PORTFOLIO PROJECT 4 — PART A OF 2

Information Security Management System

Part A: ISMS Manual, Scope, and Risk Assessment — Rockops Protection Agency (ISO/IEC 27001:2022)

Prepared by J Damien Scott, SRMP GRCP

July 2026

Portfolio note. Rockops Protection Agency is a fictional physical security and executive protection firm invented for this project. No real company, client, or individual is described. Domain availability referenced in Part B was checked against a live registrar on the date of writing to keep the example realistic; no domain was purchased and no Google Workspace tenant was created. This document and its companion, Part B: Google Workspace Deployment and Security Configuration Runbook, together form a single ISMS build and should be read as a pair.

Table of Contents

1. Purpose and Definitions

An Information Security Management System (ISMS) is a documented, risk-based framework, defined in ISO/IEC 27001, by which an organization governs the confidentiality, integrity, and availability of its information. The standard does not mandate specific technology; it mandates a management process: a defined scope, a policy, a risk assessment, a set of controls selected to treat identified risks, and a cycle of review. This document is Part A of a two-part ISMS build for a composite organization, Rockops Protection Agency. It establishes the governance layer: scope, policy, roles, risk assessment, and the Statement of Applicability (SoA) that ISO/IEC 27001 Clause 6.1.3(d) requires. Part B translates the technological controls named here into a specific, sequenced configuration of Google Workspace, the productivity platform Rockops has chosen, performed inside the Google Admin console.

A note on claim types, consistent with the rest of this portfolio. A fact is verifiable against a primary source, here principally the published structure of ISO/IEC 27001:2022 Annex A and Google's own product documentation. Evidence supports an interpretation without settling it alone, such as a single vendor blog's framing of a pricing tier. Interpretation is my reading of what the evidence means for Rockops specifically. Judgment is an evaluative claim about adequacy, such as whether a control is proportionate to Rockops' risk. A recommendation is an action I suggest Rockops' leadership take. Section 4 in particular turns on a judgment call, the choice of Google Workspace edition, and I mark it as such rather than presenting it as a foregone conclusion.

2. Organizational Context

Rockops Protection Agency is a composite, fictional physical security and executive protection firm with approximately 125 employees, organized roughly as follows: executive leadership and corporate functions including finance, sales, and human resources (about 15 people); operations and dispatch, who coordinate guard posts and client communications from a central office (about 10 people); field protection agents and security officers, who staff client sites and executive protection details (about 85 people, the large majority of the headcount); a small IT and security administration function (about 5 people); and a training and licensing compliance team (about 5 people). Field agents are issued no corporate mobile hardware; Rockops permits Bring Your Own Device (BYOD) for this population, who use personal smartphones to receive schedules, file incident reports, and communicate through the company's Google Workspace environment while working, often alone, at client sites.

This context matters for two reasons that recur throughout this document. First, the information Rockops handles is unusually sensitive for a company of its size: client site security assessments and floor plans, alarm and access codes, executive protection principals' schedules and residential details, and the guard force's own background-check and firearms-licensing records. A security company is, in a real sense, in the business of being trusted with other people's secrets, and an information security failure at Rockops carries physical safety consequences, not just financial ones. Second, the workforce that handles the

most sensitive information, field agents, is also the workforce least likely to be sitting at a managed corporate workstation behind a corporate firewall. The BYOD reality is not a side issue for this ISMS; it is close to the center of it, which is why Part B gives endpoint management for personal devices more sustained attention than a typical small-business Workspace deployment would.

2.1 ISMS Scope Statement

The scope of this ISMS is the Google Workspace productivity and collaboration environment (Gmail, Drive, Calendar, Chat, and Meet) used by all Rockops personnel, including field agents accessing that environment from personal, BYOD-enrolled devices, together with the identity, access, and device-management controls that govern it. Excluded from this phase of the ISMS: the physical access control and alarm systems installed at client sites, which are owned and operated by clients and are addressed through contractual security requirements rather than through Rockops' own technical controls, and Rockops' physical office premises security (badging, CCTV, visitor control), which falls under Annex A's Physical Controls theme and is noted in Section 6 as a planned second-phase scope extension rather than addressed in technical depth here. This is a judgment call about sequencing, not a claim that physical premises security is unimportant: a 125-person company implementing its first ISMS gets the most immediate risk reduction from securing the single platform nearly everyone touches every day.

3. Information Security Policy

This is the top-management policy statement required by ISO/IEC 27001 Clause 5.2. Rockops Protection Agency commits to protecting the confidentiality of client security information and personnel records, the integrity of dispatch, scheduling, and incident-reporting data, and the availability of field communications, in proportion to the harm that a failure in any of these three properties would cause to a client, an employee, or the business. This policy applies to all employees, contractors, and personal devices enrolled for business use, and it is reviewed at least annually or after any significant change to Rockops' Google Workspace configuration, headcount, or client contract terms.

