SAMPLE · ILLUSTRATIVE

gooseframe
LLC

PRACTICAL INCIDENT RESPONSE READINESS ASSESSMENT

Incident Response Readiness Review

Prepared for **Northbeam Software, Inc.**

A point-in-time readiness assessment & prioritized action plan

Engagement
IR Readiness — Standard Tier

Assessment window
Illustrative · sample dates

Prepared by
Joshua Geise
Gooseframe LLC

Classification
Confidential

This is a sample. Northbeam Software, Inc. is a fictional company created to illustrate Gooseframe's IR Readiness deliverable. All findings, names, and details are invented. No real systems were accessed, scanned, or tested to produce this document.

ABOUT THIS ENGAGEMENT

What this assessment is

Gooseframe's Incident Response Readiness Review answers one practical question for a small technical team: **if something goes wrong tomorrow, will the basics hold?** We look at the controls and habits that decide whether a security event becomes a bad afternoon or a bad quarter — identity, access, logging, backups, and the human process for responding — and we hand back a plain-English, prioritized plan you can act on without hiring a security team.

How we worked

- Structured interviews with engineering and operations leadership
- Review of configuration evidence you provided (screenshots, exports, settings)
- Mapping of findings to CISA, FTC, and NIST CSF 2.0 small-business guidance
- No exploitation, no penetration testing, no live scanning of production systems

What you get

- An executive summary your board and insurer can read
- A readiness scorecard across eight domains
- Prioritized findings grouped Fix First / Next / Later
- A 30/60/90-day roadmap and a break-glass packet

Read this first: This is a **point-in-time, evidence-based readiness opinion** — not an audit, a certification, a penetration test, or a guarantee. It reflects what was observable during the assessment window from the information made available. See **Limitations & Disclaimer** on the final page.

CHOOSE YOUR DEPTH

What each tier includes

Every engagement produces an executive-ready report and a prioritized plan. The tiers differ in how many domains are assessed, how deep the findings go, and how much live, hands-on time is included. **The pages that follow show the Standard-tier deliverable**; each section is tagged with the lowest tier it's included in.

Deliverable	Essential	Standard	Comprehensive
ASSESSMENT			
Domains assessed	3 core	All 8	All 8
Leadership interview(s)	1	up to 2	Extended, multi-team
Maturity scorecard	—	✓	✓
REPORT			
Executive summary	✓	✓	✓
Fix-First findings	✓	✓	✓
Full findings (Next / Later)	—	✓	✓
30 / 60 / 90-day roadmap	—	✓	✓
Break-glass packet	✓	✓	✓
IR handoff sheet (Day Zero)	—	✓	✓
LIVE & FOLLOW-UP			
Readout call	—	30 min	60-min working session
Written IR scenario walkthrough	—	—	✓
30-day follow-up check	—	—	✓
Typical turnaround	~1 week	1–2 weeks	~2 weeks
Price	**$750**	**$1,500**	**$2,500**

> **Most teams start at Standard.** It assesses the full environment, includes the Day Zero handoff sheet, and answers the bulk of an enterprise security questionnaire or insurance renewal. Essential is a fast, focused check; Comprehensive adds live facilitation and a follow-up.

FOR LEADERSHIP & THE BOARD

INCLUDED FROM ESSENTIAL

Executive summary

Northbeam is in a normal place for a 25-person Series A SaaS company: the product is moving fast, the cloud footprint is reasonable, and nobody owns security full-time. The fundamentals are **mostly present but unevenly enforced** — which is exactly the gap that turns a routine incident into an expensive one. None of the issues below require a big budget. Most require a decision and an afternoon.

The three things that matter most right now

#	Priority	Why it matters
1	**Enforce MFA everywhere, including admins**	MFA is on for most staff but not *required*, and two cloud admin accounts have it disabled. One phished password today is enough to reach production.
2	**Prove your backups actually restore**	Database backups exist but have never been test-restored, and they sit in the same cloud account as production. A ransomware or account-takeover event could take both at once.
3	**Write down who does what in the first hour**	There is no incident plan. In a real event, decision-making, communication, and escalation would be improvised — the costliest possible way to respond.

The good news. Identity is centralized, the team is small and reachable, logging is partially in place, and there is genuine appetite to fix things. Northbeam can close every Fix-First item below in roughly two weeks of part-time effort.

The risk if ignored. The same gaps that fail an enterprise security questionnaire or a cyber-insurance renewal are the ones an attacker uses. Today these are paperwork problems; unaddressed, they become breach problems.

