PORTFOLIO PROJECT 4 — PART B OF 2

Google Workspace Deployment and Security Configuration Runbook

Part B: Rockops Protection Agency — Executed Inside the Google Admin Console

---

Prepared by J Damien Scott, SRMP GRCP

July 2026

Portfolio note. This runbook documents, at the level of specificity a live implementation would require, the exact sequence of actions inside the Google Admin console (admin.google.com) that a Google Workspace deployment for the fictional Rockops Protection Agency would follow. No real domain was purchased and no Google Workspace tenant was created; the domain named below was checked against a live registrar on the date of writing and confirmed available, purely to keep the example concrete, and no registration or payment was made. Admin console menu paths are accurate as of July 2026 and are the kind of detail Google periodically reorganizes; treat the underlying control, not the exact click path, as the durable claim.

Table of Contents

1. Purpose and Sequencing

Part A of this ISMS build established the policy, the risk register, and the Statement of Applicability. This document, Part B, is the technical half: the specific, ordered configuration of Google Workspace that implements the Technological controls Part A's Statement of Applicability names. The sequencing below follows the order a real deployment must follow, edition and domain decisions first, because identity, mail, and endpoint policy all depend on them, then organizational structure, then the security controls layered on top.

2. Edition Selection (Carried Forward from Part A)

Part A, Section 4 recommends Google Workspace Business Plus for all 125 users, chosen over Enterprise for its lower cost and adequate control set (Vault, Advanced endpoint management, S/MIME) given Rockops' size and risk profile, with native Data Loss Prevention and Context-Aware Access deferred to a documented upgrade trigger. This section carries that decision forward into the build: every license assigned in Section 5 below is a Business Plus license.

3. Domain Acquisition and Verification

Rockops selected the domain rockopsprotection.com. A live domain-availability lookup performed on the date of writing confirmed this domain unregistered and available; the closely related rockops.com was already registered by an unrelated third party, which is itself a useful illustration of why a due-diligence check before committing to a domain in writing or in marketing material is worth the five minutes it takes.

3.1 Steps Performed in the Admin Console

1. Register the domain rockopsprotection.com with an accredited registrar (outside the Admin console).
2. In the Admin console, navigate to Account > Domains > Manage domains, and select Add a domain.
3. Choose "Add a domain you already own" and enter rockopsprotection.com as the primary domain for the account.
4. Verify domain ownership using the TXT record method: the Admin console generates a unique TXT record value, which is added to the domain's DNS zone at the registrar. Google's verification tool confirms the record within minutes to 48 hours depending on DNS propagation.
5. Once verified, add the MX records the Admin console provides (five Google mail server records at the documented priority values) at the registrar, replacing any prior mail provider's MX records.

6. Add an SPF TXT record (v=spf1 include:_spf.google.com ~all) authorizing Google's mail servers to send on Rockops' behalf; this is a prerequisite for the DKIM and DMARC configuration in Section 5.

4. Organizational Unit Structure

Organizational Units (OUs) in Google Workspace let policy, licensing, and endpoint rules be scoped by role rather than applied identically to everyone, which matters here because field agents' BYOD risk profile is materially different from the corporate office's. The OU tree below is designed so that the highest-risk population, field agents, receives the tightest device policy without over-restricting the smaller corporate population.

Organizational Unit	Population	Rationale
/Rockops Protection Agency (root)	All users (default policy floor)	Baseline: 2-Step Verification required, external sharing restricted.
/Executive & Corporate	~15 (leadership, finance, HR, sales)	Security-key 2SV requirement; S/MIME enabled; broader Drive sharing latitude for external business development.
/Operations & Dispatch	~10 (central dispatch, scheduling)	Shared Drive access to all active client folders; elevated audit-log review.
/Field Protection Agents	~85 (BYOD, client-site personnel)	Advanced endpoint management enforced as a hard condition of Gmail/Drive/Chat access; tightest Drive sharing restriction.
/IT & Security Admin	~5 (Workspace administrators)	Security-key 2SV mandatory; custom admin roles, not blanket Super Admin, per Section 5.3.
/Training & Compliance	~5 (licensing, certification tracking)	Access to HR-adjacent records; restricted Shared Drive per Part A, R-10.
/Pending Onboarding	Variable (background check in progress)	Suspended or minimally licensed until HR clears the candidate; prevents premature access to client data.

5. User Provisioning and Identity Security

5.1 Bulk User Creation

With 125 initial users, individual account creation is impractical. In the Admin console, under Directory > Users > Bulk upload, an administrator uploads a CSV containing each employee's first name, last name, target email address (firstname.lastname@rockopsprotection.com), and target Organizational Unit from Section 4. The bulk upload assigns each account to its OU at creation, so OU-scoped policies in Sections 6 through 8 apply immediately without a separate move step.

