Consensus Assessments Initiative Questionnaire (CAIQ) v4.1

37signals — Basecamp and HEY

Based on the CSA Cloud Controls Matrix (CCM) v4.1.0 / CAIQ v4.1.0

Contents

Organization: 37signals, LLC

Products in scope: Basecamp and HEY — multi-tenant SaaS operated on 37signals-owned hardware in leased colocation facilities: primary datacenters in Chicago and Ashburn, a read-only Basecamp replica in San Jose (all US), and an Amsterdam datacenter used only by HEY.

Framework: CSA Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire, version 4.1.0 — 283 questions across 17 control domains.

Report date: September 2026. Reviewed at least annually or upon significant change.

Contact: security@37signals.com

How to read this document: each question carries a **Response** (Yes / No / Partial / N/A), the **Control Ownership** under the CSA Shared Security Responsibility Model (SSRM), and an **Implementation** note describing how the control is met or, where it is not, stating the gap plainly. Where a response is affirmative because it rests on a written policy, that policy is named; where 37signals does not perform or document a control, the response is an honest **No** and is not represented otherwise.

Assurance posture: 37signals, LLC has not completed a company-level SOC 2 or ISO 27001 audit. Independent assurance that does exist is stated where relevant: the colocation provider (Summit) issues a SOC 2 Type II covering datacenter physical and environmental controls at the Chicago and Ashburn facilities (available under NDA; the San Jose and Amsterdam sites are outside it); 37signals runs third-party penetration tests and a public HackerOne bug-bounty program; and it self-assesses PCI DSS SAQ A. This questionnaire is a self-assessment of 37signals' stated posture, not an audited attestation.

Shared responsibility model (SSRM)

37signals delivers Basecamp and HEY as multi-tenant SaaS on owned hardware. Under the CSA Shared Security Responsibility Model, the provider owns the application, platform, and infrastructure in full; the customer owns what sits above the application boundary — its data, users, endpoints, configuration, and its own controller-side regulatory posture. Each response below carries a control-ownership tag:

Ownership tag	Meaning
Provider	37signals owns design, implementation, and operation. The customer has no lever.
Provider (via subservice Summit)	37signals owns the outcome and discharges it through its colocation provider under SOC 2 and DPA flow-down (datacenter physical / environmental controls).
Shared	37signals supplies a capability or guarantee; the customer must configure, invoke, or govern it. The archetypal SaaS split.
Customer	The customer (controller / account owner) owns it; 37signals provides no mechanism, or an out-of-band one.

The two genuinely shared domains are **Data Security & Privacy (DSP)** — 37signals is the processor and mechanism provider, the customer is the controller — and **Identity & Access Management (IAM)**, where the absence of SSO/SAML/SCIM places member provisioning and least-privilege enforcement on the customer. **Datacenter Security (DCS)** is provider-via-subservice: the physical and environmental controls belong to Summit, and 37signals owns the outcome and the contractual flow-down.

Responses by domain

A&A — Audit & Assurance

#	Question	Response	Control ownership	Implementation
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Audit & Assurance Policy (P-01) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Audit & Assurance Policy (P-01) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	Shared (37signals + Summit)	Annual independent assessment exists at the infrastructure layer only (Summit SOC 2 Type II covering physical/ environmental controls; annual cycle; current report Jul 2024–Jun 2025, FY2026 in audit; available under NDA) and, for HEY, an annual CASA Tier 2 assessment. 37signals LLC itself has not completed a SOC audit and holds no company-level SOC 2 / ISO 27001. Application-layer assurance is the continuous public HackerOne bug-bounty program (public since Oct 2020) — continuous external testing, not a standards-based annual assessment; formal third-party security reviews/ penetration tests were performed for HEY and Basecamp 5 (most recent public: HEY pre-launch reviews, 2020) and are not on an annual cadence.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?	No	Provider	No documented risk-based audit plan
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/ contractual, and statutory requirements applicable to the audit?	No	Provider	Targeted verification only (PCI SAQ A annual; GDPR via DPA/SCCs); no all-requirements compliance program

#	Question	Response	Control ownership	Implementation
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence and aligned with relevant auditing standards?	No	Provider	No formal audit-management process
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	No	Provider	No documented risk-based corrective-action-plan program for audit findings (HackerOne remediation is vuln-only, adjacent)
A&A-06.2	Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?	No	Provider	No audit-finding remediation-status stakeholder reporting

AIS — Application & Interface Security

#	Question	Response	Control ownership	Implementation
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Application-security policy and procedure are documented in the Application & API Security Policy (P-02, adopted 2026-08-31) and the published Security Overview (incorporated by reference in the DPA): SIP/Ops review all code and infrastructure changes against OWASP guidance before release; all staff receive security training; third-party security reviews/ pentests for HEY and Basecamp 5.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually, or upon any significant changes?	Yes	Provider	Governed by 37signals' Application & API Security Policy (review cadence + secure-API measures) (P-02) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
AIS-02.1	Are baseline requirements to secure applications established, documented, and maintained?	Yes	Provider	OWASP-aligned baseline; homogeneous 'vanilla Rails' stack limits variance
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	No	Provider	No formal application-security metrics program is defined against business objectives or compliance obligations. Vulnerabilities are triaged and remediated by severity-based prioritization rather than a published SLA matrix; descriptive public HackerOne program metrics (response efficiency, time to first response, bounties paid) are the citable operational measures.

#	Question	Response	Control ownership	Implementation
AIS-04.1	Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?	Yes	Provider	Secure SDLC is defined in the P-02/P-04 policies and implemented as: OWASP-guided SIP/Ops security review of every code and infrastructure change before release, automated SAST and dependency audits in CI (Brakeman, bundler-audit, importmap audit), third-party penetration tests and the continuous HackerOne program, and health-checked Kamal deployment. Product planning/design follows the published Shape Up methodology, which does not encode security-specific gates at the requirements/ design phases; there is no single standalone SDLC document.
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and meeting organizational delivery goals?	Yes	Provider	Acceptance criteria are encoded in the automated pipeline rather than a standalone strategy document: every release must pass the CI test suite, Brakeman SAST (fails on any warning), and dependency vulnerability audits, then boot and pass the Kamal health check before receiving traffic; third-party pentests and the continuous HackerOne program supplement release testing. Compliance-adherence criteria are not separately encoded in the testing gates.
AIS-05.2	Is testing automated when applicable and possible?	Yes	Provider	SAST automated pre-release; CI test suite; Kamal automates health-checked deploy verification
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	Provider	Kamal open-source zero-downtime deploy: boot+health-check before cutover — standardized

#	Question	Response	Control ownership	Implementation
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	Provider	Kamal automates build→boot→health-check→cutover
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Provider	A defined intake, acknowledge, triage, investigate, patch, and disclose process is published in the 37signals Security Response policy; public HackerOne bug-bounty program since October 2020 (private program since approximately 2015); findings from third-party pentests and SIP change review follow the same remediation path, deployed through the standard pipeline.
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Partial	Provider	Dependency-level remediation is automated where possible: Dependabot opens weekly dependency-update pull requests reviewed by SIP (with special attention to security updates), CI dependency audits (bundler-audit, importmap audit) block known-vulnerable versions, and Kamal automates deployment of merged fixes. Application-code vulnerability remediation is deliberately human-driven (engineer fix plus review), with only the deployment step automated.

#	Question	Response	Control ownership	Implementation
AIS-08.1	Are processes, procedures, and technical measures defined and implemented to secure APIs?	Yes	Shared (37signals secures API; customer secures own tokens/ OAuth apps)	The public Basecamp REST API is served over HTTPS only, requires OAuth 2.0 (Basic authentication is not accepted), enforces per-client rate limits (429 with Retry-After) and mandatory client identification via User-Agent, as documented in the public API reference; API code is covered by the same OWASP change review, CI SAST, third-party pentest, and HackerOne regime as the applications, formalized in the Application & API Security Policy (P-02). Shared: customers secure their own OAuth applications and access tokens.
AIS-08.2	Are reviews and updates for any improvements conducted at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Application & API Security Policy (review cadence + secure-API measures) (P-02) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

BCR — Business Continuity Management & Operational Resilience

#	Question	Response	Control ownership	Implementation
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-02.2	Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-03.1	Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?	Yes	Shared (provider-heavy)	Published de-facto continuity strategy: BGP Anycast active/active, geo-diversity, layered redundancy, recovery drills. Not framed as formal 'BC strategy per risk appetite'
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
BCR-05.1	Is relevant documentation developed, identified, and acquired both internally and from external parties, to support business continuity and operational resilience plans?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-05.3	Is business continuity and operational resilience documentation reviewed at least annually or upon significant changes?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Partial	Shared (provider-heavy)	Restore and disaster-recovery drills exercising diverse disaster/failure scenarios ran regularly from late 2022 through early 2024; the practice has lapsed since and a restart is pending. A current at-least-annual or change-triggered exercise cadence cannot be affirmed.
BCR-07.1	Are communication channels with all relevant stakeholders established and maintained during business continuity and resilience procedures?	Yes	Shared (provider-heavy)	Account owner contacted within 24h + public real-time status page (37status.com)

