



CYRAVEX SECURITY

OFFENSIVE INSIGHT. DEFENSIVE STRENGTH.

SAMPLE DELIVERABLE / SECURITY ADVISORY

Security Advisory Maturity & Roadmap

Illustrative executive advisory assessment demonstrating security-program maturity, risk prioritization, governance design, and a practical 90-day / 12-month roadmap.

CLASSIFICATION

PUBLIC SAMPLE

No real client data

ADVISORY MODEL

MATURITY + ROADMAP

Executive + technical view

VERSION

1.0

September 2026

Fictional organization, maturity scores, risks, and metrics only. No real client data was used.

01 / EXECUTIVE SUMMARY

Strong technical foundations need a stronger operating model

The illustrative organization has meaningful security controls in place, but governance, risk ownership, evidence discipline, and repeatable security decision-making are not yet mature enough to scale with enterprise growth.

OVERALL MATURITY 2.6 / 5 Developing	HIGH RISKS 6 Leadership attention	90-DAY ACTIONS 14 Prioritized	12-MONTH TARGET 3.5 / 5 Defined / Managed
--	--	--	--

EXECUTIVE MESSAGE

The near-term priority is not to deploy more tools. It is to formalize ownership, close material risks, standardize control evidence, and build a governance cadence that turns security findings into accountable business decisions.

- Create a formal risk register and risk-acceptance process with named owners and review dates.
- Standardize privileged-access, secure-SDLC, incident-readiness, and data-governance controls.
- Establish a small executive scorecard focused on risk, control effectiveness, and overdue actions.
- Use the first 90 days to create repeatability; use the following nine months to validate and mature the operating model.

02 / ASSESSMENT CONTEXT

A practical advisory baseline, not a certification exercise

This sample models a security-program review for a technology company preparing for larger customers, stronger governance, and more consistent internal security execution.

ILLUSTRATIVE OBJECTIVES

Understand current security maturity, identify material program gaps, define accountable owners, and create a sequenced improvement roadmap that leadership can operate and measure.

IMPORTANT BOUNDARY

This report is advisory and illustrative. It does not represent legal advice, formal audit attestation, accredited certification, or a guarantee of compliance.

- Review governance, risk, identity, data, application/cloud, detection/response, resilience, vendor risk, and security evidence.
- Assess whether controls are repeatable and owned - not just whether tools exist.
- Prioritize changes by business impact, external commitments, exploitability, and operational sustainability.

03 / METHODOLOGY

Maturity is measured by repeatability and evidence

The sample uses a five-level maturity model and maps themes to commonly used security-program concepts such as NIST CSF 2.0 and ISO/IEC 27001:2022 without claiming certification or audit status.

LEVEL	DESCRIPTION	WHAT IT MEANS
1 - Initial	Ad hoc, person-dependent, limited evidence	Illustrative maturity scale
2 - Developing	Controls exist but are inconsistent or incomplete	Illustrative maturity scale
3 - Defined	Documented, assigned, repeatable processes	Illustrative maturity scale
4 - Managed	Measured, reviewed, and actively governed	Illustrative maturity scale
5 - Optimized	Continuously improved using evidence and outcomes	Illustrative maturity scale

ASSESSMENT PRINCIPLE

A tool purchase does not automatically increase maturity. Maturity improves when ownership, process, evidence, monitoring, exceptions, and management review are repeatable.

04 / MATURITY SCORECARD

Current capability is uneven across control domains

DOMAIN	SCORE	STATUS
Governance & leadership		Developing
Risk management		Developing
Identity & access		Defined
Asset & data security		Developing
Application & cloud		Developing
Detection & response		Defined
Resilience & recovery		Developing
Third-party risk		Developing

RELATIVE STRENGTH

Central identity, MFA, endpoint visibility, and core cloud controls provide a useful technical foundation.

PRIMARY WEAKNESS

Governance, risk treatment, evidence, exception handling, and cross-team control ownership are not yet consistently operated.

05 / GOVERNANCE & LEADERSHIP

Security decisions need clearer authority and cadence

WHAT IS WORKING

Executive sponsorship exists, material incidents can reach leadership, and security concerns are discussed across technical teams.

GAP TO ADDRESS

Decision rights are not consistently documented. Risk acceptance, policy ownership, roadmap prioritization, and security steering rely too heavily on informal coordination.

- Create a monthly security leadership forum and quarterly executive/steering review.
- Define accountable owners for security domains, policies, major risks, and remediation programs.
- Document risk-acceptance authority and escalation thresholds.
- Maintain a 12-month security roadmap tied to business objectives and external commitments.
- Track security decisions, owners, due dates, and evidence of closure.