Overall readiness

Composite rating: DEVELOPING — foundations exist; enforcement, testing, and documentation are the gaps.

READINESS AT A GLANCE

INCLUDED FROM STANDARD

Domain scorecard

Each domain is rated on a four-level maturity scale based on the evidence reviewed. **Initial** (ad hoc / absent) · **Developing** (present but inconsistent) · **Defined** (documented & enforced) · **Managed** (measured & improving).

Domain	Maturity	Headline
Identity & MFA	Developing	SSO in place; MFA not enforced; admin gaps.
Privileged / admin access	Initial	Too many standing admins; no access reviews.
Logging & monitoring	Developing	Logs exist but are siloed and short-retention.
Backups & recovery	Initial	Backups untested and not isolated from prod.
Ransomware readiness	Initial	Recovery path unproven; no tabletop run.
SaaS configuration	Developing	Reasonable defaults; guest/sharing sprawl.
Source code & secrets	Developing	No secret scanning; weak branch protection.
Incident response process	Initial	No written plan, roles, or escalation path.

> **How to read this:** "Initial" is not a failing grade — it is the honest starting point for most teams your size. The roadmap on the following pages turns each red domain into a small, ordered set of actions.

WHAT WE FOUND & WHAT TO DO

FIX-FIRST: ESSENTIAL · FULL: STANDARD

Prioritized findings

Findings are grouped by urgency, not by domain. Each carries a recommended action and a rough effort estimate so you can sequence the work realistically around shipping the product.

▶ Fix first — within 2 weeks

ALL TIERS

MFA is optional, and two admin accounts have it off

CRITICAL

IDM-01 · Identity & MFA

WHAT WE FOUND

Google Workspace SSO is the front door for ~90% of tools, but MFA is set to "available," not "enforced." Two AWS IAM users with administrative policies have no MFA device registered.

WHY IT MATTERS

A single reused or phished password reaches email, code, and production cloud. This is the most common root cause of small-company breaches and the first box on every insurer questionnaire.

RECOMMENDED ACTION

Enforce MFA org-wide with a short grace window; register hardware/app MFA on both admin accounts today; block legacy/basic-auth protocols.

Effort: ~½ day | Cost: $0 | Owner: IT / founder-eng

Backups have never been test-restored and live next to production

CRITICAL

BKP-01 · Backups & recovery

WHAT WE FOUND

Automated RDS snapshots run daily, but no restore has ever been performed, and snapshots reside in the same AWS account as production with the same admin credentials governing both.

WHY IT MATTERS

An untested backup is a hope, not a control. If an attacker (or ransomware) compromises the prod account, in-account backups can be deleted in the same breath.

RECOMMENDED ACTION

Perform one documented test-restore to a clean environment; copy snapshots to a separate account/region with restricted, MFA-gated access; record RPO/RTO you can actually meet.

Effort: 1 day | Cost: minimal | Owner: Platform eng

No written incident response plan or escalation path

HIGH

IRP-01 · Incident response process

WHAT WE FOUND

There is no documented plan for who is notified, who decides, and how customers/regulators are communicated with during an incident. Response would be improvised over Slack.

WHY IT MATTERS

The first hour of an incident is where most damage is contained or multiplied. Without predefined roles, teams lose time to confusion exactly when it is most expensive.

RECOMMENDED ACTION

Adopt the one-page break-glass packet in this report (roles, contacts, first-hour checklist). It is the 80/20 of an IR plan and can be live the same day.

Effort: 2 hrs | Cost: $0 | Owner: Eng lead

▶ Next — within 30–60 days

STANDARD & UP

Standing admin access is too broad and never reviewed

HIGH

PAM-01 · Privileged / admin access

WHAT WE FOUND

Six of 25 staff hold Google super-admin or AWS admin rights, including two engineers who no longer need them. No periodic access review exists, and one contractor account remains active post-engagement.

WHY IT MATTERS

Every admin is an attack path and an insider-risk surface. Dormant and contractor accounts are favorite footholds.

RECOMMENDED ACTION

Cut admins to the minimum; disable the contractor account; institute a 15-minute quarterly access review; separate daily-use accounts from break-glass admin accounts.

Effort: ½ day + quarterly | Owner: IT

Logs are siloed, short-retention, and not alertable

MEDIUM

LOG-01 · Logging & monitoring

WHAT WE FOUND

CloudTrail, Workspace admin logs, and GitHub audit logs each exist but are unconsolidated. Retention is 30–90 days, and no alerts fire on high-risk events (new admin, MFA disabled, mass download).