#	Question	Response	Control ownership	Implementation
BCR-08.1	Are backups performed periodically?	Yes	Shared (37signals backs up; customer may also export full copy anytime)	Hourly backups of all databases; files backed up automatically on upload; backups stored off-site and retained up to 30 days. Customers may additionally export a full copy of their account at any time.
BCR-08.2	Is the confidentiality, integrity, and availability of the backup ensured?	Yes	Shared	GPG-encrypted (C), tested regularly (I), stored off-site in multiple locations (A)
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared	Recovery drills exercise restoration. Single-account restore is not offered; the control is system-level resiliency.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	Shared (provider-heavy)	Documented DR practice — hourly database backups stored off-site, cross-site failover between Chicago and Ashburn, incident procedures run by Operations and SIP — governed by the Business Continuity & Operational Resilience Policy (P-03) and summarised on the operational-practices page. Drill-based exercise ran regularly through early 2024 and has lapsed since; evaluation currently rests on live cross-site operations and backup verification rather than recovery drills.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	Shared (provider-heavy)	Governed by 37signals' Business Continuity & Operational Resilience Policy (+ BCP) (P-03) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Partial	Shared (provider-heavy)	Disaster-response exercises ran as a regular drill practice from late 2022 through early 2024; the practice has lapsed since and a restart is pending. Neither an annual cadence nor a change-triggered exercise can currently be affirmed.

#	Question	Response	Control ownership	Implementation
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	Provider (via subservice Summit)	Local-emergency-authority participation in exercises is a colocation-facility matter (Summit, Chicago/Ashburn) and is not published; not attested.
BCR-11.1	Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance, in accordance with applicable industry standards?	Yes	Provider (37signals HW) + subservice Summit (power/cooling/network)	Two geo-diverse DCs (~700mi), 2N UPS, N+1 cooling, diverse fiber; 'engineered to stay up even if multiple servers fail'

CCC — Change Control & Configuration Management

#	Question	Response	Control ownership	Implementation
CCC-01.1	Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Change & Configuration Management Policy (P-04) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Change & Configuration Management Policy (P-04) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
CCC-02.1	Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?	Yes	Provider	Defined and policy-documented: every change is version-controlled and peer-reviewed (OWASP-informed, Ops/SIP) before merge; automated test suites and static analysis (Brakeman, bundler-audit) run in CI and merges are gated on passing builds; changes can be validated on staging/beta; production releases go through Kamal, which boots and health-checks the new version before traffic cuts over. Standardized hardened configuration baselines are enforced for endpoints (Kandji plus daily Shipshape audit) and production systems (automated provisioning); baseline contents are held internal and available under NDA. Third-party penetration tests and the public HackerOne program provide external validation.
CCC-03.1	Is a change management procedure implemented to manage the risks associated with applying changes to assets, owned, controlled or used by the organization?	Yes	Provider	All changes Ops/SIP-reviewed before shipping + Kamal health-check + inherent rollback
CCC-04.1	Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?	Partial	Provider	Admin access is limited need-to-know over VPN+2FA and customer-data access is recorded and bi-weekly audited (console1984/ audits1984); a procedure specifically authorizing asset addition, removal, and update is not attested.

#	Question	Response	Control ownership	Implementation
CCC-05.1	Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?	N/A	Shared (customer-facing; not applicable here)	As multi-tenant SaaS there is no customer-owned or tenant-controlled environment, and platform changes are continuous and non-optional, so per-tenant change authorization does not apply.
CCC-06.1	Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?	Yes	Provider	Configuration baselines are established, documented at policy level, and enforced: company endpoints run a standard secure configuration applied by Kandji MDM (disk encryption, firewall, password rules, managed app updates) and are audited daily by Shipshape; production systems are provisioned and configured through automated configuration-management tooling to a standard secure configuration expressed as version-controlled code, and changes to that baseline pass through the same peer-reviewed change pipeline (Change-Management & Hardening-Baseline Policy, adopted 2026-08-31). The specific contents of the production baseline (packages, kernel/network hardening parameters, tooling) are held internal and available to assessors under NDA; a standalone published production-baseline document is not yet produced.
CCC-06.2	Are the baselines reviewed and updated at least annually or upon significant changes?	No	Provider	The production configuration baseline (CCC-06.1) is not yet under a scheduled at-least-annual review; review-on-change of the baseline and deviation reporting await internal attestation.

#	Question	Response	Control ownership	Implementation
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	No	Provider	Shipshape detects endpoint drift; no published production-infra baseline-deviation detection
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	Provider	Governed by 37signals' Change & Configuration Management Policy (P-04) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes	Provider	Governed by 37signals' Change & Configuration Management Policy (P-04) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	Provider	Kamal boots+health-checks before traffic cutover; failed check = no cutover; rollback inherent

CEK — Cryptography, Encryption & Key Management

#	Question	Response	Control ownership	Implementation
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Partial	Provider	The Cryptography & Key Management Policy (P-05) is established, approved, and maintained (adopted 2026-08-31, reviewed on significant change and at least annually): 37signals owns all encryption and key management; there are no customer-held keys. Key-management procedures (rotation, revocation, destruction, custody, inventory) are not documented — see CEK-12 through CEK-21.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?	Yes	Provider	Governed by 37signals' Cryptography & Key Management Policy (review cadence) (P-05) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	Provider	SIP/Ops own key/crypto operations (published role attribution); no formal crypto RACI

#	Question	Response	Control ownership	Implementation
CEK-03.1	Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?	Partial	Provider	Encryption in transit (TLS 1.2/1.3 with ECDHE key exchange; TLS 1.3 AES-256-GCM negotiated by modern clients, AEAD suites preferred — a legacy TLS 1.2 CBC fallback (ECDHE-RSA-AES128-SHA256) remains negotiable on basecamp.com/ 37signals.com and is refused by app.hey.com; publicly verifiable via SSL Labs), at rest (uploaded files AES-256 with SHA-256 integrity; database backups GPG; passwords BCrypt), and at-work field-level encryption in HEY and Basecamp 5 (Rails Active Record Encryption, AES-256-GCM via OpenSSL). Cryptographic libraries are open-standard (OpenSSL) but not certified — no FIPS 140-2/140-3 validated module is claimed. The transport-cipher paragraph in the published Security Overview predates the current configuration (certificate authority and the AES_128_CBC/ECDHE_RSA suite it cites, now only a legacy fallback).
CEK-04.1	Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?	Partial	Provider	Industry-standard primitives throughout (AES-256/ AES-128/SHA-256/BCrypt/ GPG); there is no data-classification scheme (see DSP-04.1), so algorithm selection is uniform rather than classification-based.

#	Question	Response	Control ownership	Implementation
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	Provider	Cryptography, encryption, and key-management changes (TLS/certificate configuration, cipher/library upgrades, encryption-key configuration) are managed under the standard Change & Configuration Management Policy (P-04): reviewed and approved before release through the standard deployment pipeline, with third-party/external library updates handled through the same reviewed pipeline. There is no crypto-specific change procedure beyond P-04.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	No	Provider	No crypto-change cost-benefit/residual-risk process (inherits 05.1)
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	No	Provider	No published crypto-specific risk-management program

#	Question	Response	Control ownership	Implementation
CEK-08.1	Are service providers providing service customers with the capacity to manage their own data encryption keys?	No	Provider	37signals does not offer customer-managed or customer-supplied encryption keys (no BYOK/HYOK). The key hierarchy (per-value data keys wrapped by a 37signals-held primary key) is operated entirely by 37signals by design; this is a deliberate product posture, not a documentation gap.
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	No	Provider	Access to encrypted data audited (console1984); no audit of the encryption/key-mgmt system itself
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	No	Provider	No annual crypto/key-mgmt-system audit cadence
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Provider	Application data-encryption keys are generated by Rails Active Record Encryption using OpenSSL: 256-bit AES-256-GCM keys drawn from the platform CSPRNG (SecureRandom), one random data key per encrypted value, wrapped by a 37signals-held primary key. This covers content encryption in HEY and Basecamp 5; generation standards for TLS, GPG-backup, and SSH keys are not separately documented.

#	Question	Response	Control ownership	Implementation
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Provider	Per-value data keys (a fresh random key for each encrypted field value) wrapped by a 37signals-held primary key — the Rails Active Record Encryption envelope design, open source — in HEY and Basecamp 5. Keys are never exposed to customers or third parties. Note: the Privacy Policy's at-work wording predates Basecamp 5 adoption and names HEY only; the Security Overview and the application code are authoritative. Custody detail is thin (see CEK-18.1).
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	No	Provider	No published key-rotation cadence or cryptoperiod.
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	No	Provider	No published key-revocation process

#	Question	Response	Control ownership	Implementation
CEK-14.1	Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?	No	Provider	No published key-destruction process
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	No published key-activation/ pre-activation process
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/ from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	No published key-suspension process

#	Question	Response	Control ownership	Implementation
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	No published key-deactivation process
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	Master-key custody (HSM/KMS/secret store) and the archival key repository are not publicly documented.
CEK-19.1	Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	No published compromised-key handling process

#	Question	Response	Control ownership	Implementation
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Provider	No published key-recovery/ escrow continuity assessment
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	No	Provider	No published cryptographic-material inventory or status-change reporting.

