DSS-1200 FRAMEWORK

ALL DOMAINS SATISFACTORY

SECURITY ASSESSMENT REPORT

Detailed Security Standard Report

DSS-1200 Self-Assessment · Point-in-Time

ISSUED TO
Instant Compliance Pty Ltd

ACN
111 744 668

DATE OF ISSUE
28 April 2026

ASSESSMENT TYPE
DSS-1200 Self-Assessment

ADDRESS
242 Elizabeth Street, Sydney NSW

SIGNATORY
Simon Giles, CEO

Table of Contents

1. Executive Summary 3

2. System Overview & Architecture 3

3. Risk Management & Treatment Plan 5

4. Business Continuity & Disaster Recovery 6

5. Human Resources Security Controls 7

6. Vulnerability Management Programme 8

7. DSS-1200 Domain Assessment 9

8. Assessment Summary 13

9. Management Attestation 14

SECTION 01

Executive Summary

This document constitutes the formal Detailed Security Standard (DSS-1200) Self-Assessment Report for Instant Compliance Pty Ltd (ACN 111 744 668). Instant Compliance is a Software-as-a-Service (SaaS) platform that automates AUSTRAC AML/CTF compliance for Australian financial services businesses. The platform processes sensitive financial and identity verification data on behalf of regulated entities, and as such, the security and integrity of our infrastructure is of paramount importance.

Instant Compliance has adopted the DSS-1200 framework to govern its security posture. The DSS-1200 is a modern security standard designed as a comprehensive superset of legacy frameworks, encompassing the core principles of SOC 2 and ISO 27001 whilst incorporating additional controls for cloud-native infrastructure, AI governance, and software supply chain security.

This self-assessment was conducted by executive leadership against all 12 DSS-1200 domains. The assessment reflects the operational state of the Instant Compliance platform as of 28 April 2026. All 12 domains have been assessed and controls are in place or actively managed.

> **About this Report:** This is a DSS-1200 Self-Assessment Report, prepared and attested to by the management of Instant Compliance Pty Ltd. It documents the organisation's security controls, infrastructure architecture, and data handling practices against the DSS-1200 framework.

SECTION 02

System Overview & Architecture

Instant Compliance operates a modern, cloud-native architecture designed for high availability, strict data residency compliance, and defence-in-depth security. All production infrastructure is hosted within Australia to ensure compliance with Australian privacy and data sovereignty requirements.

2.1 Infrastructure & Hosting

COMPONENT	TECHNOLOGY	LOCATION	PURPOSE
Application Hosting	Vercel (Edge Network)	Sydney, Australia	Frontend & API layer with built-in DDoS mitigation
Primary Database	PostgreSQL via Prisma 6.4	AWS ap-southeast-2 (Sydney)	Primary data store for all application records
File Storage	AWS S3	AWS ap-southeast-2 (Sydney)	Secure storage for PDFs, KYC documents, and compliance artefacts
Background Processing	AWS Lambda	AWS ap-southeast-2 (Sydney)	Asynchronous and scheduled background jobs

2.2 Identity & Authentication

COMPONENT	TECHNOLOGY	NOTES
Session Management	NextAuth.js v5 + @auth/prisma-adapter	Sessions stored securely in PostgreSQL
OAuth Providers	Google OAuth, Microsoft OAuth	Leverages provider-managed MFA
Email/Password Auth	NextAuth.js credential provider	Passwords hashed using bcrypt
KYC/KYB Verification	Sumsub WebSDK	Identity verification for end-customer onboarding

2.3 Third-Party Sub-Processors

The following third-party services are utilised in the delivery of the Instant Compliance platform. Each sub-processor has been selected based on their demonstrated security posture and contractual data protection commitments.

SUB-PROCESSOR	PURPOSE	DATA PROCESSED
Stripe	Billing & subscription management	Payment card data (PCI DSS compliant)
Anthropic (Claude API)	AI-driven compliance analysis	Compliance document content
HubSpot	Customer relationship management	Contact and account information
Ably	Real-time pub/sub notifications	Application event data
PostHog	Product analytics	Anonymised usage events
Google Calendar API	Scheduling integrations	Calendar event metadata
Nodemailer / Resend	Transactional email delivery	Email addresses and notification content
Sumsub	KYC/KYB identity verification	Identity documents and biometric data

2.4 Infrastructure Security Pedigree

Instant Compliance operates on a foundation of independently verified trust. Every infrastructure provider and sub-processor in our stack holds independent, third-party security certification. The following table details the security pedigree of our supply chain.

