Building Government-Grade Secure Access Service Edge (SASE): Compliance, Architecture, and Lessons from IRAP-Certified Deployments

Krishna Mohan Raju Yenugudati
Associate Director
Independent Researcher
Plano, United States
krishnarajuyenugudati@gmail.com

***Abstract*—Government agencies are moving away from legacy, centralized networks and adopting cloud-native, distributed environments. As a result, the traditional "moat and castle" method of security is becoming increasingly obsolete. The SASE (Secure Access Service Edge) framework will allow for a unified cloud-delivered architecture to combine software defined wide area networks (SD-WAN) with advanced security services such as Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), and Firewall-as-a-Service (FWaaS). This report provides a comprehensive methodology for the design and implementation of SASE platforms that are suitable for government entities and comply with the stringent requirements set forth by both the Information Security Registered Assessors Program (IRAP) at the Protected level in Australia and the Federal Risk and Authorisation Management Programme (FedRAMP) in the United States. The comprehensive analysis of architectural decisions in this report relates to Sovereign SASE's jurisdictional certainty, Compliance as Code via OSCAL supporting Continuous Authority to Operate (cATO), and the operational complexities associated with the commercial telecommunications industry. This will also include lessons learned from IRAP-certified deployments by organisations including Macquarie Telecom, Netskope and Fortinet that will provide public sector agencies with a roadmap for modernising their digital infrastructure, while ensuring that they remain fully compliant with national security and data sovereignty standards.**

Keywords— SASE, Cloud Security, Government Compliance, IRAP, FedRAMP, Zero Trust, Secure Gateway, Public Sector Cloud, Sovereign SASE, OSCAL.

I. Introduction

The global threat landscape is changing. The rise of advanced, state-sponsored attackers and ransomware has resulted in a re-examination of how governments secure their networks. Up until now we saw public sector agencies on heavy use of physical perimeter defenses, and bringing remote traffic into central data centers to apply security policies a which in today's software as a service (SaaS) and hybrid work environment introduces great latency and performance issues. The Secure Access Service Edge (SASE) model which we see as a solution to the above issues puts security at the cloud edge instead which in turn ties protection to the identity of the user and device not the physical connection point. For government bodies this transition is under the watchful eye of strict compliance structures like the Australian Signals Directorate's (ASD) Info Security Manual (ISM) and the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53. What we are seeing is that for these bodies it isn't just a matter of tech implementation but a very complex architectural play which also includes data sovereignty, personnel clearance issues and the automation of compliance through what we call Compliance as Code. This paper looks at the architecture which came out of the first set of IRAP certified and FedRAMP authorized SASE deploys and brings to light what we have learned from them which in turn will guide other agencies in achieving operational resilience without breaking the rules.

II. The Convergence of Network and Security: The SASE Architecture

SASE has seen the greatest transformation in enterprise networking which is over a 20 year span. What we see with SASE is the combination of network and security in a single, cloud based software stack. Also with SASE we see a "single pass" inspection model which means that traffic is decrypted once and goes through a series of security policies.

A. Core Technology Components

The integration of five main technology components into a SASE platform contributes to the overall security landscape of a SASE solution at an enterprise level.

SASE Component	Technical Function	Significance for Government Agencies
SD-WAN	Virtualizes the network overlay to optimize traffic across multiple transports.	Ensures mission-critical application performance and reduces reliance on expensive MPLS circuits.
ZTNA	Replaces traditional VPNs with identity-centric, least-privileged access.	Eliminates implicit trust; users only see the applications they are authorized to access.
SWG	Filters and inspects all internet-bound traffic to block malicious content.	Defends against web-based threats, malware, and data exfiltration in real-time.
CASB	Monitors and secures interactions between users and cloud applications.	Provides visibility into "Shadow IT" and secures sensitive government data in multi-cloud environments.
FWaaS	Delivers advanced firewall capabilities (NGFW) from the cloud.	Provides scalable, distributed protection that adapts to the user's location without hardware constraints.