DCS — Datacenter Security

#	Question	Response	Control ownership	Implementation
DCS-01.1	Are policies and procedures for physical and environmental security established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider (via subservice Summit)	Governed by 37signals' Physical & Environmental Security Policy (P-06) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
DCS-01.2	Are policies and procedures for physical and environmental security reviewed and updated at least annually, or upon significant changes?	Yes	Provider (via subservice Summit)	Governed by 37signals' Physical & Environmental Security Policy (P-06) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
DCS-02.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Partial	Provider (via subservice Summit)	The Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31) governs disposal of 37signals-owned equipment and media in colocation: storage media that held customer or personal data is sanitized or physically destroyed per NIST SP 800-88 before disposal, reuse, or return; the same requirement flows down to the colocation provider; managed staff devices are remote-wiped on loss or decommission. The policy is established, documented, and approved; the standalone written procedure and records mechanism are provisional pending internal operational confirmation, after which this row becomes Yes.
DCS-02.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Partial	Provider (via subservice Summit)	Media not physically destroyed is sanitized per NIST SP 800-88 (purge/clear methods that render recovery infeasible) before release; the specific technique per media type and the sanitization records are held internally, available under NDA. The written procedure is provisional pending internal operational confirmation; Yes once confirmed.

#	Question	Response	Control ownership	Implementation
DCS-02.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually or upon significant changes?	Yes	Provider (via subservice Summit)	The Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31) is reviewed annually and on significant change.
DCS-03.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/ information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	No	Provider (via subservice Summit)	Inter-site transfers use encrypted channels; no published offsite relocation/ transfer AUTHORIZATION policy
DCS-03.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	No	Provider (via subservice Summit)	No written/cryptographically-verifiable transfer-authorization requirement published
DCS-03.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/ information to an offsite or alternate location reviewed and updated at least annually, or upon significant changes?	No	Provider (via subservice Summit)	No offsite relocation/transfer policy exists to review (DCS-03.1 No); the Physical & Environmental Security Policy (P-06) governs the delegated physical posture only. Converts only when a transfer-authorization policy is adopted.

#	Question	Response	Control ownership	Implementation
DCS-04.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	Provider (via subservice Summit)	The Physical & Environmental Security Policy (P-06, adopted 2026-08-31) documents the secure-environment posture: all customer-data-bearing equipment sits in Summit secure areas (dual-factor biometric plus proximity access, caged/dedicated cabinets, 24/7 on-site staff, CCTV) governed by Summit's SOC 2 Type II; 37signals is fully remote with no office housing customer data, and staff devices are governed by the endpoint policy (MDM baseline, disk encryption, remote wipe). Qualified: no clean-desk/home-office physical standard is published.
DCS-04.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?	Yes	Provider (via subservice Summit)	Governed by 37signals' Physical & Environmental Security Policy (P-06) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
DCS-05.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Partial	Provider (via subservice Summit)	Physical media leaves the facilities only as vendor warranty returns (failed drives and parts returned through the colocation provider's ticketed process). The Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31) requires sanitize-or-destroy before disposal, reuse, or return, covering these returns at policy level; the written operational procedure for pre-return sanitization is provisional, so secure-transportation procedures are not yet fully documented.

#	Question	Response	Control ownership	Implementation
DCS-05.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?	Yes	Provider (via subservice Summit)	The Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31) — the artifact governing physical media leaving the facilities (sanitize-or-destroy before disposal, reuse, or return) — is reviewed annually and on significant change.
DCS-06.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	No	Provider (via subservice Summit)	No published scheme classifying physical/logical assets by business risk
DCS-06.2	Are assets' classifications reviewed and updated at least annually or upon significant changes?	No	Provider (via subservice Summit)	No published asset-classification scheme exists to review (DCS-06.1). Converts together with DCS-06.1 when a risk-based classification is documented under P-06.
DCS-07.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	Provider (via subservice Summit)	Production hardware at both primary datacenters is catalogued and tracked in access-controlled internal systems: per-site cabinet diagrams and circuit lists, a maintained hardware-fleet breakdown, and vendor service-tag/contract records; logical assets (hosts, services) are tracked via configuration-management node inventory with automatic re-inventory on change. System names are held internal. Qualified: coverage is documented for the Chicago and Ashburn sites; the San Jose read-only edge is not explicitly documented.

#	Question	Response	Control ownership	Implementation
DCS-07.2	Is the catalogue reviewed and updated at least annually or upon significant changes?	Yes	Provider (via subservice Summit)	The asset catalogue is a living system — configuration-management node inventory is re-run on every hardware change and the datacenter diagrams are maintained continuously — exceeding the annual-review bar, under the Physical & Environmental Security Policy's (P-06) review-on-change-and-annually cadence.
DCS-08.1	Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?	Yes	Provider (via subservice Summit)	Physical security perimeters: dual-factor biometric+proximity, crash-rated/anti-climb cages (Ashburn), dedicated cabinets, 24/7 staff. Chicago cage specifics via Summit SOC 2
DCS-09.1	Is equipment identification used as a method for connection authentication?	No	Provider (via subservice Summit)	VPN+2FA is USER identity, not equipment-identity connection authentication (802.1x/host-cert)
DCS-10.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	Provider (via subservice Summit)	Only authorized personnel access secure areas; ingress/egress restricted, staffed 24/7, surveilled
DCS-10.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	Provider (via subservice Summit)	Physical access-control and surveillance records for the facilities are retained by the colocation provider (Summit): CCTV with 90-day retention is Summit's published Ashburn specification, and facility access-record controls are covered by Summit's SOC 2 Type II (report held; available under NDA). Badge/biometric log retention periods are Summit's to evidence in that report.

#	Question	Response	Control ownership	Implementation
DCS-11.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	Provider (via subservice Summit)	Round-the-clock interior+exterior surveillance monitoring at facilities
DCS-12.1	Are datacenter personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?	Yes	Provider (via subservice Summit)	24/7/365 onsite staff; formal DC-personnel training records are Summit's (via SOC 2)
DCS-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	Provider (via subservice Summit)	Power and telecom cabling inside the facilities is protected by the colocation provider's secured-area controls (caged space, authorized-only access, CCTV), and diverse redundant fiber/power paths guard against damage and interference; inter-site traffic is encrypted, mitigating interception. Facility-level cabling controls are Summit's under SOC 2.
DCS-14.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	Provider (via subservice Summit)	Air-purifying full redundancy; N+1 concurrently-maintainable cooling both sites

#	Question	Response	Control ownership	Implementation
DCS-15.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Partial	Provider (via subservice Summit)	2N UPS at both Summit sites (Chicago/Ashburn), generator capacity, a 100% power-uptime SLA, and N+1 cooling; test cadence is attested in Summit's SOC 2 Type II — generators are tested annually with third-party preventive maintenance, and third-party specialists inspect power-management systems on a predefined maintenance schedule. The San Jose read-only site is Summit-managed and sits in a facility on the report's in-scope subservice-facility list, every entry of which is fully equipped with redundant UPS, backup generators, and cooling systems, with utility maintenance and testing attested per facility operator. The Amsterdam (HEY-only) site is not yet equivalently evidenced: its facility is on the same in-scope list, but Summit management of the Amsterdam installation is not attested.
DCS-16.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	Provider (via subservice Summit)	Business-critical equipment is split across two geographically separate sites (Chicago, IL and Ashburn, VA, ~600 mi apart, served by different utilities and carrier ecosystems), so no single regional environmental event affects both; facility-level siting against local environmental hazards is the colocation provider's control under its SOC 2.
DCS-17.1	Are datacenter security metrics established, monitored, and reported to secure data center assets and services?	No	Provider (via subservice Summit)	No published datacenter security metrics program

#	Question	Response	Control ownership	Implementation
DCS-18.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure continuous operations?	Yes	Provider (via subservice Summit)	Continuous operations via full redundancy (2N UPS, N+1 cooling, BGP Anycast active/active, geo-diversity). Not framed as a named continuous-operations attestation

DSP — Data Security & Privacy Lifecycle Management

#	Question	Response	Control ownership	Implementation
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Partial	Shared	Publishes handling/protection policies (Privacy Policy; Security Overview via DPA); no formal data-CLASSIFICATION scheme over customer content (customer/controller owns classification)
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?	Partial	Shared	The Privacy Policy (last updated 2026-08-30) and DPA (last updated 2026-09-01) are published on the live 37signals.com/policies site and maintained on significant change — each page refreshes its dated header and subscribers to the policy-updates mailing list (37signals.com/policies/updates) are notified — satisfying the 'or upon significant changes' limb; the Data Security, Interoperability & Portability Policy (P-07, adopted 2026-08-31) is additionally reviewed at least annually and on significant change. No formal data-classification scheme (DSP-01.1) keeps this Partial.