06 / RISK MANAGEMENT

Move from issue tracking to explicit risk treatment

CURRENT STATE

Findings are tracked in multiple systems, but inherent risk, control effectiveness, residual risk, treatment choice, acceptance authority, and review dates are not always visible in one place.

FIELD	REQUIRED PRACTICE	EXAMPLE OUTPUT
Risk statement	Cause + event + business impact	Compromise of privileged account could expose production data
Inherent risk	Impact and likelihood before controls	High
Existing controls	Preventive / detective / corrective	MFA, logging, conditional access
Residual risk	Risk after current controls	Medium
Treatment	Mitigate / Avoid / Transfer / Accept	Mitigate
Ownership	Named accountable owner	Head of Platform
Review	Due / acceptance expiry	Quarterly or event-driven

RISK RULE

Accepted risk is not closed risk. It stays visible until the acceptance expires, conditions change, or the risk is formally retired.

07 / ASSET & DATA GOVERNANCE

Ownership and data context must drive control decisions

CRITICAL ASSET OWNERS

82%

Illustrative

SENSITIVE DATA MAPPED

61%

Needs improvement

RETENTION RULES

Partial

Not consistent

UNOWNED SYSTEMS

7

Action required

PRIORITY CONTROLS

Business ownership, asset inventory, data classification, retention, backup responsibility, and approved sharing patterns.

COMMON FAILURE MODE

Security teams know where vulnerabilities exist but cannot reliably connect the system to business owner, data sensitivity, or remediation authority.

- Create a minimum asset ownership model for production systems and critical SaaS.
- Define practical data classes and handling expectations.
- Link retention and deletion rules to legal/business requirements and system owners.
- Use data sensitivity when prioritizing vulnerabilities, architecture reviews, and access controls.

08 / IDENTITY & ACCESS

Good foundations need stronger lifecycle and privileged-access governance

DOMAIN	SCORE	STATUS
MFA coverage		Strong
Privileged review		Needs cadence
Joiner/mover/leaver		Defined
Service accounts		Developing
Break-glass testing		Developing

- Quarterly privileged-access recertification with business/system owners.
- Formal joiner/mover/leaver evidence for high-risk applications.
- Service-account inventory with owner, purpose, privilege, authentication method, rotation, and retirement date.
- Break-glass accounts with separate controls, monitoring, and periodic test evidence.
- Conditional access and step-up authentication for high-risk contexts.

Security should become a normal engineering requirement

CURRENT PATTERN

Threat modeling, security testing, dependency review, and release security checks are used inconsistently across teams.

TARGET PATTERN

Risk-tier applications receive defined secure-design requirements, automated checks, independent validation when needed, and documented release exceptions.

CONTROL	MINIMUM EXPECTATION	EVIDENCE
Threat modeling	Required for material architecture / trust-boundary changes	Reviewed model / decision record
SAST / dependencies	Automated on supported repositories	CI result + owner
Secrets	No long-lived secrets in source; managed storage	Scan + vault configuration
Security testing	Risk-based testing before material release	Report / validation record
Exceptions	Time-bound approval for unresolved material risk	Exception + expiry

ENGINEERING PRINCIPLE

Secure SDLC should reduce late surprises, not create a separate approval bureaucracy for every change.

10 / CLOUD & INFRASTRUCTURE

Baseline controls are useful only when drift is visible and owned



- Define minimum cloud baseline for identity, logging, encryption, network exposure, secrets, and administrative access.
- Use infrastructure-as-code and policy checks where feasible to reduce manual drift.
- Review public exposure and privileged roles on a recurring cadence.
- Separate production and non-production administration paths.
- Ensure material cloud changes have owner, reason, and review evidence.

FOCUS

Prioritize exploitable exposure and excessive privilege before chasing low-value configuration completeness.

11 / DETECTION & INCIDENT READINESS

Visibility exists, but response roles need more validation

[illegible]

OPERATIONAL PRIORITY

Validate a small set of high-value detections and response paths against realistic attack scenarios.

LEADERSHIP PRIORITY

Define who declares an incident, who communicates, who can isolate systems, and when legal/customer/leadership escalation occurs.

- Run at least one cross-functional tabletop around a credible business scenario.
- Maintain critical contact and escalation paths outside normal collaboration tools.
- Measure detection-to-triage and decision quality for priority scenarios, not raw alert volume.