PROVIDER	SECURITY TIER	VERIFIED CERTIFICATIONS
AWS	Tier 1: Enterprise Grade	SOC 2 Type 2, ISO 27001, PCI DSS, FedRAMP, GDPR, HIPAA
Vercel	Tier 1: Enterprise Grade	SOC 2 Type 2, ISO 27001, PCI DSS v4.0, GDPR, HIPAA
Stripe	Tier 1: Enterprise Grade	SOC 2 Type 2, PCI DSS Level 1
Anthropic	Tier 1: Enterprise Grade	SOC 2 Type 2, ISO 27001, FedRAMP, HIPAA, CSA STAR
Sumsub	Tier 1: Enterprise Grade	SOC 2 Type 2, ISO 27001, PCI DSS, GDPR
HubSpot	Tier 1: Enterprise Grade	SOC 2 Type 2, HIPAA, GDPR
PostHog	Tier 1: Enterprise Grade	SOC 2 Type 2, GDPR, HIPAA
Ably	Tier 1: Enterprise Grade	SOC 2 Type 2, HIPAA, GDPR
Resend	Tier 1: Enterprise Grade	SOC 2 Type 2, GDPR

SECTION 03

Risk Management & Treatment Plan

Instant Compliance maintains a formal risk management programme to identify, assess, and mitigate risks to the confidentiality, integrity, and availability of customer data. Risks are evaluated based on their likelihood of occurrence and potential impact, resulting in a risk score that dictates the required treatment strategy.

3.1 Risk Register & Treatment Summary

The following table summarises the primary risks identified in our current operating environment and the corresponding treatment plans implemented to mitigate them to an acceptable level.

RISK ID	RISK DESCRIPTION	INHERENT RISK	TREATMENT STRATEGY & CONTROLS	RESIDUAL RISK
RSK-01	Unauthorised access to production database containing sensitive KYC data.	High	**Mitigate:** Database is isolated within a private VPC. Access requires VPN and MFA. Strict RBAC enforced. No public endpoints exposed.	Low
RSK-02	Data loss due to infrastructure failure or ransomware attack.	High	**Mitigate:** Automated daily backups of PostgreSQL database. Backups stored in geographically redundant S3 buckets with versioning enabled to prevent malicious deletion.	Low
RSK-03	Vulnerabilities introduced via third-party open-source dependencies.	Medium	**Mitigate:** Automated dependency scanning integrated into CI/CD pipeline. Build fails if high/critical CVEs are detected. Regular dependency updates scheduled.	Low
RSK-04	Exposure of sensitive data via AI analysis API (Anthropic).	Medium	**Mitigate:** Enterprise API agreement in place ensuring zero data retention for model training. Data payloads strictly scoped to minimum required context.	Low
RSK-05	DDoS attack causing platform unavailability.	Medium	**Transfer/Mitigate:** Leveraged Vercel's edge network infrastructure which provides inherent, globally distributed DDoS mitigation and WAF capabilities.	Low

SECTION 04

Business Continuity & Disaster Recovery

Instant Compliance has established a Business Continuity and Disaster Recovery (BCP/DR) plan designed to ensure the rapid restoration of services in the event of a catastrophic failure, natural disaster, or significant security incident.

4.1 Architecture Resilience

Our cloud-native architecture is inherently designed for resilience. The frontend application is deployed across Vercel's globally distributed edge network, ensuring high availability even if specific regional nodes experience degradation. Our primary AWS infrastructure (PostgreSQL and S3) is deployed across multiple Availability Zones (AZs) within the ap-southeast-2 (Sydney) region, providing redundancy against single-datacenter failures.

4.2 Recovery Objectives

We have defined and tested the following recovery objectives for our core platform services:

- **Recovery Time Objective (RTO):** 4 Hours. This is the maximum acceptable duration of time that the application can be offline following a declared disaster before services must be restored.
- **Recovery Point Objective (RPO):** 1 Hour. This represents the maximum acceptable amount of data loss measured in time. Our automated backup schedule ensures that we can restore the database to a state no older than one hour prior to the incident.