#	Question	Response	Control ownership	Implementation
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Partial	Shared	Logical deletion is committed and irreversible (deleted from active systems within 30 days, from backups within 60; content cannot be recovered once permanently deleted). Physical media: the Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31) requires media that has held customer data to be sanitized or physically destroyed before disposal, reuse, or return per NIST SP 800-88, with contractual flow-down to the colocation subservice provider (Summit). Held at Partial: the standard sets the requirement, but internal confirmation that the written procedure is applied in the disposal/RMA flow is pending; upgrades to Yes on that attestation.
DSP-03.1	Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?	Partial	Shared	Narrative inventory of provider-collected personal data (‘What we collect and why’); customer-uploaded content not inventoried (controller’s job)
DSP-03.2	Is the inventory reviewed and updated at least annually or upon significant changes?	Partial	Shared	The provider-collected inventory (‘What we collect and why’) lives in the Privacy Policy on the live 37signals.com/policies site (last updated 2026-08-30) and is maintained on significant change — the dated header is refreshed and policy-updates mailing-list subscribers are notified — satisfying the ‘or upon significant changes’ limb; no fixed annual cadence. Inventory of customer-uploaded content remains the controller’s responsibility, so this remains Partial.

#	Question	Response	Control ownership	Implementation
DSP-04.1	Is data classified according to type and sensitivity levels?	No	Shared/Customer	Customer content is not sensitivity-classified; it is stored without inspection. Classification of that content is the customer's responsibility as controller.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Partial	Provider	Data flows are documented narratively: categories processed (Privacy Policy 'What we collect and why'; DPA Annex I), storage locations (Security Overview — Chicago and Ashburn; San Jose read-only for Basecamp 5; Amsterdam for HEY), transfers (EEA/UK to US under SCCs Modules 2/3), and onward transmission to the published per-product subprocessor lists (purpose and location, all US). Formal data-flow diagrams are not published and remain a provisional artifact pending internal confirmation.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?	Yes	Provider	The narrative data-flow documentation (Privacy Policy, DPA Annex I, Security Overview data locations, subprocessor lists) is maintained on significant change on the live policies site and falls under the Data Security, Interoperability & Portability Policy (P-07, adopted 2026-08-31), reviewed on significant change and at least annually. Qualified: the formal data-flow diagram artifact is provisional pending internal confirmation, so the annual review currently covers the narrative documentation only.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared	Customer retains ownership (ToS); 37signals is processor/steward under DPA controller/processor structure

#	Question	Response	Control ownership	Implementation
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Partial	Provider	Ownership/stewardship documentation (ToS, last updated 2025-09-02; DPA, last updated 2026-09-01; Privacy Policy, 2026-08-30) is published on the live 37signals.com/policies site and maintained on significant change, with dated headers and notification to policy-updates mailing-list subscribers; each was revised within the past 12 months. No fixed annual review cycle is attested for the ToS/DPA themselves (the Data Security, Interoperability & Portability Policy (P-07) that references them is reviewed annually and on change).
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	Provider	Security-by-design in substance: at-work field encryption, default-no-access, OWASP review
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	Shared	Default-no-access, per-session consent, at-work encryption, content private by default
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	Shared	Content is visible only to the people the account invites (project access is invitation-based; public sharing links are explicit, opt-in, and customer-revocable); 37signals staff have no default access (explicit per-session consent, console1984/audits1984); at-work encryption in HEY and Basecamp 5.

#	Question	Response	Control ownership	Implementation
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Partial	Shared/Customer	A GDPR Article 35 screening is conducted and documented as 37signals' standing position (since 2018, with a written internal record): for provider-controlled processing none of the mandatory triggers apply (no profiling with legal effect, no self-collected special-category data, no public monitoring), so no full DPIA is required or performed; the screening is re-run on material product change or new technology (any AI/LLM feature triggers a fresh screen). Customers are controllers of their content and own any DPIA over it; 37signals provides reasonable assistance under DPA §2.3. The screening record is internal (available under NDA), not published.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	Shared (provider-heavy)	In transit: TLS over all public networks. Cross-border: EEA/UK/Swiss to US transfers under the DPA with SCCs (Module 2 controller-to-processor, Module 3 processor-to-processor), UK Addendum, and FADP terms. At rest: uploaded files AES-256; backups GPG-encrypted; application databases not encrypted at rest except at-work field-level encryption in HEY and Basecamp 5. Access limited by default-no-access with audited console sessions.

#	Question	Response	Control ownership	Implementation
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	Shared	Right of Access/Correction (self-service editing), deletion on closure; customer fulfills DSRs, DPA assists
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	Shared	‘Collect only what we need’; DPA restricts processing to documented instructions; GDPR/CCPA honored
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	Provider	Subprocessors bound by written agreements no less protective than 37signals’ DPA; published subprocessor list; SCCs Module 3

#	Question	Response	Control ownership	Implementation
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	Provider	DPA §5.2 commits 37signals to notify customers of any new subprocessor before authorizing it to process personal data, with a 10-business-day objection right and termination/refund remedy (§5.3); the current per-product list is published (Basecamp subprocessors, last updated 2026-08-30, all US). Qualified: the DPA directs customers to subscribe to a GitHub page for change notification, but that repository has been archived since December 2023 while the list has since changed; the currently operative advance-notice channel is being re-confirmed and the DPA reference corrected.
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	No	Provider	No published policy governing production data use in non-production/test
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared	Published lifecycle: active 30d / backup 60d / trash ~25d / purge ~90d; off-site backups max 30d

#	Question	Response	Control ownership	Implementation
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	Shared	Encryption in transit (TLS), files AES-256 at rest, GPG-encrypted backups, and at-work field-level encryption in HEY and Basecamp 5 (application databases otherwise not encrypted at rest); default-no-access to customer data with explicit per-session consent, console sessions recorded (console1984) and audited bi-weekly by Security (audits1984) for HEY, Basecamp 5, and Fizzy; deletion committed within 30/60 days.
DSP-18.1	Does the service provider ensure that a procedure is in place and communicated to service customers for managing and responding to requests by law enforcement authorities for the disclosure of personal data, in accordance with applicable laws and regulations?	Partial	Provider	37signals' published policy is to respond to law-enforcement demands only when compelled by legal process or a narrow emergency; the policy does not explicitly commit to notifying the customer where notification is not legally barred.
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Provider	Documented in the Security Overview: primary datacenters in Chicago, IL and Ashburn, VA; a read-only outpost in San Jose, CA for Basecamp 5 (all US); the Amsterdam outpost is HEY-only — no Basecamp EU facility. Files are replicated across separate datacenters; database backups are stored off-site (retained up to 30 days). Data location is published; the off-site backup locale is not itemized publicly.

GRC — Governance, Risk Management & Compliance

#	Question	Response	Control ownership	Implementation
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Partial	Provider	Founder-led, with a published and maintained security program (Security Overview) and privacy program (Privacy Policy + DPA); there is no single named governance-program policy and no attested annual review cadence.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Information Security Governance & Policy-Review Policy (P-00) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
GRC-02.1	Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?	Partial	Provider	A documented risk-management method and register exist internally: scope, Likelihood × Impact scoring, banded acceptance thresholds with named-owner sign-off for High, Mitigate/Accept/Transfer/Avoid treatment with an action owner per risk, reviewed annually or on significant change; provisionally adopted 2026-08-30 with a named owner, treatments tracked to closure. Partial: the register is an initial one (8 risks), not yet frozen, not yet through a review cycle, and not published — a formal, maintained ERM program is in progress, not established.

#	Question	Response	Control ownership	Implementation
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	Provider	Governed by 37signals' Information Security Governance & Policy-Review Policy (P-00) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	Provider	Governed by 37signals' Information Security Governance & Policy-Review Policy (P-00) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	Provider	Published+implemented infosec program (Security Overview) covering personnel/access/network/ encryption/physical/incident/ patching/pentest/deletion. Not formally mapped to all 17 CCM domains — this CAIQ IS that mapping
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	Provider	Ops + SIP have published defined ownership. No named governance/risk officer (no DPO/CISO title)
GRC-07.1	Are all relevant standards, regulations, legal/ contractual, and statutory requirements applicable to your organization identified and documented?	Yes	Shared (customer owns own regulatory scope)	GDPR (DPA+SCCs), CCPA (Privacy Policy), PCI DSS (SAQ A) identified+addressed. No single consolidated regulatory register. HIPAA out of scope

#	Question	Response	Control ownership	Implementation
GRC-07.2	Are the identified requirements reviewed at least annually or upon significant changes?	Yes	Provider	Governed by 37signals' Information Security Governance & Policy-Review Policy (P-00) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
GRC-08.1	Is contact established and maintained with related special interest groups and other relevant entities?	Yes	Provider	Governed by 37signals' Information Security Governance & Policy-Review Policy (P-00) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

HRS — Human Resources Security

#	Question	Response	Control ownership	Implementation
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	No	Provider	Background checks are not performed on 37signals workers, as stated in the published Security Overview — a deliberate position, not a documentation gap. Compensating controls: written confidentiality agreements before any access to code and data (Security Overview; DPA §4.1), server access via VPN plus 2FA limited to workers who need it, customer-account access only with the customer's explicit per-session permission (Handbook 'Our internal systems'), and bi-weekly audit of employee access to customer data in HEY, Basecamp 5, and Fizzy via console1984/audits1984 (Security Overview).