WHY IT MATTERS

If you cannot see it, you cannot respond to it — or reconstruct it afterward. Short retention also undercuts insurance and breach-investigation needs.

RECOMMENDED ACTION

Centralize the three log sources; extend retention to ≥1 year for audit logs; add a handful of high-signal alerts. A low-cost SIEM tier or cloud-native tooling is sufficient at this scale.

Effort: 1–2 days | Owner: Platform eng

No secret scanning; main branch lacks protection

MEDIUM

SEC-01 · Source code & secrets

WHAT WE FOUND

GitHub push protection and secret scanning are disabled, and the primary repo's main branch allows direct pushes without required review. One historical commit contains a now-rotated API key.

WHY IT MATTERS

Leaked secrets are a direct line into production and third-party services; unprotected branches let a single compromised laptop ship malicious code.

RECOMMENDED ACTION

Enable secret scanning + push protection (free on your plan); require PR review and status checks on main; confirm the exposed key is fully rotated and scope-limited.

Effort: 2–3 hrs | Owner: Eng lead

▶ Later — opportunistic / as you grow

STANDARD & UP

Area	Recommendation	Severity
SaaS sharing hygiene	Audit external guests and "anyone with link" sharing in Workspace; set default link scope to internal.	LOW
Device posture	Adopt lightweight MDM for laptops (disk encryption + screen lock enforcement).	LOW
Vendor inventory	Maintain a simple register of SaaS vendors with data access — feeds future SOC 2 work.	LOW
Security awareness	Quarterly 20-minute phishing/security refresher for all staff.	LOW

SEQUENCED PLAN

INCLUDED FROM STANDARD

30 / 60 / 90-day roadmap

The same findings, ordered as a realistic schedule for a team whose day job is shipping product.

Days 0–30 · Stop the bleeding	Effort: ~3 days total

- **Enforce MFA org-wide** and register MFA on both admin accounts (IDM-01)
- **Test-restore a backup** and copy snapshots to an isolated account (BKP-01)
- **Publish the break-glass packet** — roles, contacts, first-hour checklist (IRP-01)
- Disable the dormant contractor admin account (PAM-01, quick win)

Days 31–60 · Tighten access & visibility	Effort: ~3–4 days total

- **Right-size admin access** and stand up a quarterly review (PAM-01)
- **Centralize logs** and add high-signal alerts (LOG-01)
- **Enable secret scanning + branch protection** on core repos (SEC-01)

Days 61–90 · Prove it works	Effort: ~2 days total

- **Run a 60-minute tabletop** against the break-glass packet; capture what broke
- Close SaaS sharing gaps and start the vendor register (Later items)
- Re-rate the scorecard; target **Defined** on identity, backups, and IR process

> **Net effort:** roughly **8–9 working days spread over a quarter** moves Northbeam from "Developing" to a defensible "Defined" posture — and answers the bulk of any enterprise security questionnaire or insurance renewal honestly.

USE THIS IN A REAL EVENT

INCLUDED FROM ESSENTIAL

Break-glass packet

A one-page incident starter you can adopt today. Print it, pin it in your incident Slack channel, and fill the bracketed fields. This is the minimum viable incident plan referenced in finding IRP-01.

Who does what

Role	Owner (fill in)	Responsibility in an incident
Incident Lead	[Name / phone]	Runs the response, makes the call on severity and next steps. One person, always.
Tech Lead	[Name / phone]	Investigates, contains, and executes technical actions (lock accounts, rotate keys, isolate).
Comms / Exec	[Name / phone]	Owns customer, internal, and (if needed) regulator/ insurer communication. Approves external messages.
Scribe	[Name]	Timestamps every action and decision in one channel. Critical for insurance and lessons learned.

First-hour checklist

- ☐ Declare an incident; name the Incident Lead
- ☐ Open a dedicated channel; start the timeline
- ☐ Contain: disable affected accounts, rotate exposed credentials
- ☐ Preserve evidence before cleanup (logs, snapshots)
- ☐ Assess scope: what data/systems are involved?
- ☐ Decide on customer/insurer notification timing
- ☐ Do **not** wipe or rebuild until evidence is captured

Key contacts (fill in)

Cyber insurer hotline [carrier + policy #]

Cloud provider support [AWS support tier]

Legal counsel [name / firm]

Outside IR firm [if retained]

Primary SaaS vendors [Workspace / GitHub]

> **Insurer first.** Most cyber policies require prompt notification and may dictate which IR vendor you use. Call them before engaging outside help.