4.3 Backup & Restoration Procedures

The PostgreSQL database undergoes automated, continuous backups. Transaction logs are archived every 5 minutes, and full snapshots are taken daily. These backups are stored in a separate, secured AWS S3 bucket with versioning enabled to protect against accidental or malicious deletion. Restoration procedures are documented in our engineering runbooks and are tested annually via simulated disaster recovery tabletop exercises.

SECTION 05

Human Resources Security Controls

Security at Instant Compliance begins with our personnel. We maintain strict human resources security controls to ensure that all employees and contractors understand their responsibilities and are vetted appropriately before being granted access to company systems or customer data.

5.1 Background Screening

Prior to employment, all prospective employees and contractors undergo a comprehensive background screening process, commensurate with their role and the level of access they will require. This process includes:

- Verification of identity and right to work in Australia.
- Verification of employment history and professional references.
- National Police Check (criminal history screening) for all personnel with access to production systems or sensitive customer data.

5.2 Security Awareness Training

All personnel are required to complete a formal security awareness training programme upon hire, and annually thereafter. The training curriculum covers:

- Phishing and social engineering awareness.
- Secure password management and MFA requirements.
- Data privacy principles (including the Privacy Act 1988) and the handling of sensitive KYC/AML data.
- Incident reporting procedures.

Completion of this training is tracked and logged by the HR department. Failure to complete mandatory training results in the suspension of system access.

5.3 Onboarding & Offboarding Procedures

Instant Compliance utilises documented checklists for both the onboarding and offboarding of personnel to ensure consistent application of security controls.

- **Onboarding:** Access to systems is granted strictly on a role-based, least-privilege basis. All new accounts require MFA configuration before initial login. Employees must formally acknowledge the Acceptable Use Policy and Information Security Policy.

- **Offboarding:** Upon termination of employment (voluntary or involuntary), a documented offboarding checklist is executed. All system access, including email, Slack, AWS, and GitHub, is revoked within 24 hours of the termination date. Company-issued hardware is remotely wiped and recovered.

SECTION 06

Vulnerability Management Programme

Instant Compliance operates a continuous vulnerability management programme to proactively identify, assess, and remediate security weaknesses in our application code, third-party dependencies, and cloud infrastructure.

6.1 Continuous Automated Scanning

We utilise industry-leading automated scanning tools integrated directly into our CI/CD pipeline to ensure that vulnerabilities are caught before they reach production.

- **Dependency Scanning:** Our codebase relies on various open-source libraries (e.g., NextAuth.js, Prisma). We utilise automated Software Composition Analysis (SCA) tools to continuously scan our dependency tree against known vulnerability databases (such as the NVD). If a high or critical CVE is detected in a dependency, the build pipeline is automatically halted until the dependency is updated or patched.
- **Static Application Security Testing (SAST):** Source code is automatically scanned during the pull request process to identify common security flaws, such as hardcoded secrets, injection vulnerabilities, and cross-site scripting (XSS) risks.

6.2 Recent Audit & Remediation

Prior to the issuance of this report, a comprehensive, full-stack security audit was conducted using our automated vulnerability management platform. This audit encompassed both application-level dependencies and infrastructure-as-code configurations.

The audit identified a small number of high-severity vulnerabilities within outdated third-party NPM packages. In accordance with our vulnerability management SLAs, the engineering team immediately triaged these findings, updated the affected packages to their secure versions, and deployed the patches to production. A subsequent re-scan confirmed that all identified high and critical vulnerabilities were successfully remediated, resulting in a clean security posture baseline.

6.3 Remediation SLAs

When vulnerabilities are identified, they are prioritised based on their CVSS score and exploitability in our specific environment. We adhere to the following Service Level Agreements (SLAs) for remediation:

- **Critical Severity:** Remediated within 48 hours of discovery.
- **High Severity:** Remediated within 14 days of discovery.

- **Medium Severity:** Remediated within 30 days of discovery.

SECTION 07

DSS-1200 Domain Assessment

The following section details the security controls implemented by Instant Compliance across all 12 domains of the DSS-1200 framework. Each domain has been assessed against the relevant criteria and a status determination has been made.