5.2 2-Step Verification and Advanced Protection

1. Navigate to Security > Authentication > 2-step verification. Enforce 2SV for all organizational units at the root level, with a defined grace period (14 days) to allow field agents time to enroll a second factor on their personal device without being locked out mid-shift.
2. For the /Executive & Corporate and /IT & Security Admin OUs specifically, require a security key or passkey as the second factor rather than allowing SMS or a one-time-code app; these two OUs hold the highest-value credentials (financial approval, tenant administration) and are the population most worth protecting against SIM-swap and phishing-resistant-bypass attacks.
3. Enroll all designated Super Admin accounts (targeted at no more than two named individuals) in Google's Advanced Protection Program for the highest available account-takeover resistance.

5.3 Admin Roles: Least Privilege

Rather than granting Super Admin to every member of IT, Account > Admin roles is used to create two custom roles in addition to the default Super Admin: a Help Desk Admin role, scoped to password resets and 2SV re-enrollment only, for day-to-day support tickets, and a User Management Admin role, scoped to Directory and OU changes, for onboarding and offboarding staff. Super Admin is held by exactly two named individuals, consistent with the principle that the most powerful role should have the smallest population.

6. Endpoint Management for BYOD

This section is the technical core of the BYOD control set and the direct implementation of Part A's highest-scored risk, R-01. Because field agents are not issued corporate hardware, the objective is not device control in the traditional sense; it is separating corporate data from personal data on a device Rockops does not own and enforcing baseline hygiene as a condition of that corporate data being present at all.

1. In the Admin console, navigate to Devices > Mobile & endpoints > Settings, and set the management level to Advanced mobile management for the /Field Protection Agents, /Operations & Dispatch, and /IT & Security Admin OUs (Advanced management is included in Business Plus, per Part A, Section 4).
2. Require a work profile on Android devices (Android Enterprise "work profile" mode) and managed, user-enrolled configuration on iOS, rather than full device management, so Rockops policy applies only to the corporate-data container (Gmail, Drive, Chat, Calendar app data) and never touches the employee's personal photos, messages, or apps.
3. Set minimum requirements as a condition of corporate data sync: a device screen lock (PIN, pattern, or biometric), full-device encryption enabled, and a minimum OS version (a rolling window, for example the current major release and one prior). A device that

does not meet these is blocked from Gmail/Drive sync until it is updated, addressing Part A risk R-08.

4. Disable the ability to copy data from a managed work app (Gmail, Drive) into an unmanaged personal app on the same device. This is a direct, if partial, compensating control for the absence of native Enterprise-tier DLP: it cannot inspect content the way true DLP does, but it closes the most common accidental-leak path, copying a client site plan into a personal notes app.
5. Enable selective ("corporate data only") remote wipe, tested and documented in the offboarding runbook (Section 10), so a lost or stolen phone, or a terminated employee's phone, can have Rockops' Gmail, Drive, and Chat data and the managed work profile removed without touching the employee's personal data, an important distinction to communicate clearly in the BYOD policy agreement every field agent signs at onboarding.

7. Gmail Security Configuration

1. Complete DKIM: in Apps > Google Workspace > Gmail > Authenticate email, generate a DKIM key and publish the resulting TXT record at the domain registrar, then enable signing.
2. Configure DMARC: publish a DMARC TXT record starting at p=quarantine with reporting enabled (rua tag pointed to a monitored mailbox), moving to p=reject after a monitoring period confirms no legitimate mail is being misclassified. This sequencing avoids the common failure mode of jumping straight to p=reject and silently dropping legitimate client correspondence.
3. In Apps > Google Workspace > Gmail > Safety, enable enhanced pre-delivery message scanning, attachment sandboxing for suspicious file types, and external-sender warning banners, which directly address Part A risk R-02, phishing targeting dispatch staff.
4. Disable automatic forwarding to external, non-rockopsprotection.com addresses at the domain level (Apps > Google Workspace > Gmail > User settings), addressing Part A risk R-03.
5. Enable S/MIME for the /Executive & Corporate OU, where end-to-end message signing and encryption is most likely to be contractually or legally relevant.

8. Google Drive and Sharing Controls

1. In Apps > Google Workspace > Drive and Docs > Sharing settings, set external sharing to "Only people in the organization can be given access," overriding the default "Anyone with the link" option that most consumer Workspace deployments leave enabled.
2. Where a specific client relationship requires external collaboration, add that client's domain to an explicit allowlist rather than opening sharing broadly; this keeps the exception auditable and narrow.

3. Require that client-facing material, particularly site security assessments and floor plans, live in Shared Drives with membership managed by the Operations Director, rather than in an individual field agent's My Drive with ad hoc sharing. Shared Drive membership survives an individual's offboarding automatically, which also simplifies Section 10.
4. Configure an Admin console alert (Section 9) on abnormal mass-download activity from a Shared Drive, functioning as a compensating detective control for the DLP capability Business Plus does not include natively (Part A, Section 4.1).