HAND THIS TO YOUR IR FIRM ON DAY ZERO

INCLUDED FROM STANDARD

IR handoff sheet

A signed retainer means someone answers the phone. **This sheet is what lets them do real work the moment they pick up.** In the first hours of an incident, responders need visibility first and authority second — every hour lost to "who owns the console?" or "can legal approve access?" is an hour the attacker keeps moving. Pre-fill this, keep it with your break-glass packet, and hand it over on the first call.

Platform & access inventory

The systems a responder needs read/investigative access to — and whether a dormant IR account already exists. Pre-provisioned, MFA-enrolled, disabled-by-default accounts turn access into a switch instead of a negotiation.

System	Console	Owner	IR account ready?	Enable procedure
Identity Google Workspace	admin.google.com	[name]	✗ not provisioned	Super-admin assigns role to dormant *ir-responder@*
Cloud AWS (prod + staging)	console.aws.amazon.com	[name]	✗ not provisioned	Enable pre-built *IR-ReadOnly* IAM role; MFA pre-set
Endpoint / EDR	— none deployed —	—	✗ no EDR	Gap: no endpoint telemetry available to responders
SIEM / logging	[tool]	[name]	✗ not provisioned	Grant investigator role on log platform
Source code GitHub	github.com/northbeam	[name]	✗ not provisioned	Add *ir-readonly* team with audit-log access
Critical SaaS (billing, support, data)	per-app	[name]	⚠ varies	List each app + how a responder gets read access

Logging & retention inventory

Responders reconstruct an attack from logs — including what happened *before* detection. If dwell time is six weeks and retention is two, the initial access and early movement are already gone. **90 days is the minimum baseline.**

Log source	Location	Retention	Meets 90-day floor?
Identity / auth + MFA events	Workspace admin	180 days	✓ yes
Cloud control plane (CloudTrail)	AWS	90 days	✓ at minimum
GitHub audit log	GitHub	~90 days	⚠ verify plan tier
Email security events	Workspace	30 days	✗ below floor
Network / VPN / firewall	[device]	14 days	✗ below floor
Endpoint / EDR telemetry	— none —	n/a	✗ not collected

Decision authority

Action	Who can authorize
Declare an incident	[name / role]
Isolate host / shut down system	[name / role]
Rotate credentials / revoke tokens	[name / role]
Approve external IR firm access	[name / role]

Out-of-band comms

Channel [e.g. Signal group, phone tree]

Members [incident mgr, IR firm, leads]

> **Assume corporate email/Slack may be compromised.** The handoff channel must live *outside* the affected environment and be tested before you need it — an untested channel is an experiment run during a crisis.

> **The readiness test:** can a responder enable a dormant account and pull 90 days of authentication logs within 30 minutes of the call? On this sample, the answer is "not yet" across most systems — which is the single highest-leverage thing Northbeam can fix before an incident, not during one. Framework: Gooseframe Day Zero readiness methodology.

IMPORTANT

Limitations & disclaimer

Point-in-time opinion. This report reflects observations made during the assessment window based on interviews and configuration evidence voluntarily provided by Northbeam Software, Inc. Security posture changes continuously; findings may not reflect the environment before or after this window.

Not an audit, certification, or penetration test. This engagement is a readiness review. It does not constitute a SOC 2, ISO 27001, HIPAA, or other compliance audit or certification, and it does not include penetration testing, exploitation, vulnerability scanning, or active testing of production systems. No assurance opinion is expressed or implied.

No guarantee. Implementing these recommendations reduces risk but cannot eliminate it. Gooseframe LLC makes no representation or warranty that following this report will prevent any security incident, breach, data loss, or insurance claim denial, or that it will satisfy any specific regulatory, contractual, or carrier requirement.

Client responsibility. The accuracy of this assessment depends on the completeness of the information provided. Prioritization, implementation, and ongoing operation of all controls remain the responsibility of Northbeam Software, Inc. Where legal, regulatory, or insurance obligations are referenced, the client should confirm specifics with qualified counsel and its carrier.

Confidential. This document is confidential and intended solely for Northbeam Software, Inc. The scope, exclusions, and limitation of liability agreed in the engagement letter govern this work.

Prepared by Joshua Geise · Gooseframe LLC · Practical Incident Response Readiness · Sample deliverable for illustration only.