Enterprise Security & Audit Readiness Vault

Done-For-You 72-Hour Deliverable Preview & Architecture Specification

Supervising Technical Architect:	Acey Squire (Lead Architect & Founder)
Operating Jurisdiction:	London, United Kingdom · Independent Technical Security Advisory Desk
Compliance Standards Aligned:	AICPA SOC 2 Type II · ISO/IEC 27001:2022 · CSA CAIQ v4 · SIG Lite
Turnaround SLA:	72 Hours Standard SLA · Covered by 14-Day Revision Support Guarantee
Confidentiality Protocol:	Mutual NDA Enforced · Strictly Confidential Architecture Processing

EXECUTIVE OVERVIEW:
This sample document demonstrates the structural depth, audit standards conformity, and technical precision embedded in every Done-For-You Enterprise Security & Audit Readiness Vault compiled by The Runbook Index. When high-growth B2B technology providers encounter extensive enterprise vendor security questionnaires from Tier-1 clients, enterprise risk committees demand far more than generic template text. They demand verifiable cloud architecture controls, KMS key rotation procedures, strict RTO/RPO SLAs, and human-supervised operational runbooks.

THE 5 BESPOKE MODULES DELIVERED IN EVERY VAULT:

Module	Deliverable Scope	Format
IR-01	Incident Response Runbook (P0–P3 matrices, 15m escalation, evidence preservation)	Word + Markdown
INFOSEC-01	Master Information Security Policy (35+ pages, Access Control, KMS, SSDLC)	Word (.docx)
BCDR-01	Business Continuity & Disaster Recovery Plan (60m RTO / 5m RPO multi-region failover)	Word + Excel
SEC-EVAL-01	Pre-Filled Enterprise Security Assessment (90%+ pre-completed CAIQ / SIG Lite answers)	Excel (.xlsx)
VRM-01	Vendor Risk & Sub-Processor Heatmap (Supply chain scoring across AWS/Stripe/OpenAI)	Excel (.xlsx)

MODULE IR-01: BESPOKE INCIDENT RESPONSE RUNBOOK

Section 3.2: Technical Severity Classification & Escalation Matrix

Every incident is categorized against four formal severity levels to ensure appropriate technical escalation, cross-functional notification, and regulatory breach disclosure timelines:

Severity	Impact Scope	War Room SLA	Customer Notice
P0 Critical	Active production outage; confirmed data breach; cryptographic key compromise.	**Immediate (≤ 15 mins)**	≤ 60 mins (Status Page)
P1 High	Core subsystem degraded; redundancy failover operating on single AZ; elevated error rates.	**≤ 30 mins**	≤ 2 hours
P2 Medium	Non-critical service degradation; internal tool failure; secondary sub-processor offline.	**≤ 2 hours**	As required
P3 Low	Minor bug; cosmetic UI defect; non-exploitable automated vulnerability scanner flag.	**Next Business Day**	Release Notes

Section 4.1: Live Incident Commander Protocol & Evidence Preservation

1. War Room Mobilization: The Incident Commander immediately spawns an encrypted voice bridge and dedicated incident Slack/Teams channel. All ad-hoc communication outside the designated channel is forbidden to maintain a clean timeline.

2. Forensics & Forensic Snapshots: Before any server reboot or remediation container termination, memory dumps and immutable AWS EBS / GCP disk snapshots must be taken with SHA-256 checksums logged for auditor inspection.

3. Regulatory Disclosure Clock: Under UK GDPR Article 33 and EU GDPR, any confirmed breach involving personal data triggers a mandatory 72-hour notification clock to the Information Commissioner's Office (ICO).

MODULE SEC-EVAL-01: PRE-FILLED QUESTIONNAIRE ANSWERS

Enterprise CAIQ v4 & SIG Lite 2026 Pre-Filled Sample

Below is an illustrative sample of evidence-backed draft responses compiled by our desk, demonstrating the level of technical detail enterprise procurement teams evaluate:

Standard Ref / Question	Illustrative Evidence-Backed Draft Response
CAIQ CRY-01 ***How are data encryption keys managed and rotated?***	All cryptographic keys are provisioned and managed via AWS Key Management Service (KMS) backed by FIPS 140-2 Level 3 validated Hardware Security Modules (HSMs). Keys undergo automated 365-day rotation. Strict separation of duties is enforced between KMS Key Administrators and cryptographic users via IAM policies requiring multi-factor authentication (MFA).
SIG BCDR-04 ***What are your verified production RTO and RPO metrics?***	Production recovery targets are formally specified as **RTO ≤ 60 minutes** and **RPO ≤ 5 minutes**. Database transactions are replicated synchronously across three Availability Zones with automated 5-minute incremental WAL archive streaming to an encrypted, immutable S3 bucket.
SOC2 CC6.1 ***How is technical access to production environments restricted?***	Zero direct password or long-lived SSH access to production instances is permitted. Engineering access is brokered through an Identity Provider (Okta/Google Workspace) enforcing hardware WebAuthn (FIDO2) MFA, short-lived ephemeral certificates (8-hour TTL), and just-in-time role escalation requiring secondary peer approval.
SIG VENDOR-02 ***How do you conduct third-party penetration testing?***	Annual grey-box penetration tests are conducted by independent CREST-accredited security firms. High-severity vulnerabilities require remediation within 14 calendar days; medium vulnerabilities within 30 days. Full executive penetration test summaries are made available to enterprise clients under mutual NDA.

READY TO CLOSE YOUR ENTERPRISE DEAL IN 72 HOURS?
Deploy your customized Done-For-You Vault for a one-time £1,950 fee.

hello@runbookindex.com
runbookindex.com