9. Audit Logging, Alerts, and Monitoring

Reporting > Audit and investigation in the Admin console provides the log sources; Security > Alert center is where those logs become actionable. The alert rules below are the minimum set for a company handling Rockops' risk profile.

Alert Rule	Trigger	Response Owner
Suspicious login	Sign-in from an unrecognized location or impossible-travel pattern.	IT / Security Admin
2SV enrollment lapse	A user in a 2SV-required OU has not completed enrollment past the grace period.	IT Admin (Help Desk role)
Admin role change	Any change to Super Admin or custom admin role membership.	Managing Director (notified), IT Admin (executes)
Mass Drive download	A single user downloads an abnormal volume of files from a Shared Drive in a short window.	Operations Director, IT Admin
External sharing spike	A spike in files shared outside the allowlisted client domains.	IT Admin
Device compromised / rooted	Endpoint management detects a rooted or jailbroken BYOD device attempting sync.	IT Admin (device blocked automatically pending review)

10. Vault Retention and Legal Hold

In Apps > Google Workspace > Vault, retention rules are configured for Gmail and Chat: a default three-year retention period, chosen because a security services company should reasonably expect a client dispute or incident-related claim to surface within that window, and a litigation-hold workflow that HR or outside counsel can invoke on a specific custodian's account without altering that individual's day-to-day access. This satisfies Annex A 5.33, Protection of records, referenced in Part A's risk register and Statement of Applicability.

11. Offboarding Runbook

Given how much sensitive access sits on personal, BYOD-enrolled devices, offboarding is the single highest-leverage procedure in this entire build, directly addressing Part A risks R-04 and R-06. The target is full de-provisioning within one hour of an HR-issued, for-cause termination

notice, and by end of the employee's final working day for a standard, non-adversarial departure.

1. HR issues a termination notice to the IT Admin (User Management role) through the agreed notification channel, timestamped.
2. IT Admin suspends the account immediately in Directory > Users, which blocks sign-in without deleting the account or its data, preserving anything needed for a Vault-based legal hold.
3. IT Admin triggers a selective corporate-data wipe on the individual's enrolled BYOD device or devices through Devices > Mobile & endpoints, removing the managed work profile and all synced Gmail, Drive, and Chat data while leaving the employee's personal data untouched, consistent with the BYOD agreement referenced in Section 6.
4. Ownership of any files the departing employee owned in a personal My Drive (rare, given the Shared Drive requirement in Section 8, but possible) is transferred to their manager or the Operations Director before the account is fully deleted.
5. Security keys or registered 2SV factors tied to the account are revoked, and the account is removed from any admin role it may have held.
6. The account is fully deleted from Directory after the organization's standard data-retention window has been confirmed against any active Vault hold.

12. Control Cross-Reference Table

This table closes the loop with Part A: each configuration section above is mapped to the ISO/IEC 27001:2022 Annex A control it implements, so an auditor or interviewer can move in either direction, from a named control to the specific Admin console setting that satisfies it, or from a configuration decision back to the requirement that motivated it.

Runbook Section	Configuration	Annex A Control(s)
§5.2	2-Step Verification enforcement; security keys for high-value OUs	A.5.17 Authentication information; A.8.5 Secure authentication
§5.3	Custom admin roles; two named Super Admins	A.8.2 Privileged access rights
§6	Advanced endpoint management; work-profile separation; encryption and screen-lock requirements; selective wipe	A.8.1 User endpoint devices; A.7.9 Security of assets off-premises; A.6.7 Remote working
§7	SPF, DKIM, DMARC; phishing and attachment scanning; forwarding restrictions; S/MIME	A.8.7 Protection against malware; A.8.24 Use of cryptography; A.5.14 Information transfer
§8	Default-restricted external sharing; Shared Drives for client data; allowlisted exceptions	A.5.15 Access control; A.8.12 Data leakage prevention (compensating)
§9	Alert center rules; audit log review	A.8.15 Logging; A.8.16 Monitoring activities

Runbook Section	Configuration	Annex A Control(s)
§10	Vault retention and legal hold	A.5.33 Protection of records
§11	Offboarding runbook and time target	A.6.5 Responsibilities after termination; A.5.18 Access rights

13. Presenting This Project in an Interview

This runbook demonstrates fluency with the specific admin surface (Google Admin console) a GRC or IT security role at a Workspace-based small or mid-size company would actually touch, not just the standards vocabulary. In an interview, the strongest single thread to walk is Section 6 into Section 11: the BYOD endpoint policy and the offboarding runbook together, because they show a specific, defensible answer to the hardest question a small security company's IT environment has to answer, namely what happens to company data on a device the company does not own once the person carrying it is no longer trusted.

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