12 / RESILIENCE & RECOVERY

Recovery capability must be tested, not assumed

CURRENT STRENGTH

Backups and cloud resilience mechanisms exist for major systems.

PRIMARY GAP

Business recovery objectives, restore evidence, dependency mapping, and ransomware-oriented recovery exercises are inconsistent across services.

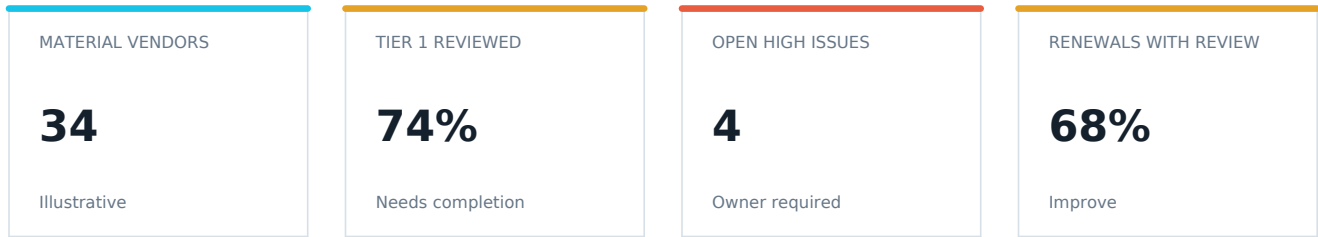
AREA	MINIMUM PRACTICE	REVIEW
Business impact	Identify critical services and dependencies	Annual / material change
RTO / RPO	Set business-approved targets	Annual
Backups	Protected, monitored, least privilege	Continuous
Restore test	Verify recoverability, not backup existence	Quarterly / risk-based
Crisis communication	Maintain decision and communication paths	Tabletop / annual

RESILIENCE RULE

A green backup dashboard is not evidence that the business can recover within required time and data-loss tolerances.

13 / THIRD-PARTY RISK

Apply depth based on business dependency and data access



- Tier vendors by data sensitivity, privileged access, operational dependency, and substitutability.
- Require deeper review for critical providers instead of identical questionnaires for every vendor.
- Track unresolved vendor risk to an internal business owner.
- Include security requirements, incident notification, data handling, and exit/termination considerations where appropriate.
- Reassess material vendors on renewal or significant change.

14 / PEOPLE, POLICY & EVIDENCE

Policies should support behavior and proof, not exist only for audits

PEOPLE CONTROLS

Role-based awareness for engineering, privileged administrators, finance, and leadership is more useful than generic annual training alone.

POLICY CONTROLS

Keep a small owned policy set with clear review dates, supporting procedures, and evidence of operation.

POLICY / STANDARD	OWNER	OPERATING EVIDENCE
Access Control	Security / IT	Access reviews, JML tickets, exceptions
Secure Development	Engineering / Security	CI checks, threat models, testing
Incident Response	Security / Leadership	Tabletop, incident records, contacts
Data Handling	Privacy / Business / Security	Classification, retention, access
Vendor Security	Procurement / Security	Risk tiers, reviews, contracts

15 / PRIORITY RISK REGISTER

Illustrative material risks requiring explicit treatment

R-01	HIGH	Security Lead / Exec	30 days
Security risk ownership and acceptance are inconsistent			
Business impact: Material risks can remain unresolved without clear decision authority.			
Recommended treatment: Formalize risk register, treatment, approval, and expiry.			
R-02	HIGH	IT / Platform	45 days
Privileged access recertification is inconsistent			
Business impact: Excessive access may persist across high-value systems.			
Recommended treatment: Quarterly reviews + service-account ownership.			
R-03	HIGH	Engineering	60 days
Secure SDLC controls vary by engineering team			
Business impact: Material application risk may reach production without consistent review.			
Recommended treatment: Define risk-tier secure SDLC baseline and exceptions.			
R-04	HIGH	Security / Exec	60 days
Incident roles and tabletop evidence are incomplete			
Business impact: Response may be delayed or fragmented during a material incident.			
Recommended treatment: Approve roles, escalation, contacts, and run tabletop.			
R-05	HIGH	Data / Business	90 days
Sensitive-data inventory and retention are incomplete			
Business impact: Protection and deletion obligations may be applied inconsistently.			
Recommended treatment: Define data owners, classes, retention, critical flows.			