B. The Evolution of the Government Gateway

The former, inflexible nature of the traditional monolithic gateway does not adequately support the current Cloud First Era and therefore the Australian Signals Directorate (ASD) has commenced transitioning to an adaptive and more fluid Disaggregated Gateway Model under the framework of Resilient Digital Infrastructure (RDI). In this Model, gateway functions are separated into individual systems allowing Agencies to leverage Cloud-Native Security Service Edge (SSE) Solutions whilst still utilising high assurance Cross Domain Solutions (CDS) for Secret networks [5].

III. Compliance as the Foundation: Navigating IRAP and FedRAMP

Security for government agencies isn't merely about what they choose to do but a matter of legal statute. IRAP and FedRAMP are the two primary regulations that impact cloud and network security for government-grade SASE.

A. IRAP Protected Level Assessment

The IRAP program assesses cloud service providers against the Australian Government Information Security Manual (ISM). At the “Protected” level an IRAP assessment reports that a platform is able to handle very sensitive government information which should a breach occur, would damage national interest.

B. FedRAMP and the NIST 800-53 Baseline

The Federal Risk and Authorization Management Program (FedRAMP) High denotes the highest level of risk for the federal government concerning unclassified sensitive data.

Feature	IRAP (Australia)	FedRAMP (United States)
Primary Standard	ASD ISM & PSPF.	NIST SP 800-53.
Certification Process	Independent Assessor report; agency-led ATO.	3PAO assessment; JAB or Agency ATO.
Highest Common Level	PROTECTED (and higher).	HIGH Impact Level.
Data Sovereignty	Mandatory Australian residency for Protected.	Mandatory U.S. residency for High.
Personnel Requirements	Often requires NV1/NV2 clearance for admins.	Personnel clearance varies; often required for High.

IV. Architectural Patterns for Government-Grade SASE

Design of a SASE platform which at the same time meets extreme performance requirements and passes stringent government compliance is a task which requires a structured architectural approach. In this section we present the key design decisions for modern defensible architecture.

A. Zero Trust Access and Multi-Contextual Evaluation

Modern government ZTNA deployments move beyond simple MFA to a multi-contextual evaluation model. In this architecture, a request to access a Protected resource is scrutinized across four simultaneous context zones:

- Identity Context: Validating the subject’s role, organizational affiliation, and security clearance level (e.g., NV1 vs. Baseline).
- Task Context: Determining why access is required at this specific moment, linked to the business transaction or workflow step currently underway.
- Environment Context: Assessing the "where" and "how" of the request, including device health (patch level, EDR status), network location (trusted IP vs. public internet), and real-time threat signals.
- Data Context: Factoring in the classification of the data being accessed (OFFICIAL: Sensitive vs. PROTECTED) and the regulatory requirements associated with that specific dataset.

In accordance with the NIST 800-207 Standards, a Policy Engine (PE), performs an assessment of the policies to provide guidance to the Policy Administrator (PA), whereas a Policy Enforcement Point (PEP) enforces the authorization and access restrictions established through the policies.

B. Sovereign SASE and Three-Layer Separation

In order to provide jurisdictional certainty to government entities, there has been a trend toward using “Sovereign SASE” within a completely private/trusted infrastructure [1]. The architecture is constructed via the clear segregation among the three planes:

1) The Control Plane: A centralized management and orchestration hub where security policies are authored. It can be hosted in a private cloud and never sees actual user traffic.[1]
2) The Data Plane: Security enforcement nodes (encompassing SWG, ZTNA, and FWaaS) that execute traffic inspection at line speed. These nodes are deployed inside the organization's premises or in nationally-bounded colocation centers to ensure no user packets ever leave defined borders.[1]
3) The User Plane: Lightweight endpoint agents that continuously verify device posture and establish secure tunnels directly to the nearest authorized data plane node.[2]

C. Disaggregated and Hybrid Gateway Patterns

The ASD has put forth the Gateway Security Guidance Package which puts forward a move away from large scale "one stop shop" security devices to what we see in Disaggregated Architectures.3 This trend is to break up gateway functions into separate but compatible systems which in turn allows agencies to scale out certain services (like SSL inspection) independent of others (which may be like WAF). Also we see a lot of Hybrid Architectures which combine on premise traditional security appliances for high assurance cross domain data flow with cloud based Security as a Service solutions for remote user access.3 In this flexible model we see continuous protection which includes cloud native integrations that scan data within a service as soon as a new threat signature is identified as opposed to just at the perimeter.[4]

