23.1. Public Cloud Security Concepts

Objective

23.1.1. Agencies understand key concepts and implement controls related to securing their use of public cloud services.

Context

Scope

23.1.2. This section covers information about the key security concepts and architecture patterns related to public cloud services.

23.1.3. Cloud technologies require a different approach to the delivery of ICT services, and this extends to the way information security controls are implemented for cloud services.

23.1.4. Public cloud security builds on the application of Zero Trust concepts and principles. Zero Trust is the recommended approach to ICT system security, especially when using public cloud services.

23.1.5. Reference to other chapters and sections in this document is essential. In particular:

- Section 2.3 – Using cloud services

Mandates, directives and requirements

23.1.6. In August 2013, the government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute [CAB Min (13) 37/6B].

23.1.7. Under the 'cloud first' policy public service agencies are expected to adopt approved cloud services either when faced with new procurements, or an upcoming contract extension decision.

23.1.8. In July 2016, Cabinet subsequently agreed that agencies can also use public cloud to deliver office productivity services, provided they comply with security guidance issued by the GCDO and the GCSB [CAB-16-MIN-0316].

23.1.9. Agencies are required to identify and manage risks associated with the use of cloud services through the GCDO Cloud Risk Assessment process [CAB Min (13) 37/6B]. More information regarding cloud specific risk management can be found at digital.govt.nz.

23.1.10. Agencies are also required to certify and accredit their ICT systems and services, including those delivered through cloud technologies. Chapter 4 of this manual describes the certification and accreditation processes and these also apply to cloud services.

23.1.11. CAB Min (13) 37/6B directs that no data classified above RESTRICTED may be held in a public cloud.

Background

23.1.12. Adopting or using cloud services introduces new approaches to:

- Workload descriptions and management.
- Procurement and contract management.
- Virtualisation and the separation of resources using hyperscale technologies and strict control-plane/data-plane, tenant/tenant and tenant/provider segregation.
- Key information security services used to control the information boundary: using identity, directories and authorisation, instead of networks, gateways and firewalls.
- The approach to and selection of critical security services such as intrusion detection, key management, encryption, endpoint controls, privileged and user access management and authentication (including MFA).

Public cloud use within other cloud deployment models

23.1.13. All the standard cloud deployment models described by ISO and NIST could incorporate elements of public cloud, including:

- Private cloud, hosted on third party public cloud infrastructure.
- Multi cloud, combining elements of different vendors' public cloud services.
- Hybrid cloud, combining elements of private and public cloud services.

23.1.14. The focus of this chapter is on security concerns related to the use of public cloud technologies irrespective of the cloud service's primary deployment model. This is to avoid these concerns being considered out of scope due to inconsistencies in definitions being applied.

Characteristics of public cloud

23.1.15. There is not a single accepted definition of exactly what constitutes public cloud. Typically public cloud refers to cloud services that are generally available for anyone to use and are accessed through the internet.

23.1.16. For the avoidance of doubt, information in this chapter relates to public cloud services where:

- The infrastructure used to deliver the public cloud services is not owned by the agency (i.e., server hardware, network devices).
- The cloud infrastructure is shared between many customers ('multi-tenanted') and is accessible from the internet.
- Service provisioning is automated and customer managed.
- There is strict isolation between customer instances, and between customer instances and the service provider's management plane.
- Customer data is isolated and controls are in place that strictly manage access by the service provider.
- There is a defined shared responsibility matrix for ensuring the services meet customer security requirements. It should be noted that regardless of the model, agencies will retain ultimate accountability for the security of their information.
- There is limited flexibility in how the services are configured, and in at least some aspects there may be no flexibility to customise the service.

Responsibility for security in public cloud is necessarily shared

23.1.17. Agencies share responsibility for the security of their public cloud environments with their cloud service providers.

23.1.18. Due to differences in how cloud providers operate, there is no single model that can fully describe the boundary between agency security responsibilities and those of the cloud service provider. Cloud service provider responsibilities may even vary between their different service offerings.