#	Question	Response	Control ownership	Implementation
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	No	Provider	No background program to design against criteria (conditional on 01.1)
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually, or upon significant changes?	No	Provider	No policy to review (conditional on 01.1)
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Handbook ‘Managing work devices’ = published acceptable-use policy (Kandji Macs/Omarchy Linux required; no personal data on issued computers; unmanaged devices ‘untrusted’)

#	Question	Response	Control ownership	Implementation
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually, or upon significant changes?	Yes	Provider	The Employee Handbook ('Managing work devices') is version-controlled and maintained on significant change, meeting the 'or upon significant changes' review limb; there is no fixed annual cadence.
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Remote Work & Confidential-Data Handling Policy (P-15) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Remote Work & Confidential-Data Handling Policy (P-15) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Fully remote since inception; Handbook + Security Overview document controls (Kandji, Omarchy FDE, VPN 2FA, Tailscale, 1Password)
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually, or upon significant changes?	Yes	Provider	The Employee Handbook is version-controlled and maintained on significant change, meeting the ‘or upon significant changes’ review limb; there is no fixed annual cadence.
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	Provider	Departure handling is documented: company-issued Macs are remotely wiped via Kandji when an employee leaves (Handbook ‘Managing work devices’; Security Overview), Linux credential access is offboarded via 1Password, and the company reserves the right to seize the device or its data. Offboarding runs from a templated internal checklist; the hardware return/retention step is internal and not published.

#	Question	Response	Control ownership	Implementation
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all relevant personnel?	Yes	Provider	Onboarding roles are documented and communicated in the public Handbook ('Getting started': People team, hiring manager, Ops buddy, People Ops policy review; welcome project to-do lists). Departure handling is documented in 'Managing work devices' (Kandji remote wipe, 1Password offboarding) and 'Severance' (terms, for-cause exclusion); offboarding role assignments run from an internal templated checklist and are not published. Not one consolidated procedure.
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	Provider	All workers sign confidentiality agreements before access to code+data (Security Overview). Substance = signed pre-access agreement
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	Provider	Confidentiality agreement binds data protection; policy review with People Ops at onboarding. Exact clause incorporating infosec policies not public
HRS-09.1	Are employee roles and responsibilities relating to information assets' security and privacy, established, documented and communicated?	Yes	Provider	Ops+SIP documented security AND privacy responsibilities; Handbook privacy statements (Queenbee consent-only login)

#	Question	Response	Control ownership	Implementation
HRS-10.1	Are requirements for non-disclosure/ confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Partial	Provider	Confidentiality agreements are required and signed before access (identified and documented); review at planned intervals is not attested.
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Partial	Provider	Security awareness is universal practice — ‘everybody is trained and made aware of security concerns’ — but it is not a formally documented and evaluated training program with completion tracking.
HRS-11.2	Are regular security awareness training updates provided?	Partial	Provider	Training is ongoing as universal practice and Shipshape audits machine hardening daily; a cadence of formal security-awareness training updates is not attested.
HRS-12.1	Are employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	Provider	Personnel engaged in processing Personal Data receive appropriate training on their responsibilities and execute written confidentiality agreements (DPA §4.1, contractual); everybody is trained on security concerns and best practices for their systems (Security Overview). Access to customer data is additionally gated by explicit per-session customer permission and audited bi-weekly via console1984/ audits1984, with at-work encryption limiting exposure. Training is not tracked as a formal completion-recorded program.

#	Question	Response	Control ownership	Implementation
HRS-12.2	Are employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Partial	Provider	The Handbook and operational procedures are continuously updated (in git) with a weekly communication cadence; role-targeted security-procedure updates are not attested.
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	Provider	Onboarding policy review with People Ops + confidentiality agreement + training. Explicit legal/ statutory/regulatory notification not itemized

IAM — Identity & Access Management

#	Question	Response	Control ownership	Implementation
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared	The Identity & Access Management Policy (P-08, adopted 2026-08-31, reviewed annually and on significant change) documents customer self-service identity administration and staff joiner/mover/leaver and least-privilege access; applied in practice per the public Security Overview (VPN plus 2FA need-to-know staff access, bi-weekly console1984/audits1984 access audit) and communicated via the internal handbook.

#	Question	Response	Control ownership	Implementation
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Shared	Governed by 37signals' Identity & Access Management Policy (P-08) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IAM-02.1	Are policies and procedures for the management of authentication credentials, including passwords, established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared (37signals sets policy; customer chooses compliant credentials)	Authentication is handled by 37signals ID (Launchpad): a minimum 12-character password, rejection of passwords equal to the username or email, and a known-breached-password check via Have I Been Pwned (k-anonymity); passwords are BCrypt-hashed. No character-composition rule or strength meter is imposed — the policy is length- and breach-list-based rather than composition-based.
IAM-02.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Shared	Governed by 37signals' Identity & Access Management Policy (P-08) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IAM-03.1	Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?	Partial	Shared	Staff access is bi-weekly audited (console1984), the customer end-user roster is managed by owners/admins, and identity is a single cross-product 37signals ID; there is no formal staff identity-inventory register.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared	Ops+SIP own access/identity/network/firewall/logs — separated from application-level roles
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Shared	Admin access need-to-know over VPN+2FA; default no employee access to customer content (per-session consent)

#	Question	Response	Control ownership	Implementation
IAM-06.1	Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	Shared	Governed by 37signals' Identity & Access Management Policy (P-08) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IAM-07.1	Is a process in place to de-provision or modify identity access in a timely manner?	Yes	Shared	Governed by 37signals' Identity & Access Management Policy (P-08) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IAM-08.1	Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance, and at least annually or upon significant changes?	Partial	Shared	All employee access to customer data is audited bi-weekly (exceeding the annual requirement); the audit reviews customer-data access rather than full least-privilege and separation-of-duties revalidation across all systems.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?	Partial	Shared	Ops and SIP hold distinct privileged functions (access/network/logs vs. app admin); evaluation of the segregation is not explicitly attested.
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Partial	Shared	Staff access to customer data is granted per-session via console1984 consent (time-limited); time-limiting of standing infrastructure-administrator access is not established in published sources.

#	Question	Response	Control ownership	Implementation
IAM-10.2	Are procedures implemented to prevent the accumulation of segregated privileged access?	Yes	Shared	Governed by 37signals' Identity & Access Management Policy (P-08) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IAM-11.1	Are processes and procedures for service customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	Shared (customer in the grant loop)	Customer express per-session consent is required before staff access customer data (console1984); access is recorded and bi-weekly audited. A narrow abuse-investigation exception is stated.
IAM-12.1	Are processes, procedures, and technical measures that ensure identities' activities are identifiable through uniquely associated IDs defined, implemented, and evaluated?	Yes	Shared	Unique email identity → single cross-product 37signals ID; login events logged w/ IP/browser/OS/ timestamp
IAM-13.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared (37signals provides; customer enrolls/enforces)	Native 2FA (TOTP authenticator app plus optional WebAuthn hardware security key) in Basecamp and HEY. Basecamp: account owners can require 2FA for all members (opt-in enforcement, not default-on). HEY: 2FA is required for all paying customers. Staff administrative access is over VPN plus 2FA.