3.1 Roles and Responsibilities (RACI)

Activity	Managing Director (Exec. Sponsor)	ISMS Manager (collateral duty)	IT / Workspace Super Admin	Operations Director	H R
Approve and review the Information Security Policy	A	R	C	C	C
Maintain the risk register (Section 5)	I	A	R	R	C
Own the Statement of Applicability (Section 6)	A	R	C	I	I

Activity	Managing Director (Exec. Sponsor)	ISMS Manager (collateral duty)	IT / Workspace Super Admin	Operations Director	HR
Configure and maintain Google Workspace controls (Part B)	I	C	A / R	C	I
Personnel screening and termination offboarding	I	C	R	C	A
Incident response for an information security event	A	R	R	R	C
Annual management review of the ISMS	A	R	C	C	C

At 125 employees, Rockops does not have a dedicated Chief Information Security Officer, and this table assumes that role is a collateral duty held by a senior operations or IT leader, an ISMS Manager, who reports to the Managing Director. This is a realistic and defensible structure for a company this size; ISO/IEC 27001 Annex A 5.2 requires that roles be assigned and understood, not that a company of 125 people carry a full security executive headcount.

4. Platform Decision: Google Workspace Edition (Judgment Call)

Rockops has already selected Google Workspace as its productivity platform; the open decision this ISMS had to resolve was which edition. This section documents that judgment because it drives several of the technical controls in Part B and because a hiring panel or an auditor should expect the reasoning to be explicit, not assumed.

As of July 2026, Google Workspace offers four self-service business tiers, Business Starter, Business Standard, Business Plus, and Enterprise, plus a custom-priced Enterprise tier with no user cap (Google Workspace, 2026). Business Starter, Standard, and Plus are each capped at 300 users; Rockops' 125 employees fit comfortably within that ceiling with room to grow. The material difference for a security-sensitive company is at the top of that range: Business Plus adds Vault (retention, legal hold, and eDiscovery), 5 terabytes of pooled storage per user, S/MIME encryption, and "Advanced" endpoint management, while native Data Loss Prevention (DLP) and Context-Aware Access are reserved for the Enterprise tier, which is priced through custom negotiation rather than published self-service pricing (Google Workspace, 2026; Qualtir, 2026).

Recommendation: Rockops should provision Business Plus, not Enterprise, for all 125 users. This is the greatest-return-on-investment position available: Business Plus's Advanced endpoint management, detailed in Part B Section 6, delivers the specific controls a BYOD security workforce needs most, namely enforced work-profile separation, encryption and screen-lock requirements as a condition of corporate data access, and remote wipe of corporate data only, without the cost and procurement overhead of an Enterprise contract. Vault satisfies the record-retention obligations a security company should expect to face given the litigation exposure inherent in the industry (Annex A 5.33, Protection of records). The tradeoff, and it is a real one, is that Business Plus does not include native DLP or Context-Aware Access. Part B

Section 8 documents the compensating controls Rockops puts in place instead, and Section 6.2 below sets an explicit trigger for revisiting this decision.

4.1 Upgrade Trigger

Rockops should re-evaluate Enterprise Standard, specifically for its native DLP and Context-Aware Access, if any of the following occurs: headcount approaches 250 (leaving inadequate headroom under the 300-user Business-tier cap), a client contract explicitly requires documented DLP controls as a condition of the engagement, or a security incident traced to Drive external sharing occurs despite the compensating controls in Part B. Absent one of those triggers, Business Plus is the defensible, cost-proportionate choice for a company of this size and risk profile.

5. Risk Assessment

5.1 Methodology

Risks are scored on a five-point likelihood and impact scale (1 = low, 5 = high), consistent with the methodology used across this portfolio so that scores are comparable across projects. Inherent risk is likelihood multiplied by impact before controls; residual risk reflects the score after the mitigation named in the register is implemented.

5.2 Risk Register

ID	Risk	L	I	Inh.	Mitigation	Res.	Annex A Ref.
R-01	A field agent's personal phone is lost or stolen while a client's site security plan is accessible in Gmail or Drive.	4	5	20	Advanced endpoint management enforces screen lock and encryption as a condition of access; remote corporate-data wipe on report of loss (Part B, Section 6).	6	A.8.1, A.7.9
R-02	A phishing email targeting dispatch staff compromises a client's protection-detail schedule.	4	5	20	Gmail advanced phishing protection, 2-Step Verification enforcement, and security-awareness training (Part B, Section 5; Section 7 below).	6	A.8.5, A.6.3
R-03	A field agent forwards work email to a personal, non-Workspace account for convenience.	3	4	12	Automatic forwarding to external domains disabled by default at the domain level (Part B, Section 5).	3	A.5.14, A.8.12
R-04	A departing employee retains access to Gmail, Drive, or Chat after termination.	3	5	15	Offboarding runbook: immediate suspension and BYOD corporate-data wipe within a defined time target (Part B, Section 10).	3	A.6.5, A.5.18