23.1.19. The following is an example of how responsibilities for security in a cloud service could be shared, although every service is different:

Agency Responsible	Shared Responsibility	Provider Responsible
➢ Identifying, managing and accepting risk ➢ Information/data management and labelling ➢ Device access policies and control		➢ Physical infrastructure capacity management ➢ Physical asset management ➢ Physical environment security ➢ Infrastructure maintenance and patching ➢ Customer Isolation
➢ Account management and privilege assignments	Identity, credential and access management	➢ Authentication options incl. MFA
➢ Encryption key management	Encryption	➢ Encryption algorithms and parameters
➢ Configuration settings	Customer environment security	➢ Control implementations
➢ Validation of report contents	Independent assurance	➢ Commissioning audit reports
➢ Collecting and correlating events across platforms	Incident detection	➢ Platform telemetry and anomalies
➢ Tenancy monitoring and incident response	Incident response	➢ Incidents impacting multiple tenants

23.1.20. It is essential that agencies understand where the cloud service provider's responsibilities end and their own begin for each cloud service they consume, so there is no gap left unaddressed.

23.1.21. Agency security processes, such as certification and accreditation or incident response, must be revised to ensure compatibility with their cloud service provider's responsibilities.

Risks and benefits associated with public cloud services

23.1.22. Public cloud services can provide agencies with significant security benefits when adopted in a controlled and well understood manner, including:

- Pervasive identity and authorisation model.
- Consistent, software-orchestrated environments running immutable workloads.
- Automated response to security incidents or misconfigurations.
- Fine-grained access control.
- Scalable logging, monitoring and audit.
- Improved levels of baseline security.
- Enhanced visibility of security state.

23.1.23. The use of public cloud services introduces additional specific risks that require careful control selection to manage.

23.1.24. The following examples highlight key areas of public cloud-specific risks that need to be understood and managed:

- Traditional barriers limiting the movement of agency data across legal jurisdictions can be significantly reduced through the use of cloud services.
- Cloud service provider self-service tools can be subject to manipulation impacting agency infrastructure.
- Agency systems delivered using cloud services are typically accessible from the internet, including management interfaces, unless controls are put in place.
- Agency data is stored on shared platforms, in multiple locations, with agencies ultimately being accountable for ensuring information is secured.
- Cloud environments present large, high value targets, where single exploits can impact large numbers of customers.
- Cloud services are easier to consume without needing to involve common governance processes, such as change control, increasing the risk of using shadow services without adequate information security controls in place.
- On-demand services, coupled with rapid-elasticity, can lead to inappropriate use of agency cloud environments. Agencies are responsible for tracking billing and usage metrics and ensuring appropriate controls are in place to manage fiscal constraints.

23.1.25. The GCDO Cloud Risk Assessment process is intended to help agencies understand these, and other, risks associated with the use of public cloud.

Public cloud impacts on security control selection

23.1.26. Depending on whether responsibility for implementing security controls rests on the cloud service provider or the agency, enterprise security controls or standards may not be possible to implement uniformly in public cloud services, for example:

a. Agents used to manage configuration or collect system telemetry may not be able to be deployed across public cloud services.
b. Log messages may not be able to be centrally collected, or log information tailored to agency requirements, from public cloud services.
c. Network information, such as packet captures, may not be feasible to collect.
d. Traditional security devices, such as firewalls and proxy servers, may not be able to be deployed.

