies to protect against sophisticated cyber threats.

Zero-Trust Identity and Access Management:

Implementing a zero-trust approach to restrict access and enforce multi-factor authentication can significantly reduce the risk of unauthorised access.

Data Management and Encryption:

Proper data management practices, including encryption and compliance with information management standards, are essential to protect data integrity and confidentiality.

Incident Response and Recovery:

Developing and regularly testing incident response plans, along with automated backup and recovery processes, are critical for minimizing the impact of data breaches.

Optimizing Cyber Security Investments:

Agencies should leverage threat intelligence, automate threat detection and response, and prioritise training to enhance their cyber security posture and maximise the value of their investments.

BACK TO TOP

BACK TO TOP

ENDNOTES

1 Australian Government, 2024, **Notifiable data breaches report July to December 2023**
2 Victorian Government, accessed November 2023, **Managing the Privacy Impacts of a Data Breach**
3 NSW Government, 2020, **Data Breach Guidance for NSW Agencies**
4 Victorian Government, accessed November 2023, **Managing the Privacy Impacts of a Data Breach**
5 Australian Government, 2021, **Secure Cloud Strategy [PDF]**
6 Australian Government, 2021, **Secure Cloud Strategy [PDF]**
7 CrowdStrike, 2024, **Global Threat Report**
8 CrowdStrike, 2024, **Global Threat Report**
9 AWS, accessed December 2023, Shared Responsibility Model
10 Australian Government, accessed November 2023, Cloud Computing Security for Tenants
11 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
12 CrowdStrike, 2023, 2023 Cloud Risk Report
13 AWS, accessed November 2023, Reaching Essential Eight maturity on AWS: AWS Prescriptive Guidance
14 IDC, 2022, **High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises [PDF]**
15 CrowdStrike, 2023, **2023 Cloud Risk Report**
16 CrowdStrike, accessed November 2023, **Global Threat Report**
17 Australian Government, 2022, State of the Service Report [PDF]
18 See, for example, Cameron Sinclair, Intermedium, November 2021, Addressing NSW's cyber security failings – the state of play
19 Australian Government, accessed November 2023, **Skills Priority List**
20 Australian Government, accessed March 2024, **Skills Priority List**
21 Victorian Government, accessed November 2023, Risk scenario 2 – Legacy systems case study
22 Australian Government, 2023, 2023–2030 **Australian Cyber Security Strategy [PDF]**
23 Australian Government, accessed November 2023, Information Security Manual (ISM)
24 CrowdStrike, 2023, 2023 Cloud Risk Report
25 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
26 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
27 Human Rights Watch, 2022, **"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic**
28 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
29 AWS, accessed November 2023, **2023 H1 IRAP report is now available on AWS Artifact for Australian customers**
30 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
31 Australian Government, accessed November 2023, **Insights: Audit Lessons Cyber Security**
32 CrowdStrike, 2023, **2023 Cloud Risk Report**
33 CrowdStrike, 2023, **2023 Cloud Risk Report**
34 Tory Shepherd, The Guardian, September 2022, **Insider cyber threats pose 'significant' risk to Australia's defence force, brief warns**
35 Australian Government, 2023, **Countering The Insider Threat: A guide for Australian Government [PDF]**
36 Paul Wagenseil, SC Media, 2022, **How identity and access management fits into zero trust**
37 AWS, accessed November 2023, **Reaching Essential Eight maturity on AWS: AWS Prescriptive Guidance**
38 CrowdStrike, 2023, **2023 Cloud Risk Report**
39 CrowdStrike, 2023, **2023 Cloud Risk Report**
40 Australian Government, accessed November 2023, **Restricting Administrative Privileges**
41 Australian Government, accessed November 2023, **Cloud Computing Security for Tenants**
42 Australian Government, accessed November 2023, Essential Eight Explained
43 Victorian Government, VAGO, 2023, **Cybersecurity: Cloud Computing Products**
44 Australian Government, 2023, **Building trust in the public record**
45 For example, Australian Government, accessed November 2023, **Information Management Standard for Australian Government**
46 Australian Government, accessed November 2023, **Guidelines for Cryptography**
47 See, for example, Australian Government, 2023, **Cyber Incident Response Plan Guidance [PDF]** and Queensland Government, 2018, **Incident management guideline**
48 IDCARE, accessed November 2023, **What is IDCARE**
49 NSW Government, accessed November 2023, **ID Support NSW**
50 Australian Government, accessed November 2023, **Cloud Computing Security for Tenants**
51 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
52 Intermedium, 2022, **Government Cyber Security Readiness Indicator**
53 CrowdStrike, 2023, **2023 Global Threat Report**
54 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
55 Australian Government, accessed November 2023, **Information Security Manual (ISM)**
56 Australian Government, 2023, **2023-2030 Australian Cyber Security Strategy [PDF]**
57 Australian Government, 2023, **2023-2030 Australian Cyber Security Strategy [PDF]**
58 Australian Government, 2023, **Data and Digital Government Strategy [PDF]**
59 US Government, accessed November 2023, **NIST Risk Management Framework**

BACK TO TOP

kinetic IT

KINETICIT.COM.AU

☎ 1300 782 207

✉ INFO@KINETICIT.COM.AU

/KINETIC-IT

@KINETIC_IT_AUS

@KINETICITAU