D. High-Assurance Multi-Tenancy and Data Isolation

In a commercial telco ecosystem serving multiple government agencies, robust isolation is a prerequisite. Architectural patterns for multi-agency SASE include:

- Database-per-Tenant: Ensuring completely separate database instances for each agency to prevent accidental cross-contamination.
- Workload Isolation (SC-39): Utilizing unprivileged Linux containers built on OCI standards to ensure that customer workloads cannot interfere with other tenants or the underlying platform.
- Network Segmentation (SC-7): Implementing strict subnetting and virtual security appliances to enforce boundary protection between public-facing and internal management components.

E. Single-Pass Processing and Performance Optimization

Government SASE platforms circumvent the latency penalties involved with "service chaining" (where traffic is decrypted & re-encrypted at each security tool) by employing Single-Pass Inspection. An illustration of this type of analysis is Cato's Single Pass Cloud Engine (SPACE), which opens a connection to a device, analyzes the data being sent through that device in real-time against many different policies at the same time (firewall, malware, DLP), and then sends the data back out through the device. This allows the re-encryption policies to be applied at line speed (which is important for time-sensitive government applications).

V. Technical Controls and Encryption Standards for Protected Information

The ISM, as issued by the Australian Government publication "Information Security Management", defines specific technical requirements concerning the safeguarding of information classified at the Protected level.

A. ASD-Approved Cryptographic Protocols and Algorithms

All network traffic transiting a government-grade SASE gateway must be encrypted using ASD-Approved Cryptographic Protocols (AACP) and Algorithms (AACA).

Cryptographic Family	Approved Algorithm	Minimum Requirement (Protected Level)
Symmetric Encryption	AES	128, 192, or 256 bits (256 preferred).
Asymmetric / Public Key	Diffie-Hellman (DH)	2048+ Modulus (3072+ preferred).
Elliptic Curve	ECDH / ECDSA	224+ bits field size; NIST Curve P-384 preferred.
Digital Signatures	RSA	2048+ Modulus (3072+ preferred).
Hashing	SHA-2	SHA-224, SHA-256, SHA-384, or SHA-512.

B. Secure Web Access and Application Traffic

For web based services, SASE platforms have to enforce HTTPS for all of which is web and application traffic also which should include Mandatory Strict Transport Security (HSTS) policies to prevent session hijacking and man in the middle attacks.

VI. Compliance as Code: Automating the Authorization Process

SASE platforms coupled with Compliance as Code lets agencies modify the "Authorization to Operate" (ATO) processes into engineering automated ATO processes. This enables agencies to keep pace with rapid digital change while adhering to the stiff requirements of the government.

A. Standardizing Compliance with NIST OSCAL

OSCAL is a "universal translator" for security which puts out machine readable formats like XML, JSON, and YAML for security info. In terms of SASE security we see OSCAL which is a way to put security controls in a standard that is easy for machines to read. This in turn allows agencies to get away from manual data entry and version control issues. Here we see a path to a "DevSecOps" approach to compliance [2].

Also with the machine readable OSCAL packages which can be put into agency tools we see AOs spending from weeks to hours in review time which was previously spent going over thousands of pages of manual docs.

B. Achieving Continuous Authority to Operate (cATO)

Compliance as Code's goal is to shift from "point in time" audits to Continuous Authority to Operate (cATO). In this we take in real time data from SASE which includes ZTNA access logs, SWG threat alerts, and CASB policy hits and we map it to a particular ISM or NIST control. We have automated testing and validation in the CI/CD pipeline which confirms that any changes to a config are in fact compliant with the government security baseline before they go into production [3]. If a config strays from the set security state we have put in place the system will either start a remediation process or it will not deploy non compliant configurations.

C. Operational Impact and Financial Efficiency

Implement automated compliance systems which see large scale benefits to government entities. Also we see that organizations adopt Compliance as Code reports to have reduced their manual compliance work by over 60%. Also these practices improve audit accuracy which usually is at 82% in traditional manual processes to 95% with the use of automation.