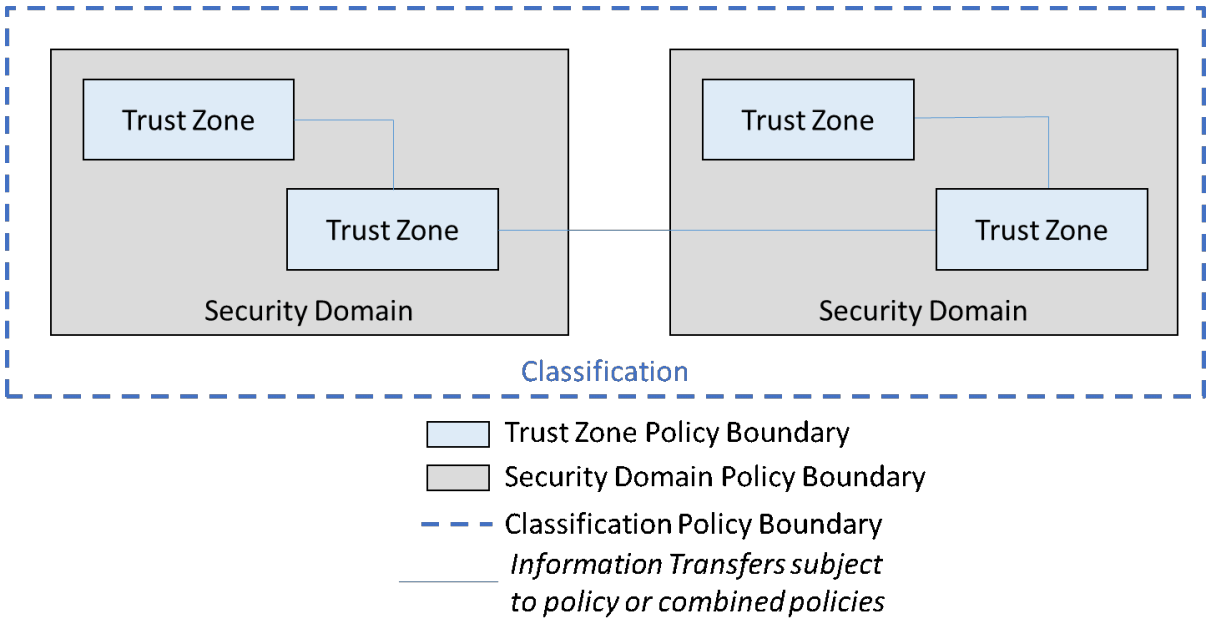
Security boundaries in cloud

23.1.27. Security boundaries exist to identify where differing security requirements and policies need to be applied to information and infrastructure assets operated in support of agency outcomes. Well defined security boundaries are a key construct in support of:

- Protecting environments by providing control enforcement points to manage information flows between internal systems and externally to the environment.
- Providing containment points where the impact of incidents can be limited in scope, which also aids in recovery.

23.1.28. Well defined security boundaries can ensure that information is accessible for authorised users and that restrictions do not limit those users' access to information to which they are entitled.

23.1.29. There are three key constructs used to describe security policy boundaries in the NZISM. These are *classification*, *security domain* and *trust zone*. Information and systems are subject to the combined requirements described in these policies.



23.1.30. In public cloud, the *classified system* refers to the highest level of classified information that can be stored, or processed, by systems in the agency's

cloud environment. The highest level of classified information the classified system can store or process is based on the lower of:

- The highest classification the system is accredited to operate at, AND
- The lowest clearance level authorised users of the system hold.

The highest classification of information a *classified system* in public cloud can be accredited to operate with is RESTRICTED.

23.1.31. Minimum security requirements based on classification are described in the Protective Security Requirements and the NZISM.