D-01 Governance & Risk Management

✓ Satisfactory

Instant Compliance maintains a formal security programme overseen by the Chief Executive Officer (Simon Giles) and Chief Technology Officer (Mike Giles). Security responsibilities are clearly delineated between executive leadership and engineering. A formal risk register is maintained and reviewed regularly to identify, evaluate, and mitigate threats to the platform. Security considerations are embedded into product planning and engineering decisions at the outset of each development cycle.

D-02 Identity & Access Management

✓ Satisfactory

Access to production infrastructure — including AWS, Vercel, and the PostgreSQL database — is strictly limited to authorised engineering personnel operating under the principle of least privilege. All production access requires multi-factor authentication (MFA). Customer authentication is secured via NextAuth.js with session data stored in the database. OAuth integrations with Google and Microsoft delegate authentication to those providers' enterprise-grade identity platforms, which enforce MFA at the provider level. Access rights are reviewed periodically and revoked promptly upon personnel changes.

D-03 Data Protection & Privacy

✓ Satisfactory

All customer data, including database records and S3-stored documents, is encrypted at rest using AES-256 encryption. All data in transit between the client, the Vercel edge network, and AWS infrastructure is encrypted using TLS 1.2 or higher. Data residency is strictly maintained within Australia (AWS ap-southeast-2 and Vercel Sydney deployment region), ensuring compliance with Australian data sovereignty requirements. AWS S3 buckets are configured to block all public access; file retrieval requires authenticated, time-bound presigned URLs generated by the application backend, ensuring that no document is ever directly accessible without authorisation.

D-04 Infrastructure & Network Security

✓ Satisfactory

The Vercel deployment platform provides inherent DDoS protection and Web Application Firewall (WAF) capabilities at the edge network layer, protecting the application from volumetric attacks and common web exploits. AWS security group configurations are maintained to restrict inbound traffic to only the ports and protocols required for application operation. Administrative access to infrastructure is never exposed to the public internet. Environment separation is enforced, with development, staging, and production environments maintained as distinct, isolated configurations.

D-05 Application & Software Security (DevSecOps)

✓ Satisfactory

Security is integrated directly into the software development lifecycle at Instant Compliance. All code changes require peer review and approval before being merged into the production branch. The codebase and its full dependency tree are subjected to automated security scanning. A comprehensive vulnerability audit was conducted prior to the issuance of this report; all identified high-severity vulnerabilities were successfully remediated, resulting in a clean scan result. Secrets and API keys are managed via environment variables and are never committed to source control.

D-06 Cloud & Container Security

✓ Satisfactory

Instant Compliance utilises managed, serverless infrastructure via Vercel and AWS Lambda, which abstracts underlying operating system management and patching responsibilities to the respective cloud providers. This architecture significantly reduces the attack surface compared to traditional virtual machine deployments, as there are no persistent servers requiring manual patching or hardening. AWS Lambda functions are assigned IAM roles with the minimum permissions required to execute their specific tasks, adhering strictly to the principle of least privilege at the compute layer.

D-07 AI & Emerging Technology Security

✓ Satisfactory

Instant Compliance utilises the Anthropic Claude API for AI-driven compliance analysis. Data submitted to the API is strictly scoped to the minimum context required for the analysis task. We rely on Anthropic's enterprise data privacy commitments, under which customer data submitted via the API is not used to train or improve their foundational models. AI-generated outputs are treated as advisory and are subject to human review within the compliance workflow, ensuring that no automated AI decision is presented to a customer as a definitive legal determination without appropriate context.

D-08 Supply Chain & Third-Party Risk

✓ Satisfactory

Third-party software dependencies are continuously monitored for known vulnerabilities via automated SCA tools, which provide alerts and remediation guidance when new CVEs are identified in the dependency tree. Sub-processors are selected based on their ability to demonstrate robust security postures; key sub-processors including Stripe (PCI DSS Level 1), Anthropic, and Vercel maintain their own rigorous security certifications. Data Processing Agreements (DPAs) are in place with all sub-processors that handle personal data on behalf of Instant Compliance customers.