Compliance Metric	Manual Process	Automated (CaC)	Impact
Audit Preparation Time	Weeks/Months	Hours/Days	60-70% Reduction
Compliance Accuracy	~82%	~95%	Improved Reliability
Control Enforcement	Periodic/Reactive	Real-time/Proactive	80% Fewer Errors
Onboarding Timeline	18+ Months	~90 Days	3-4x Faster

VII. Lessons from IRAP-Certified Deployments and Case Studies

Practical applications of SASE have resulted in valuable insights about architectural development, employee vetting, and data storage within the regions in which they were deployed.

Vendor	Certification Level	Core Use Case / Strength
Macquarie / Netskope	IRAP Protected	Integration of SSE with SD-WAN; 24/7 NV1+ cleared operations.
Versa Networks	FedRAMP High Ready	Mission-resilient access across tactical edge and cloud environments.
Fortinet	Gartner Leader / Sovereign SASE	Single-vendor unified stack with full jurisdictional control.
Datadog	IRAP Protected	Advanced observability for mission-critical workloads in A/NZ.
CyberArk	IRAP Protected	Workforce Identity and Endpoint Privilege management for public sector.

A. Case Study: Macquarie Telecom and Netskope Integration

Macquarie Telecom's work with Netskape is a model for IRAP certified SASE. We saw that success was not due to having just local data centers, but also having a management layer of Australian based, NV1+ cleared experts which we had 24/7 monitoring. That which put forward technical skill as enough we saw in this case was that the people running the technical side of things also had to have the right security clearances.

B. Case Study: Fortinet Unified SASE for Federal Agencies

Fortinet presents a single vendor solution which puts an end to the issue of management of different appliances. We see this "single pass" approach which is that once we decrypt the traffic we also run it through at the same time for malware and access violations which in turn we see has great results in terms of performance.

VIII. Operational Realities: Managing the SASE Lifecycle

Implementing SASE is not a static task but a continuous lifecycle management process. For government agencies, this requires a fundamental shift in how IT services are procured and operated.

A. Deployment Strategy Selection

The choice between single-vendor and multi-vendor architectures is a critical decision.

- Single-Vendor Efficiency: Consolidating networking and security into one stack reduces the "integration tax." This model provides a unified data lake and consistent policy enforcement points across all nodes.

- Best-of-Breed Flexibility: Multi-vendor strategies allow agencies to retain specialized SD-WAN while adopting advanced security. However, this often leads to "policy drift," where security rules in the cloud and on-premises become out of sync [7].

- Strategic Evaluation Criteria:
  - Support and Clearance: Use of local personnel (NV1/NV2) for monitoring.
  - Scalability: Ability to handle sudden traffic spikes without performance loss.
  - Sovereignty: Ensuring management consoles remain within national jurisdiction.

B. Phased Implementation Roadmap

A successful deployment follows a structured framework to minimize risk.

- Alignment and Collaboration: Networking and security teams must merge into a unified cross-functional unit.
- Technical Planning:
  - Asset Discovery: Identifying "shadow IT" and unmanaged cloud instances.
  - Skills Audit: Assessing if the workforce is trained in cloud-native protocols.
- Execution Phases:
  - Pilot Deployment: Launching SASE for a non-critical unit to establish a baseline.
  - Connectivity Optimization: Transitioning from legacy MPLS to dynamic routing.

C. Managing the Shared Responsibility Model

Security is a partnership between the agency and the service provider.

- Agency Responsibilities: Agencies must configure identity providers and define granular access policies.
- Provider Responsibilities: Providers handle the hardening of underlying infrastructure and physical data center security.
- Critical Oversight:
  - Continuous Monitoring: Moving from periodic to real-time oversight.
  - SLA Enforcement: Regularly auditing provider compliance against IRAP reports.

IX. Future Outlook: Resilient and Autonomous Infrastructure

The next generation of government SASE will be defined by AI-driven autonomy and preparation for the quantum era.