23.1.32. A *security domain* in public cloud can be categorised as a group of *trust zones* operating under a common set of security requirements and policies. These security requirements and policies are formed through a combination of:

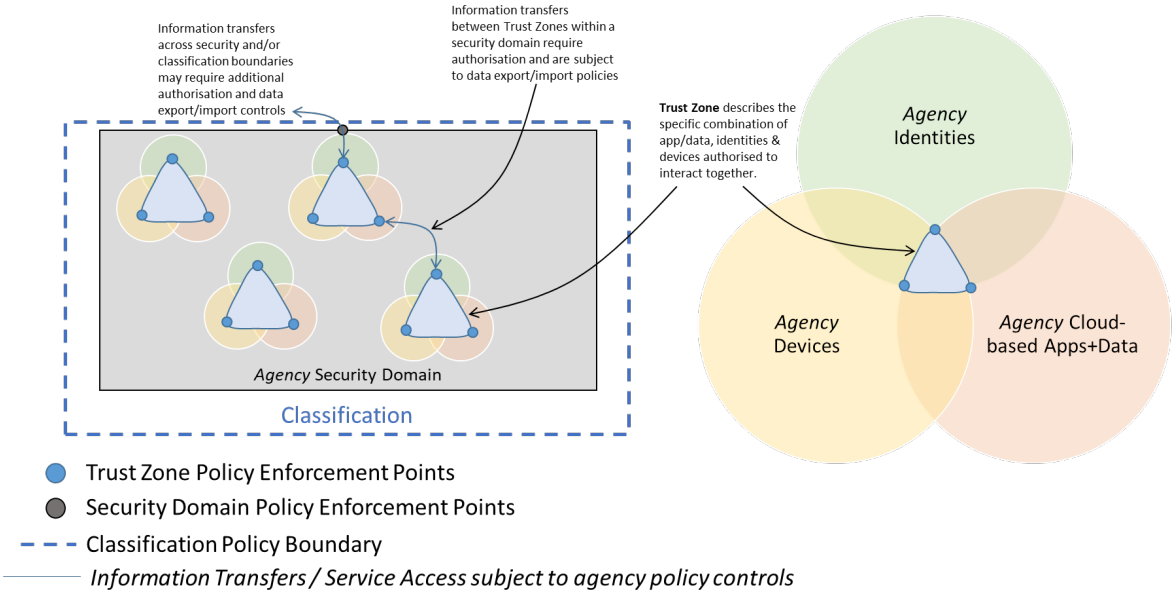
- Minimum security control requirements from the PSR and NZISM, determined by the classification.
- Security control requirements to manage the unique threat environment presented by the use of the public cloud services.
- Additional security control requirements to manage specific risks identified through risk assessments.

23.1.33. Examples of the unique threat environment related to the use of public cloud services include:

- Access to the underlying infrastructure by the public cloud service provider systems and staff.
- Differing relative importance of security controls, such as identity, and the addition of different types of privileged access such as for managing service subscriptions and billing (including terminating services) that can have immediate effect.
- Geographic locations where the public cloud services are being delivered from.
- Security controls being defined and implemented by the public cloud service provider.
- The ease of extending access to third parties, including third party applications, through in-built federation and directory integration services in public cloud.
- The ease of shifting data between services and geographic locations in public cloud environments compared to on-premise systems.
- The control and visibility of the security state of the underlying infrastructure platforms, including the physical hosting environment.

23.1.34. Defining *trust zones* provides a mechanism to differentiate security controls used to manage access to information and services within an agency's public cloud environment.

23.1.35. In the public cloud environment, *trust zones* represent combinations of public cloud services (made up of user, system and data objects) that are authorised to interact with each other and are protected by a common set of security capabilities. The security controls associated with these security capabilities are applied at policy enforcement points:



23.1.36. Traditional policy enforcement point implementations based on location-based network perimeter security controls can be difficult to successfully replicate in public cloud environments.

23.1.37. In public cloud, access control policy enforcement points are tied to authorised combinations of user, system, and data object identities.