#	Question	Response	Control ownership	Implementation
IAM-13.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	No	Shared	No published digital-certificate/mTLS posture for SYSTEM identities (transport TLS ≠ system-identity auth)
IAM-14.1	Are processes, procedures, and technical measures for the secure management of authentication credentials, including passwords, defined, implemented, and evaluated?	Yes	Shared	Passwords are salted BCrypt hashes, never plaintext (published cost factor 10; cost 12 for newly set passwords); screened against breached-password corpora (HIBP k-anonymity); 12-character minimum; self-service and admin-triggered reset by emailed link; 2FA with optional hardware key.
IAM-15.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared	Structured permissions (owner/admin roles, project-level, per-person visibility, RBAC-style); staff role-separated. Weakest limb: no dedicated published authz-model sentence

IPY — Interoperability & Portability

#	Question	Response	Control ownership	Implementation
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?	Yes	Shared	Governed by 37signals' Data Security, Interoperability & Portability Policy (P-07) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	Shared	Governed by 37signals' Data Security, Interoperability & Portability Policy (P-07) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	No	Provider	No named policy or procedure for application-development portability. In practice the stack is open-source (Ruby on Rails) and production deploys use Kamal, 37signals' open-source, provider-agnostic container deployment tool (Operational Practices page), so portability is real but undocumented as policy. Honest No; not N/A.
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	Shared	Governed by 37signals' Data Security, Interoperability & Portability Policy (P-07) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Data Security, Interoperability & Portability Policy (P-07) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
IPY-02.1	Are service customers able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared	Basecamp: public REST API (github.com/basecamp/bc3-api) — HTTPS-only, OAuth 2.0, JSON; any user can authorize a client and retrieve the data they have access to, enabling integration and migration. Account owners can additionally export a full HTML copy of the account from Adminland (bulk backup, not machine-readable). Qualified: the documented programmatic interface is Basecamp's; HEY offers account data export but no equivalent public API.
IPY-03.1	Are cryptographically secure network protocols implemented for the management, import, and export of data in accordance with industry standards?	Yes	Provider	All mgmt/import/export over TLS/HTTPS; API HTTPS-only
IPY-04.1	Do agreements include provisions specifying service customers' data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Yes	Shared	The four elements are spread across the ToS, DPA, and Help, not one clause. (a) Format — full HTML export by account owners, linked from the ToS cancellation section (Help). (b) Duration — content inaccessible immediately on cancellation; deleted from active systems within 30 days and from backups within 60 (ToS); if the customer changes their mind, restore is possible only within the first 30 days after cancellation (Cancellation Policy). (c) Scope — entire account including archived projects and optional Pings (Help); DPA §8 obliges return of Personal Data on termination. (d) Deletion — permanent and unrecoverable (ToS); certification of deletion on request (DPA §11.8). No separate contractual portability SLA is offered.

I&S — Infrastructure & Virtualization Security

#	Question	Response	Control ownership	Implementation
I&S-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Infrastructure & Virtualization Security Policy (P-09) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
I&S-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Infrastructure & Virtualization Security Policy (P-09) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
I&S-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Partial	Provider	Servers 'operate at full redundancy … engineered to stay up even if multiple servers fail' and excessive-resource alerts escalate to Ops; a formal capacity-planning process against required performance is not documented.
I&S-03.1	Are communications between environments, services, and applications monitored?	Yes	Provider	Dedicated network 'secured with firewalls and carefully monitored'; internally-built auto-block system

#	Question	Response	Control ownership	Implementation
I&S-03.2	Are communications between environments, services, and applications encrypted?	Partial	Provider	Customer/public traffic is encrypted (TLS); file replication between datacenters travels over private, end-to-end encrypted connections. Within the firewalled, segmented private production network, service-to-service traffic may be transferred unencrypted (published Security page) — compensated by firewalls, segmentation, and monitoring. Not blanket internal encryption.
I&S-03.3	Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?	Yes	Provider	A firewalled, segmented production network restricts connections between environments and services to authorized paths (Security Overview; Network-Defense policy); administrative remote access to servers is only via VPN with two-factor authentication, limited to workers who need it.
I&S-03.4	Are network configurations reviewed at least annually?	No	Provider	No published annual network-config review
I&S-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	No	Provider	No published allowed-services/protocols/ports justification + compensating-controls documentation

#	Question	Response	Control ownership	Implementation
I&S-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Partial	Provider	Production systems are provisioned and configured through automated tooling to a standardized, hardened secure-configuration baseline (Change-Management & Hardening-Baseline Policy, adopted 2026-08-31; automated provisioning is documented internal practice); baseline contents are internal, available under NDA. Endpoint hardening is published (Kandji per the Handbook; Shipshape per the Security Overview). Gap: no standalone, version-controlled production-baseline document or scheduled baseline review yet (provisional pending internal confirmation); hypervisor/ control-plane hardening is not specifically addressed.
I&S-05.1	Are the environments separated into production and non production environments to reduce the risk of sensitive production data being used in non-production environments?	Partial	Provider	Production and non-production environments are separated: a distinct staging environment with its own database precedes production (Operational Practices §2; Change-Management & Hardening-Baseline Policy; deploy configuration). Caveat: internal engineering documentation designates beta — which uses the production database — as a testing environment, and HEY's staging database is seeded from a production snapshot, so production data is used in non-production/ testing contexts; sanitization is not evidenced. Provisional pending internal confirmation.

#	Question	Response	Control ownership	Implementation
I&S-05.2	Is production data sanitized or protected before being used for any authorized non-production purpose?	No	Provider	Production data is not sanitized before authorized non-production use: internal engineering documentation records HEY's staging database as a production snapshot and beta testing against the production database, with no sanitization step documented. Overlaps DSP-15.
I&S-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?	Yes	Provider	Standardized multi-tenant SaaS with per-account logical isolation on a dedicated firewalled network; no formal tenant-segregation-controls attestation exists beyond the published isolation description.
I&S-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	N/A	Provider	37signals runs its products on owned hardware in colocation facilities and has completed its exit from cloud hosting and cloud storage (dev.37signals.com); there is no migration of servers, services, applications, or data to cloud environments. Public and inter-datacenter traffic encryption is answered at I&S-03.2/CEK-03.

#	Question	Response	Control ownership	Implementation
I&S-08.1	Are high-risk environments identified and documented based on data sensitivity, threat exposure, and business impact?	Partial	Provider	Sensitive-data boundaries are identified publicly (PCI SAQ A payment boundary; at-work field encryption for HEY/ Basecamp 5 content; segmented production network per the Network-Defense policy) and a public network-architecture overview exists (EVPN/VXLAN core, layered redundancy, diverse paths); detailed network architecture is also documented internally (held internal). No formal, risk-scored high-risk-environment register is evidenced, published or internal.
I&S-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	Provider	Defense-in-depth: a dedicated firewalled network, an internally built monitoring and auto-block system (scanning, failed logins), and Ops escalation. Intrusion detection is a custom system rather than a named commercial IDS/IPS.

LOG — Logging & Monitoring

#	Question	Response	Control ownership	Implementation
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared (provider-heavy)	Governed by 37signals' Logging & Monitoring Policy (P-10) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
LOG-01.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Shared (provider-heavy)	Governed by 37signals' Logging & Monitoring Policy (P-10) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Partial	Shared (provider-heavy)	Audit/infrastructure log retention is defined and technically enforced: central logs are retained 30 days (retention enforced by the log platform; search indices kept 30 days max), and privileged-console session records are incinerated after 30 days (Basecamp) / 60 days (HEY). Log-platform access is restricted to Ops/SIP on the internal network. Documented internal practice, available under NDA. Held at Partial: the question's security limb includes integrity — tamper-protection/immutability of logs is not documented (LOG-10 is No).
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared (provider-heavy)	An internally built system monitors network and application activity and auto-blocks scanning and failed-login patterns. It is a custom system rather than a named commercial IDS/SIEM.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	Shared (provider-heavy)	Excessive-resource alerts escalate to Ops; auto-block feeds Ops/SIP
LOG-04.1	Is audit log access restricted to authorized identities, and are records of that access maintained?	Partial	Shared (provider-heavy)	Log-file management is scoped to Ops/SIP (restricted) and console access is recorded and bi-weekly audited; logging of access to the audit logs themselves is not explicitly attested.

#	Question	Response	Control ownership	Implementation
LOG-05.1	Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?	Yes	Shared (provider-heavy)	Internally-built system detects+auto-blocks anomalies; escalates to Ops/ SIP. No published SIEM/log-correlation layer
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	Shared (provider-heavy)	Anomalies escalate to Ops/ SIP for investigation; bi-weekly data-access review; 24h customer-contact supports timeliness
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	Shared (provider-heavy)	A reliable time source is run as documented internal practice: internal chrony NTP servers, provisioned as configuration-as-code, synchronize from public NTP pools and serve the internal network including network equipment and configuration-managed hosts; synchronization health is exported as metrics and monitored (Prometheus, Grafana). Evidence is internal documentation and configuration-as-code, available under NDA.

#	Question	Response	Control ownership	Implementation
LOG-07.1	Are logging requirements for information meta/ data system events established, documented, and implemented?	Yes	Shared (provider-heavy)	Logging requirements are established at policy level (Logging & Monitoring Policy P-10: account access including source IP; centralized log management; scope set against the threat environment) and implemented: all account access is logged by IP, login events are recorded with IP/ browser/OS/timestamp with user-reviewable history, and every privileged console session is recorded (console1984). A detailed event-catalogue/logging standard is not published.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment and as per relevant regulatory requirements?	Yes	Shared (provider-heavy)	The Logging & Monitoring Policy (P-10) sets the logging scope against the threat environment and reviews it on change and at least annually; regulatory-driven review rides the governance policy's review-on-change trigger (significant change to processing or subprocessors).
LOG-08.1	Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?	No	Shared/Customer (customer-facing)	No customer-facing capability to detect, scrub, or tokenize sensitive data in logs, and no customer log-access or export path. This reflects a product design decision.
LOG-09.1	Are audit records generated, and do they contain relevant security information?	Yes	Shared (provider-heavy)	Login events recorded (IP/ browser/OS/timestamp); all account access logged by IP; new-device notifications; user login history. Auth/access-scoped (no full in-app action audit trail)

#	Question	Response	Control ownership	Implementation
LOG-10.1	Are audit records protected from unauthorized access, modification, and deletion?	No	Shared (provider-heavy)	No published audit-record immutability/tamper-protection (read-only/WORM/deletion-protection) attestation
LOG-11.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	No	Shared (provider-heavy)	No published monitoring/internal-reporting over crypto operations/key management (compounds CEK key-lifecycle gap)
LOG-12.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	No	Shared (provider-heavy)	Per-field content keys under master key exist; no full key-lifecycle nor key-lifecycle-event logging published
LOG-13.1	Is physical access logged and monitored using an auditable access control system?	Partial	Shared (Summit operates; 37signals leases)	Physical access at Summit (Chicago/Ashburn): dual-factor biometric+proximity, 24/7 staff, surveillance; auditable via Summit SOC 2 Type II, which also covers the log-retention limb. The San Jose read-only site and the Amsterdam (HEY) site are outside that assurance.
LOG-14.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Partial	Shared (provider-heavy)	Excessive-resource and security alerts escalate to Ops, and the monitoring/auto-block system feeds Ops/SIP; reporting of failures of the monitoring systems themselves is not explicitly attested.