A. AI-Driven Policy and Incident Response

AI is evolving from just being an added functionality to being the driving force behind SASE architecture. The latest SASE solutions utilize ML for behavioral baselining. Therefore, they are able to identify anomalies not captured by traditional signature-based solutions, such as an IoT device sending an abnormally high volume of data or a user accessing data from an unexpected geo-location.6 In 5G and 6G environments, AI driven management performs real-time predictive analysis and, therefore, can take action within milliseconds [6]. For example, during a DDoS attack, it can perform lockout of abnormal user identities or slice isolation. This type of security is called “closed loop” security and reduces the need for human operators while also driving down the time to respond to incidents from hours to minutes.

B. The Transition to Post-Quantum Cryptography (PQC)

In the case of “harvest now, decrypt later” attacks which is a growing issue in which groups collect encrypted data to break once quantum computers are advanced enough agencies are reporting very tight time tables for PQC transition. Also at present we see that national requirements are for agencies to prepare inventories of all crypto systems and to adopt what is known as “crypto-agility” the ability to change out algorithms without which business will come to a standstill. Also we are seeing that SASE platforms have started to include NIST put forth quantum resistant algorithms like CRYSTALS-Kyber (for key exchange) and Dilithium (for digital signatures) into the TLS handshakes and Zero Trust Network Access tunnels [4]. This in turn is what is going to see to it that basic communication remains protected going forward which in turn will preserve the long term health of government info.

Migration Action	Target Outcome
Inventory Cryptographic Systems	Identify all applications using public-key cryptography.
Implement Crypto-Agility	Enable the ability to swap algorithms without code rewrites.
Adopt Hybrid Cryptography	Deploy TLS 1.3 with ML-KEM for immediate protection.

X. Conclusion

SASE adoption for government agencies means they are moving away from static location based security to a more flexible identity based security which we see is more visible and resilient. As agencies' architectures grow in this new model we see the importance of supporting a mobile public sector workforce and in also fighting the ever growing issue of cyber threats like ransomware and state sponsored attacks. In the early goings of IRAP certified and FedRAMP authorized implementations we've seen that for technical excellence to be put into practice with operational rigor it must include data sovereignty, personnel vetting and the auto scaling of governance through "Compliance as Code" which we are seeing as the 3 key operational tenets.

Government agencies will see to it that they are in place for the put in of agentic systems and machine readable frameworks like OSCAL as far as they remain 'audit ready'. Based on principles of legal certainty and a multi stage, step by step collaborative model, the Government for the first time out will put forward to protect the Sovereign SASE's most important assets. In the end Government grade SASE will present the case for the development of decentralized quantum technology that in turn will protect the Government's mission and therefore the National Interests. In this study we present what is in effect a blueprint and a roadmap for public sector IT leaders for this critical transition.

References

[1] P. Kumar, "Agent-Aware Zero Trust: A Framework for Securing Agentic AI in SASE and Cloud Architectures," *Computer Fraud & Security*, Feb. 2026.

[2] S. R. Thati, "Compliance as Code: Automating Compliance in Cloud Systems," *World Journal of Advanced Research and Reviews*, vol. 26, no. 2, pp. 1216-1223, Mar. 2025.

[3] A. Singh, V. Pareek, and A. Sharma, "Automating Compliance in Cloud Data Platforms Using Policy-as-Code," *ResearchGate Technical Report*, Jan. 2025.

[4] N. N. Singh, "Post-Quantum Cryptography-Safe Network Architectures: Design Frameworks and Implementation Strategies for Enterprise Zero-Trust Environments," *SAR Journal of Electronics and Computer Science*, vol. 4, no. 8, pp. 807-820, Aug. 2025.

[5] S. Mahmood et al., "Securing Edge Devices in IoT and 6G: A Trust-Based Approach," *IEEE Access*, vol. 13, pp. 1112-1128, Jan. 2025.

[6] D. Tomar, "AI-powered security for 5G and 6G communication networks," *International Journal of Sciences and Innovation Engineering*, vol. 2, no. 10, pp. 1292-1306, Oct. 2025.

[7] T. Yadavalli, "Addressing Security and Compliance Challenges in Google Cloud Storage for Regulated Industries," *SSRN Electronic Journal*, Jun. 2025.