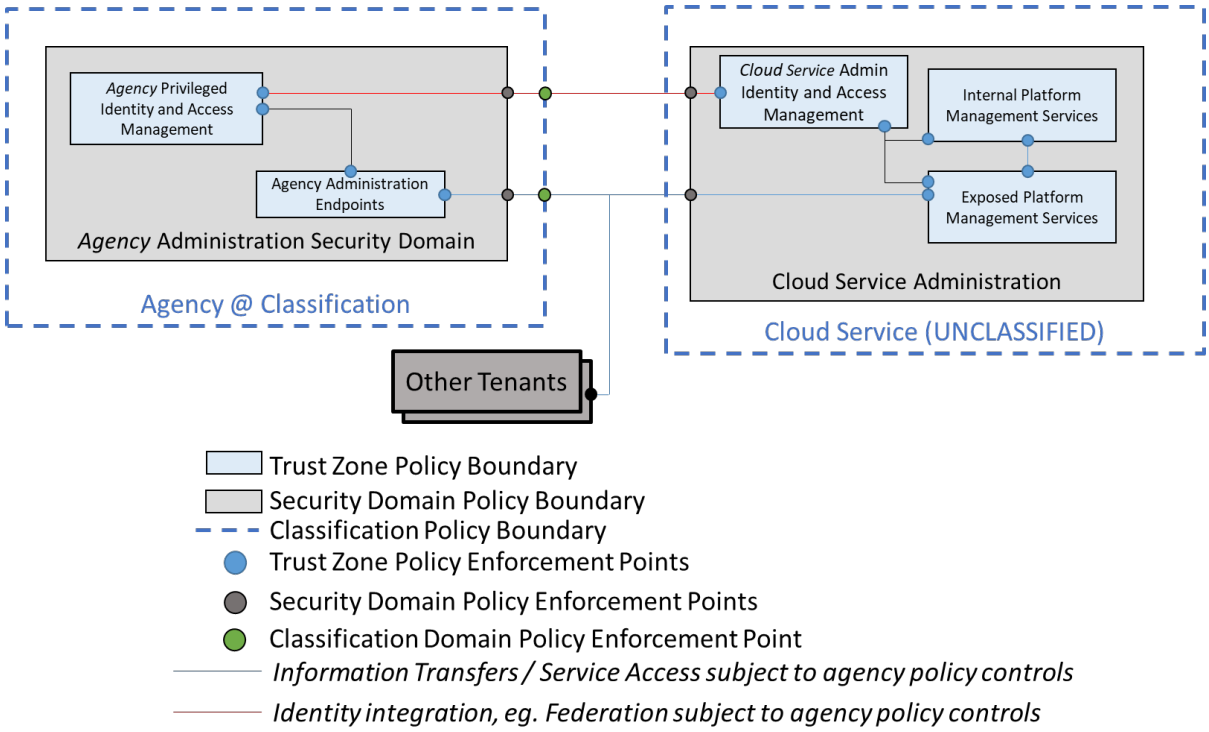
Security boundaries between cloud providers and customers

23.1.38. A significant difference between public cloud and traditional computing is the additional set of administration services used by the cloud service provider to manage the overall cloud platform.

23.1.39. Some of these administration services are exposed to tenants to facilitate tenancy management, such as maintaining customer contact and billing details or creating and deleting top level tenant resources. In some circumstances, third parties can be provided access to perform these actions on

behalf of tenants.

23.1.40. Due to the significant impact from a compromise, access to these services and the associated privileged identities requires a high degree of trust in those responsible. Ensuring separation of duties (i.e., multi-user authorisation, see section 16.7.19) in this area is highly recommended.