D-09 Incident Response & Resilience

✓ Satisfactory

The distributed, serverless architecture of the Instant Compliance platform provides inherent high availability and resilience against localised infrastructure failures. The PostgreSQL database is configured with automated backups, enabling data recovery in the event of an incident, with a defined RTO of 4 hours and RPO of 1 hour. An incident response process is maintained by the engineering team, with defined escalation paths to executive leadership. Application errors and anomalies are monitored in real-time, enabling rapid detection and response to potential security events.

D-10 Physical & Environmental Security

✓ Satisfactory

Instant Compliance operates as a cloud-native company and does not maintain physical data centres or server rooms. Physical and environmental security for all production infrastructure is managed entirely by our cloud providers (AWS and Vercel), both of whom maintain rigorous physical security controls that are independently audited under SOC 2 and ISO 27001. For endpoint security, company devices used to access production systems are required to have full-disk encryption enabled and strong authentication configured.

D-11 Compliance & Legal Obligations

✓ Satisfactory

Instant Compliance is designed specifically to assist regulated entities with their obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) and the AUSTRAC regulatory framework. The platform is built with an inherent understanding of Australian privacy principles under the Privacy Act 1988, and the handling of all personal information — including KYC and KYB data collected via Sumsub — is conducted in accordance with those principles. Legal and regulatory obligations are reviewed by executive leadership on an ongoing basis.

D-12 Continuous Monitoring & Threat Intelligence

✓ Satisfactory

Application performance, errors, and security-relevant events are monitored continuously. PostHog provides visibility into application usage patterns, enabling the detection of anomalous behaviour. Vercel's platform provides real-time logging and alerting for edge network events. Automated scanning tools provide continuous monitoring of the dependency tree for newly disclosed vulnerabilities, ensuring that the engineering team is promptly notified of any emerging supply chain risks that require remediation.

SECTION 08

Assessment Summary

The following table summarises the outcome of the DSS-1200 self-assessment across all 12 domains.

DOMAIN	NAME	STATUS	NOTES
D-01	Governance & Risk Management	✓ Satisfactory	Executive-led security programme and risk register in place
D-02	Identity & Access Management	✓ Satisfactory	MFA enforced; least-privilege access model
D-03	Data Protection & Privacy	✓ Satisfactory	AES-256 at rest; TLS 1.2+ in transit; AU data residency
D-04	Infrastructure & Network Security	✓ Satisfactory	WAF & DDoS protection via Vercel; no public admin ports
D-05	Application & Software Security	✓ Satisfactory	Automated audit completed; all high CVEs remediated
D-06	Cloud & Container Security	✓ Satisfactory	Serverless architecture; least-privilege IAM roles
D-07	AI & Emerging Technology Security	✓ Satisfactory	Anthropic API; no training data exposure
D-08	Supply Chain & Third-Party Risk	✓ Satisfactory	Continuous monitoring; DPAs with all sub-processors
D-09	Incident Response & Resilience	✓ Satisfactory	Automated DB backups; defined RTO/RPO and response process
D-10	Physical & Environmental Security	✓ Satisfactory	Cloud-native; physical security delegated to AWS/Vercel
D-11	Compliance & Legal Obligations	✓ Satisfactory	AML/CTF Act; Privacy Act 1988 compliance
D-12	Continuous Monitoring	✓ Satisfactory	Real-time monitoring via Vercel, PostHog, automated scanners

Overall Assessment Result: All 12 DSS-1200 Domains Satisfactory. No domain was assessed as failing or requiring immediate remediation as of the date of this report.

SECTION 09

Management Attestation

I, Simon Giles, Chief Executive Officer of Instant Compliance Pty Ltd (ACN 111 744 668), hereby attest that the security controls, architectural details, and operational practices described in this DSS-1200 Self-Assessment Report are accurate and reflect the operational state of the Instant Compliance platform as of 28 April 2026.

This assessment has been conducted in good faith against the Detailed Security Standard (DSS-1200) framework. Instant Compliance Pty Ltd is committed to the continuous improvement of its security posture to protect our customers, their data, and the integrity of the Australian financial services businesses that rely on our platform.

Simon Giles

Simon Giles
Chief Executive Officer, Instant Compliance Pty Ltd
28 April 2026