#	Question	Response	Control ownership	Implementation
LOG-14.2	Are accountable parties immediately notified about anomalies and failures?	Partial	Shared (provider-heavy)	Alerts escalate to Ops for immediate investigation, with SIP incident response and 24-hour customer contact for customer-affecting incidents; notification about failures of the monitoring systems themselves is not attested (see LOG-14.1).

SEF — Security Incident Management, E-Discovery & Cloud Forensics

#	Question	Response	Control ownership	Implementation
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-01.2	Are policies and procedures reviewed and updated annually, or upon significant changes?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Partial	Shared	Published timely-incident commitment: account owner contacted within 24 hours, with continuous monitoring and Ops escalation; there is no formal named incident-management policy document.

#	Question	Response	Control ownership	Implementation
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually, or upon significant changes?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-03.1	Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Partial	Shared	SIP/Ops design, review, and test incident response internally, and impacted customers are contacted within 24 hours; supply-chain communication and a documented plan artifact are gaps.
SEF-04.1	Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?	Yes	Shared	SIP/Ops review and test IR processes; the Security Incident Response & Forensics Policy (P-11, adopted 2026-08-31) sets the review/exercise cadence at 'on change and at least annually', with no completed review cycle yet. DR drills ran through early 2024 and have lapsed since; current drills are not the evaluation mechanism.
SEF-05.1	Are information security incident metrics established, monitored and reported?	No	Shared	Public status page (uptime/ incident history) is availability metrics, NOT security-IR performance metrics (detection time/MTTR)

#	Question	Response	Control ownership	Implementation
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	Shared	Internally-built auto-block + Ops escalation triages security events; HackerOne triages inbound external reports
SEF-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents in accordance with incident categories and severity levels?	Yes	Shared	SIP/Ops respond to incidents; 24h customer contact; severity-based handling via HackerOne triage. Not a documented category/ severity playbook
SEF-07.2	Are these processes and procedures reviewed, updated, and tested at least annually?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-08.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	Shared (37signals notifies; customer acts)	DPA §7 notify 'without undue delay'; Security Overview 24h account-owner contact
SEF-08.2	Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Partial	Shared	Breach notice within 24 hours and per applicable data-protection law (GDPR standard via the DPA); a supply-chain breach-reporting SLA is inferred from DPA flow-down rather than stated.

#	Question	Response	Control ownership	Implementation
SEF-09.1	Is a secure repository of security incident records established and maintained?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-09.2	Are incident records regularly reviewed to identify patterns, root causes, and systemic vulnerabilities, and are relevant corrective measures implemented?	Yes	Shared	Governed by 37signals' Security Incident Response & Forensics Policy (P-11) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
SEF-10.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Partial	Shared	A law-enforcement request-handling policy and inbound security contacts (security@, HackerOne) are published; no maintained register of regulator and authority points of contact exists.
SEF-10.2	Are points of contact reviewed and updated at least annually?	Partial	Shared	The published contacts (security@, HackerOne, the law-enforcement request process) are maintained under P-11's review cadence; there is no regulator/authority contact register to review (see SEF-10.1).

STA — Supply Chain Management, Transparency & Accountability

#	Question	Response	Control ownership	Implementation
STA-01.1	Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
STA-01.2	Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-02.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-02.2	Are the policies and procedures that apply the SSRM reviewed and updated annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-03.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain?	Yes	Shared	Applied down chain via DPA §5.1 flow-down (no less protective) + published subprocessor list; not labeled 'SSRM'
STA-04.1	Is the service customer given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	Shared	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
STA-05.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?	Yes	Shared	Ownership and applicability of every CCM control is delineated per control in the Control ownership column of this CAIQ, derived from a canonical per-domain ownership model (Provider / Provider-via-subservice / Shared / Customer) covering all 17 CCM domains (see the Shared responsibility model section) and reconciled row by row.
STA-06.1	Is the SSRM documentation reviewed and validated?	Yes	Shared	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-07.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	Provider	37signals implements and operates its SSRM portions and audits the highest-risk one internally: all staff access to customer data in HEY, Basecamp 5, and Fizzy is audited bi-weekly via console1984/audits1984 (public Security Overview); annual PCI DSS SAQ A self-assessment. External assessment is application-layer only — third-party penetration tests and the continuous public HackerOne program. No company-level SOC 2/ISO attestation; the datacenter SOC 2 Type II (Summit) covers physical/environmental controls only.

#	Question	Response	Control ownership	Implementation
STA-08.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	Provider	37signals publishes and maintains per-product subprocessor lists (Basecamp, HEY, Highrise, Campfire, Backpack; Basecamp/HEY last updated 2026-08-30, all entities US-based) plus a company-level processors list; new subprocessors are announced before authorization with a 10-business-day objection window (DPA §5.2–5.3). Datacenter colocation (Summit, Chicago/Ashburn/San Jose) is inventoried separately as the infrastructure subservice. A general (non-data) vendor register is not published.
STA-09.1	Is a process defined, implemented, and enforced for establishing a Bill of Material for the service supply chain?	No	Provider	37signals does not publish or maintain a Service Bill of Materials for customers: with continuous deployment, a published SBOM snapshot would be stale within days and misleading. Component provenance is nonetheless controlled — every production application pins its third-party dependencies in version-controlled lockfiles updated only through the reviewed change pipeline, with scheduled automated dependency-update review — and subprocessor/infrastructure dependencies are covered by the published subprocessor lists and DPA flow-down.
STA-09.2	Is the Bill of Material reviewed and updated at least annually or upon significant changes?	No	Provider	No customer-facing SBOM is maintained (see STA-09.1); dependency inventories (lockfiles) are updated continuously through the reviewed change pipeline rather than on an annual review cycle.

#	Question	Response	Control ownership	Implementation
STA-10.1	Are risk factors associated with supply chain relationships periodically reviewed?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-11.1	Do service agreements between service providers and service customers (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy • Operational Resilience	Partial	Shared	A checklist control ('at least the following provisions') with three provisions not incorporated as agreed terms. The Terms of Service, DPA, and Security Overview cover: scope and US data location; information-security obligations (DPA §6.1, Annex II TOMs); incident notification (DPA §7, without undue delay; account owner contacted within 24h per the Security Overview); termination and deletion timelines (ToS; DPA §8); data export/portability; data privacy (DPA plus SCCs). Right to audit is satisfied by third-party audit/certification copies on request under NDA (DPA §6.2; SCC audit terms §11.7) — 37signals holds no company-level SOC 2, and datacenter reports are NDA-gated. Not incorporated as agreed terms: a change-management process (ToS reserves changes without notice; subprocessor changes get advance notice plus objection), a logging/monitoring capability clause, and operational-resilience SLAs (ToS: no SLA offered). The SSRM is not labeled as such.

#	Question	Response	Control ownership	Implementation
STA-12.1	Are supply chain agreements reviewed at least annually or upon significant changes?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
STA-13.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	No	Provider	The recurring internal compliance test is the bi-weekly staff-data-access audit (console1984/audits1984); there is no broad at-least-annual internal assessment program covering standards, policies, procedures, and SLA activities.
STA-14.1	Are policies that require all supply chain service providers to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Partial	Provider	DPA §5.1 requires every personal-data subprocessor to sign obligations no less protective than 37signals' DPA; suppliers outside that scope, and explicit audit/personnel-policy/service-level flow-down, are not itemized in public clauses.
STA-15.1	Are the organization's service providers' IT governance policies and procedures reviewed at least annually or upon significant changes?	Partial	Provider	Subprocessors' security and privacy obligations are set contractually (DPA §5.1) and checked at onboarding; the highest-risk provider class (datacenter colocation) is assessed through its independent SOC 2 Type II report, obtained each audit cycle and shareable under NDA. 37signals does not run a scheduled annual review of every subprocessor's own IT-governance policies; assurance for the remaining (small, US-based) subprocessor set rests on contractual flow-down and change-driven review.