Virtualisation and multi-tenant security in public cloud

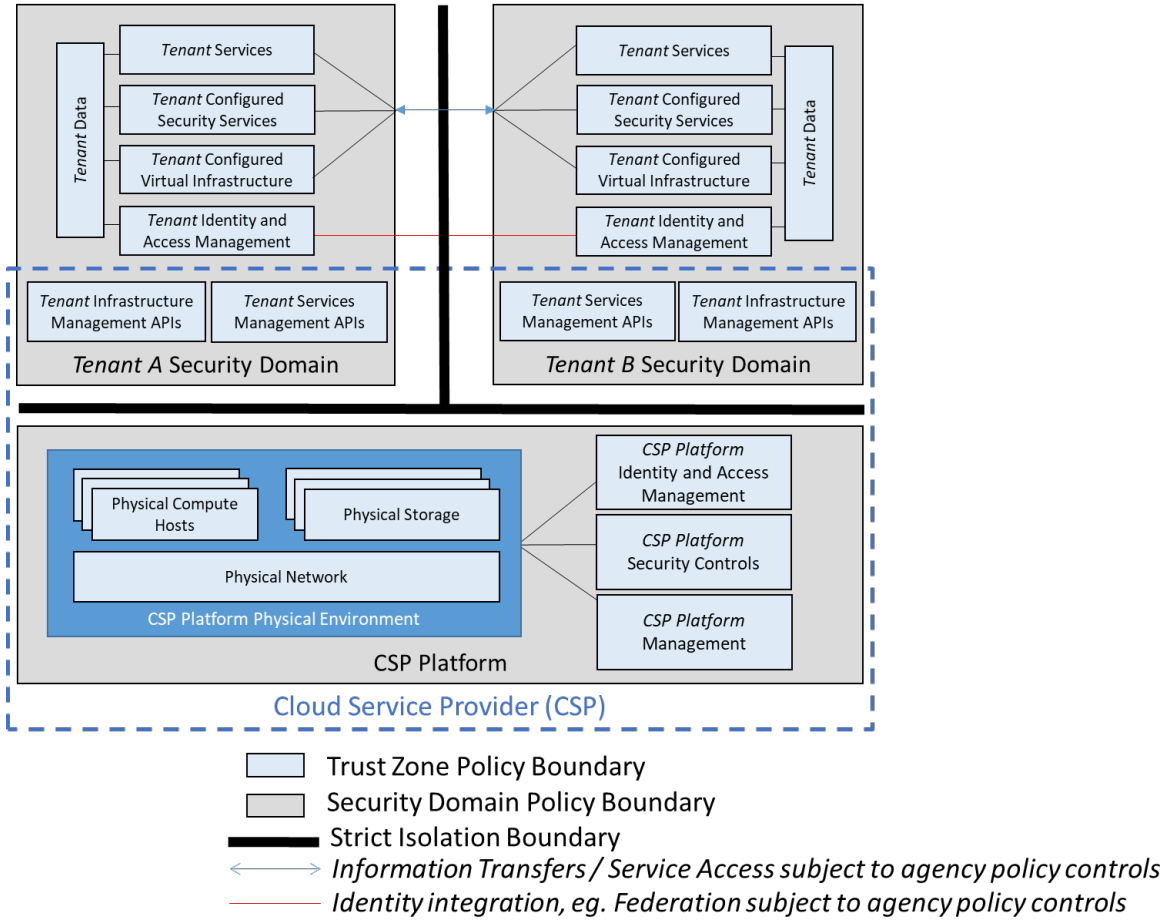
23.1.41. Within a public cloud environment adequately architected, designed, and implemented virtualisation technologies can be used to provide isolation between tenants and separation between security domains.

23.1.42. Public cloud service providers that are designed to use technology to implement strict isolation between tenant environments, and separate customer management from platform management, are more likely to provide adequately architected security controls to support security domain separation in a virtualised environment.

23.1.43. Examples of adequately architected security controls that support tenant isolation in public cloud services can include:

a. Zero touch configuration of infrastructure using well defined infrastructure as code pipelines.
b. Separation of the cloud provider platform's administrative control interfaces from customer accessible tenant management services.
c. An inability for cloud provider staff to access customer data except through customer authorised access channels (i.e., the platform does not provide 'back door' access to customer data).

23.1.44. At a minimum, a security domain control boundary exists between components where different parties undertake configuration and management responsibilities.