ID	Risk	L	I	Inh.	Mitigation	Res.	Annex A Ref.
R-05	A shared Drive folder containing a client's floor plans is set to "Anyone with the link."	4	4	16	External sharing restricted by default at the domain level; sensitive folders held in Shared Drives with membership managed by Operations, not ad hoc individual sharing (Part B, Section 8).	4	A.8.12, A.5.15
R-06	A disgruntled or terminated guard exfiltrates client PII before an offboarding action completes.	2	5	10	Time-bound offboarding target and mass-download alerting in the Admin console alert center (Part B, Sections 9 and 10).	4	A.8.16, A.6.5
R-07	Weak or reused passwords on personal Google accounts used for BYOD access.	3	3	9	2-Step Verification enforced org-wide; security keys required for the IT Admin and Executive OUs (Part B, Section 5).	2	A.5.17, A.8.5
R-08	An unmanaged personal device with an outdated OS accesses corporate Gmail and Drive.	3	3	9	Advanced endpoint management blocks access from devices below a minimum OS version (Part B, Section 6).	2	A.8.1
R-09	A vishing caller impersonating a client requests an unscheduled change to a protection detail's route.	3	4	12	Security-awareness training covering social engineering; verification callback procedure documented in the operations runbook.	3	A.6.3, A.6.8
R-10	Background-check and firearms-licensing records held in Drive are accessible beyond HR.	2	5	10	Sensitive HR records held in a restricted-access Shared Drive with named membership; classification labeling per Rockops' data-handling standard.	3	A.5.12, A.8.3

Column key: L = Likelihood (1–5), I = Impact (1–5), Inh. = Inherent risk score, Res. = Residual risk score after the listed mitigation. Annex A Ref. cites the ISO/IEC 27001:2022 Annex A control(s) most directly engaged.

6. Statement of Applicability

ISO/IEC 27001:2022 Annex A organizes 93 controls into four themes: Organizational (37 controls, A.5.1–A.5.37), People (8 controls, A.6.1–A.6.8), Physical (14 controls, A.7.1–A.7.14), and Technological (34 controls, A.8.1–A.8.34) (International Organization for Standardization, 2022). A complete Statement of Applicability addresses all 93; the summary below groups them thematically, states applicability to Rockops' current scope, and, for the Technological theme, points to the specific Google Workspace configuration in Part B that implements the control. This is the document that ties governance to implementation: a control is not "done" because a policy names it, it is done because a configuration, a contract clause, or a trained behavior enforces it.

Theme	Applicable to Rockops' Scope	Representative Controls	Implementation Reference
Organizational (37)	Yes, in full	A.5.1 Policies; A.5.9 Asset inventory; A.5.14 Information transfer; A.5.15 Access control; A.5.23 Cloud services; A.5.33 Protection of records	This document (policy, roles); Part B Sections 5, 8, 9 (technical enforcement)
People (8)	Yes, in full	A.6.1 Screening; A.6.3 Awareness training; A.6.5 Termination responsibilities; A.6.7 Remote working	HR screening process (outside Workspace); Part B Section 10 (offboarding); annual awareness training program
Physical (14)	Partially, phase two	A.7.9 Security of assets off-premises (BYOD devices)	Part B Section 6 addresses A.7.9 directly. Office-premises controls (A.7.1–A.7.8, A.7.10–A.7.14) are out of scope for this phase; see Section 2.1.
Technological (34)	Yes, in full	A.8.1 Endpoint devices; A.8.5 Secure authentication; A.8.7 Malware protection; A.8.12 DLP; A.8.15 Logging; A.8.16 Monitoring; A.8.24 Cryptography	Part B, Sections 5 through 11 (the technical build), with a full cross-reference table in Part B, Section 12

7. Continual Improvement and Audit Cadence

ISO/IEC 27001 Clause 9.3 requires management review at planned intervals, and Clause 10.2 requires continual improvement following nonconformities. Rockops adopts the following cadence: a quarterly risk-register review by the ISMS Manager, an annual management review presented to the Managing Director covering the risk register, the Statement of Applicability, and any incidents from the preceding year, and an annual phishing-simulation exercise for all staff with results reported as a metric to leadership. Suggested key metrics: the percentage of BYOD devices enrolled in advanced endpoint management (target: 100 percent before any device accesses corporate Gmail or Drive), the phishing-simulation click rate (tracked over time, not judged against an absolute benchmark in year one), and the elapsed time between an HR termination notice and full account de-provisioning (target under one hour for for-cause terminations, detailed in Part B, Section 10).

8. Presenting This Project in an Interview

This project pairs a governance document (this one) with a technical implementation document (Part B) and shows the connective tissue between them explicitly: every technological control named in the Statement of Applicability points to a specific Admin console configuration, and every configuration in Part B points back to a specific Annex A control. In an interview, the strongest thread to walk is the Business Plus versus Enterprise decision in Section 4: it is a real, defensible, cost-conscious judgment call rather than a default answer, and being able to explain the accepted risk (no native

DLP) and its compensating control is exactly what a GRC or security-engineering interviewer is listening for.

References

Google Workspace. (2026). Compare flexible pricing plan options. https://workspace.google.com/pricing

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

Qualtir. (2026, June 8). Google Workspace plans: Which one is right for your business in 2026? https://qualtir.com/blog/google-workspace-plans-guide