#	Question	Response	Control ownership	Implementation
STA-16.1	Is a process defined and implemented for conducting risk-based security assessments of the supply chain?	Yes	Provider	Governed by 37signals' Supply Chain / Subprocessor Risk Management Policy (P-12) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

TVM — Threat & Vulnerability Management

#	Question	Response	Control ownership	Implementation
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities and threats to protect systems against vulnerability exploitation?	Yes	Provider	The Threat & Vulnerability Management Policy (P-13, adopted 2026-08-31; approved, communicated, applied, reviewed at least annually) documents the practice: continuous public HackerOne program (public since Oct 2020; private disclosure program since approximately 2014–2015 — the Security Response page evidences the longstanding pre-HackerOne researcher-acknowledgment history) plus third-party pentests, pre-release SAST, and dependency/patch management.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Threat & Vulnerability Management Policy (P-13) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.

#	Question	Response	Control ownership	Implementation
TVM-02.1	Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Provider	Governed by 37signals' Threat & Vulnerability Management Policy (P-13) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	Governed by 37signals' Threat & Vulnerability Management Policy (P-13) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	Provider	Vulnerability detection exceeds the monthly bar at the application layer and external surface: continuous external testing via HackerOne; Detectify automated scans daily (adaptive cadence) across basecamp.com, launchpad.37signals.com, hey.com, and app.hey.com; weekly Dependabot plus bundler-audit CVE checks and Brakeman SAST enforced in CI on every build. Qualified: a monthly vulnerability-detection mechanism for production hosts, network equipment, and managed endpoints is not separately documented.

#	Question	Response	Control ownership	Implementation
TVM-04.1	Are a threat analysis process and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for cloud systems?	No	Provider	No published threat-analysis process to identify/assess/review cloud threat landscape
TVM-04.2	Are threat models built according to industry best practices to inform the risk mitigation strategy?	No	Provider	No published industry-best-practice threat models
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Partial	Provider	Detection-signature updates are a documented internal practice: malware-signature databases on the Basecamp file-scanning and HEY mail-scanning pipelines are persisted per node and auto-updated from vendor and community feeds on a scheduled job, with metrics exported and alert rules in place, plus spam-filtering feeds. Held at Partial: the question's explicit weekly-or-better cadence is not yet evidenced — vendor feeds default to at-least-daily but the runbooks state no cadence, and the internally built monitor/auto-block signature cadence is unattested. A one-line internal attestation of update cadence upgrades this to Yes.

#	Question	Response	Control ownership	Implementation
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	Provider	Automated dependency-update and dependency-vulnerability identification runs on all production apps per the Threat & Vulnerability Management Policy (P-13, adopted 2026-08-31, which names dependency/patch management on the production stack): GitHub Dependabot (weekly, SIP-reviewed, staged cooldowns) plus bundler-audit CVE checking and Brakeman SAST enforced as blocking CI steps on every build (publicly visible in the open-source Fizzy repository; same configuration in Basecamp and HEY). Complements the minimal-dependency ('vanilla Rails') philosophy. Not yet named in a public 37signals statement.
TVM-07.1	Are processes, procedures and technical measures defined, implemented and evaluated for the periodic performance of penetration testing by independent third parties?	Yes	Provider	Continuous independent third-party testing via the public HackerOne program (a continuous but informal pentest channel), plus an annual CASA Tier 2 assessment for HEY (hey.com/security: passed annually) and historical formal third-party pentests for HEY and Basecamp 5. No fixed periodic cadence or published date for the most recent formal pentest.
TVM-08.1	Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?	Yes	Provider	Regular security patching (scheduled) + severity-triaged emergency remediation via HackerOne. No published remediation-SLA-by-severity table

#	Question	Response	Control ownership	Implementation
TVM-09.1	Is vulnerability remediation prioritized using a risk-based method from an industry-recognized framework?	Yes	Provider	HackerOne triage prioritizes by CVSS severity (recognized framework) mapped to bounty tiers. No published internal remediation-SLA/priority matrix
TVM-10.1	Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?	No	Provider	No published risk-based THREAT-prioritization method/ framework distinct from vuln CVSS scoring
TVM-11.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	Provider	HackerOne = track/report externally-reported vulns intake→remediation w/ reporter notification; affected customers contacted within 24h. Internal vuln-status reporting to mgmt not published
TVM-12.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Partial	Provider	Identification and intake metrics are public through the HackerOne program (hackerone.com/basecamp; as of August 2026, 100% response efficiency, $507,983 in total bounties paid, 18-hour average time to first response; program public since October 2020, private since approximately 2014-2015); remediation-outcome metrics and their reporting cadence are not published.

UEM — Universal Endpoint Management

#	Question	Response	Control ownership	Implementation
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	Provider	Handbook ‘Managing work devices’ = published endpoint policy: managed macOS (Kandji), managed Linux (Omarchy), unmanaged Android/iOS/Windows ‘untrusted’ (barred from code/secrets)
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	Provider	The Handbook ‘Managing work devices’ page is git-tracked and updated on significant change (public commit history); additionally the endpoint policy layer (P-14 and the Endpoint Data-Protection Policy, adopted 2026-08-31) commits to annual and on-change review. The first annual cycle is not yet completed.
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	Provider	Governed by 37signals’ Endpoint (UEM) Security Policy (P-14) — part of the existing-practice policy set adopted 2026-08-31, reviewed at least annually or upon significant change.
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	No	Provider	Endpoints are a homogeneous managed fleet (standard Kandji baseline on Macs, Omarchy standard image on Linux) with MDM-managed OS/app updates, which keeps compatibility uniform in practice — but no defined, documented compatibility-validation process exists; the Endpoint (UEM) Security Policy (P-14) does not state one.

#	Question	Response	Control ownership	Implementation
UEM-04.1	Is an inventory of all endpoints used and maintained to store, access and process company data?	Partial	Provider	Kandji centrally manages Macs (a managed-device inventory) and Omarchy Linux is the other managed class; unmanaged mobile and Windows devices that may access company data are not inventoried.
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Partial	Provider	Kandji enforces standard configuration on Macs (disk encryption, firewall, password rules, updates), Omarchy provides the Linux standard, Shipshape alerts on drift daily, and VPN/Tailscale gates access; unmanaged devices that may access company data are governed by policy prohibition rather than technical enforcement (see UEM-04.1).
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Partial	Provider	Kandji manages Macs and applies password rules; an enforced automatic screen-lock timeout is not explicitly attested in published sources.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Partial	Provider	Kandji manages endpoint configuration and applies the latest security updates, and Omarchy is maintained in-house; this MDM-driven management is adjacent to, not governed by, the organizational change-management process.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	Provider	Kandji enables disk encryption on managed Macs; Omarchy ships full-disk encryption. Strongest UEM answer

#	Question	Response	Control ownership	Implementation
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Partial	Provider	No dedicated anti-malware/ EDR agent is deployed on endpoints — a deliberate tooling decision, stated plainly (built-in macOS XProtect is not claimed as an attested control). The compensating-control posture is formalized in the Endpoint Data-Protection Policy (adopted 2026-08-31): MDM-enforced baseline (full-disk encryption, automatic screen lock, host firewall), daily fleet audit, remote wipe, scoped/consent-gated/ audited data access, and a no-personal-device rule.
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	Provider	Kandji enables firewall on managed Macs; Omarchy ships a firewall
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Partial	Provider	No endpoint DLP product is deployed and no formal risk assessment drives DLP rules — stated plainly (the 'per a risk assessment' limb remains open: the documented risk register (GRC-02.1, Partial) does not yet assess endpoint-DLP risk). Policy-level compensating controls are formalized in the Endpoint Data-Protection Policy: no personal data on work devices, code and secrets only on managed devices, scoped/consent-gated/ audited data access, and an MDM-enforced baseline with remote wipe.
UEM-12.1	Are remote geo-location capabilities enabled for all managed mobile endpoints, in accordance with applicable laws and regulations?	N/A	Provider	There are no managed mobile endpoints; managed endpoints are Mac laptops and Omarchy Linux, and mobile devices are explicitly unmanaged, so the control's target set is empty.

#	Question	Response	Control ownership	Implementation
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Partial	Provider	Remote company-data deletion is implemented for the Kandji-managed Mac fleet: remote wipe on loss, theft, or departure (published in the Handbook; formalized in the Endpoint Data-Protection Policy). The Omarchy Linux class of managed endpoints has no remote-wipe channel — loss or departure is handled by immediate credential and VPN revocation (1Password, Tailscale) with full-disk encryption protecting data at rest, which mitigates exposure but is not remote data deletion. Partial: the control is implemented for one of the two managed endpoint classes. The company reserves the right to seize devices.
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	Provider (third-party endpoints)	Contractors sign confidentiality agreements (contractual) + may only hold code/secrets on managed device (technical/policy) + subprocessor DPA flow-down. No attested technical verification of every 3rd-party endpoint