Collaboration between agencies in public cloud

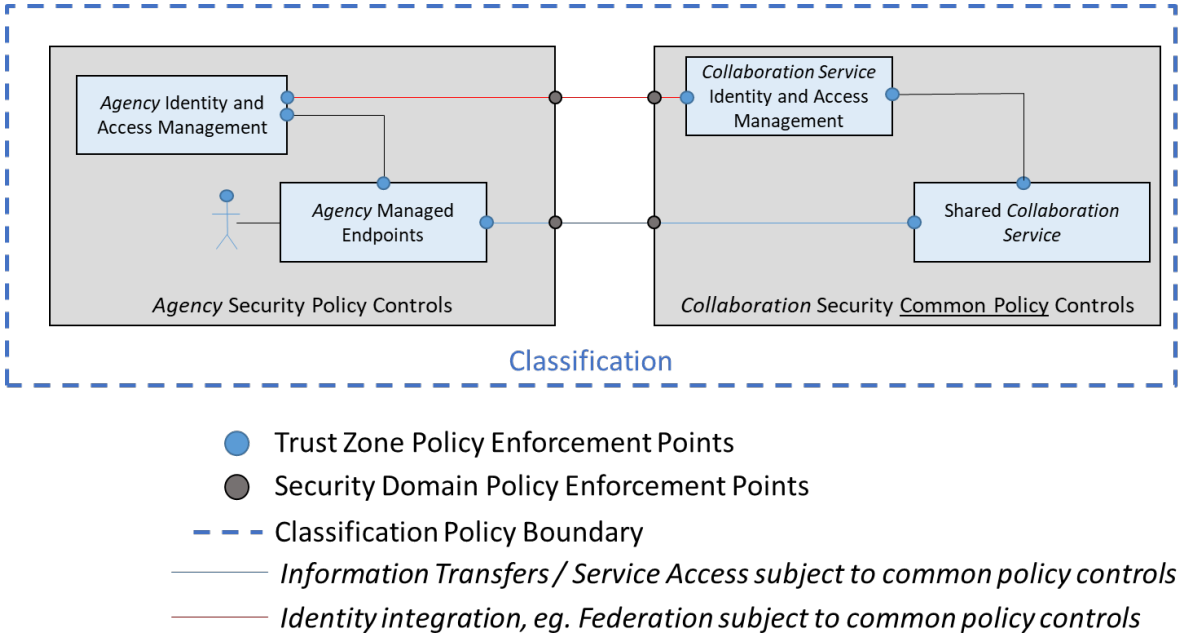
23.1.45. Public cloud services, due to their multi-tenant design and support for integration to multiple identity providers, can provide a convenient platform for collaboration systems between agencies.

23.1.46. It is usually not possible, nor desirable, to implement traditional DMZ or Landing Zone network architectures to facilitate third party access to an agency's public cloud services where collaboration is the goal.

23.1.47. For public cloud collaboration systems, it is often more practical to grant access to individual third party identities, or to federate (i.e., trust) the third party's identity service to perform authentication on the collaboration system's behalf.

23.1.48. When multiple identity systems are used to control access to shared public cloud collaboration systems, the shared system operates to a *common policy* that covers all of the participating agencies security requirements.

23.1.49. The *common policy* reflects a different security domain from each of the participating agencies, providing the equivalence of a DMZ environment in public cloud.



23.1.50. When systems are operating in separate security domains, agencies must follow the guidance regarding *Information transfer and release in public cloud* described in this chapter of the NZISM.

Information transfer and release in public cloud

23.1.51. Information being released from trust zones, destined either internally or externally to the security domain, must always follow the requirements for *Data management* described in Chapter 20 and *Gateway security* described in Chapter 19 of the NZISM. This includes where data is being backed up or replicated to systems operating in a different trust zone.

References

23.1.52. Further references can be found at:

Reference	Title	Publisher	Source
CAB Min (13) 37/6B	Cloud computing risk and assurance framework (CAB Min (13) 37/6B)		Cabinet minutes for public cloud services | NZ Digital government
CAB-16-MIN-0316	Accelerating the adoption of public cloud services CAB-16-MIN-0316		
NIST SP 800-145 (2011)	The NIST definition of cloud computing	NIST	SP 800-145, The NIST Definition of Cloud Computing | CSRC
NIST SP 500-293 (2014)	US Government cloud computing technology roadmap	NIST	US Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements to Further USG Agency Cloud Computing Adoption; and Volume II: Useful Information for Cloud Adopters | NIST
NIST SP 500-291 (2011)	NIST cloud computing standards roadmap	NIST	NIST-SP 500-291, NIST Cloud Computing Standards Roadmap | NIST
NIST SP 800-144 (2011)	Guidelines on security and privacy in public cloud computing	NIST	Guidelines on Security and Privacy in Public Cloud Computing | NIST
NIST SP-800-210 (2020)	General access control guidance for cloud systems	NIST	General Access Control Guidance for Cloud Systems | NIST
ISO/IEC 17789:2014	Information technology -- Cloud computing -- Reference architecture	ISO/IEC	ISO - ISO/IEC 17789:2014 - Information technology — Cloud computing — Reference architecture
ISO/IEC 27017:2015	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC	ISO - ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	CSF Tools	CSF	Welcome to CSF Tools - CSF Tools
	Trusted internet connections	CISA	TIC | CISA
	Cloud security technical reference architecture	CISA	Cloud Security Technical Reference Architecture | CISA
	Cloud Security Alliance	CISA	Home | CSA (cloudsecurityalliance.org)

PSR References

23.1.53. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR mandatory requirements	GOV2 - Take a risk-based approach GOV5 - Manage risks when working with others GOV6 - Manage security incidents INFOSEC1 - Understand what you need to protect INFOSEC2 - Design your information security INFOSEC3 - Validate your security measures INFOSEC4 - Keep your security up to date	Mandatory requirements | Protective Security Requirements
PSR protocol for information security	Management protocol for information security	Management protocol for information security | Protective Security Requirements

Rationale & Controls

Cloud security boundaries

23.1.54.R.01. **Rationale**

Security boundaries identify the scope of security policy applicability, and determine where *data management* controls will apply. Refer to Chapter 20 – Data Management.

23.1.54.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7349]

Agencies MUST clearly identify and understand where classification, security domain, and trust zone boundaries exist **prior** to implementation or adoption of public cloud services.

23.1.54.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7350]

Where multiple identity systems under different security policies are used to control access to an agency's instance of a public cloud service, the instance MUST be considered to be in a separate security domain from services where access control is managed solely by the agency's identity system.

Shared responsibility model

23.1.55.R.01. **Rationale**

The responsibility for the selection, implementation, management, and maintenance of controls in public cloud services is shared between the provider and the consumer. Precisely where the responsibilities lie depends on the provider and the service and deployment models (refer to NIST SP 800-145) used in the delivery of the specific public cloud service.

23.1.55.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7353]

Agencies MUST clearly identify and understand their cloud service provider's security responsibilities for each service consumed, and the aspects of security that the agency is responsible for, **prior** to implementation or adoption of the service.

23.1.55.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7354]

Agencies SHOULD clearly document the aspects of security they and their provider are responsible for.

23.1.55.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7355]

Agencies SHOULD review existing security processes to ensure compatibility with their cloud service provider's responsibilities.

Automation and infrastructure as code

23.1.56.R.01. **Rationale**

Tools and APIs that generate code used to configure cloud services enable automated deployment and management of resources in a repeatable manner.

23.1.56.R.02. **Rationale**

Infrastructure as code, where resources and their configurations are defined in machine-readable code, can drive automated deployment tools that support software engineering techniques such as version control, continuous integration and deployment, and automated security testing. In particular, disciplined version control can support the ability to roll back failed changes to the "last known good" configuration as part of agency change control processes.

23.1.56.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7359]

Agencies SHOULD deploy and manage their cloud infrastructure using automation, version control, and infrastructure as code techniques where these are available.