15 / PRIORITY RISK REGISTER - CONTINUED

Remaining material risks and treatment priorities

R-06	HIGH	IT / Product	90 days
Recovery evidence is inconsistent for critical services Business impact: Backups may not meet required recovery outcomes during disruption. Recommended treatment: Define RTO/RPO and validate restores for critical services.			
R-07	MEDIUM	Procurement / Security	90 days
Third-party review depth is inconsistent Business impact: Material suppliers may introduce unmanaged security dependencies. Recommended treatment: Vendor tiering and renewal review workflow.			
R-08	MEDIUM	Security Lead	45 days
Executive security metrics are activity-heavy Business impact: Leadership may not see unresolved risk or control effectiveness clearly. Recommended treatment: Adopt concise risk/KRI scorecard.			

16 / FIRST 30 DAYS

Create decision structure before expanding the program

PRIORITY	ACTION	OWNER	TARGET
P1	Approve risk register model	Security Lead + Exec	Week 1
P1	Assign owners to top material risks	Executive sponsor	Week 1
P1	Define monthly security leadership forum	Security Lead	Week 2
P1	Review privileged/admin access for crown-jewel systems	IT / Platform	Week 2
P1	Confirm incident leadership and emergency contacts	Security / Exec	Week 2
P2	Inventory policies, standards, evidence owners	Security / GRC	Week 3
P2	Define secure-SDLC minimum baseline	Engineering / Security	Week 4
P2	Identify critical services, RTO/RPO owners	IT / Product	Week 4

30-DAY SUCCESS CRITERIA

Leadership can see the top risks, who owns them, what treatment is expected, what evidence is required, and when decisions are reviewed.

17 / DAYS 31-90

Operationalize the highest-value controls

WINDOW	DOMAIN	OUTCOME
31-45	Governance	Run first monthly risk review; approve acceptance workflow; publish roadmap.
31-60	Identity	Complete privileged review; service-account ownership; break-glass test.
31-60	Engineering	Roll out secure-SDLC baseline to highest-risk applications.
45-75	Incident readiness	Run executive/technical tabletop; capture actions and evidence.
45-75	Data	Assign sensitive-data owners; define high-value retention and handling rules.
60-90	Resilience	Validate restore for critical service and record actual RTO/RPO performance.
60-90	Third party	Complete Tier 1 vendor review backlog and renewal workflow.
60-90	Metrics	Deliver executive scorecard with trend, owner, target, and decision.

90-DAY SUCCESS CRITERIA

The program should move from person-dependent security activity to a documented, owned, repeatable operating cycle with visible risk treatment and evidence.

18 / 12-MONTH ROADMAP

Sequence maturity so the organization can sustain it

PHASE	OBJECTIVE	KEY OUTCOMES
Q1	Foundation	Risk ownership, governance cadence, privileged access, secure SDLC baseline, incident roles, core evidence.
Q2	Consistency	Data governance, vendor tiering, cloud drift controls, detection validation, recovery testing.
Q3	Measurement	KRIs, control effectiveness, exception aging, engineering coverage, quarterly executive reporting.
Q4	Optimization	Automate evidence where valuable, refine controls using trends, reduce recurring root causes, plan next-year investment.

WHAT TO AVOID

Launching too many initiatives at once, measuring tool activity, or creating policy without operating evidence.

WHAT TO SUSTAIN

Named ownership, clear treatment decisions, repeatable reviews, verified controls, and a roadmap linked to business growth.

19 / TARGET STATE

A realistic near-term maturity target

[illegible]

TARGET-STATE NOTE

The target should be adjusted to business context, risk appetite, customer commitments, regulation, threat exposure, and available resources. Maturity is not a race to level 5 in every domain.

20 / EXECUTIVE KPI & KRI SET

Measure decisions, exposure, and control effectiveness

METRIC	TYPE	DECISION VALUE	CADENCE
Top risks overdue	KRI	Count / age of material risks beyond agreed treatment date	Monthly
High/Critical remediation SLA	KPI	Percent closed within target by severity and exposure	Monthly
Privileged review completion	KPI	High-risk accounts reviewed with owner evidence	Quarterly
Security exceptions overdue	KRI	Exceptions past expiry or review date	Monthly
High-risk app security coverage	KPI	Risk-tier applications receiving required security checks	Monthly / Release
Priority detection validation	KPI	Critical use cases tested and producing expected evidence	Quarterly
Recovery validation	KPI	Critical services with successful restore/recovery evidence	Quarterly
Tier 1 vendor open risk	KRI	Material third-party issues without approved treatment	Monthly

METRIC RULE

Every executive metric should have a target, trend, accountable owner, and a decision path. Avoid vanity measures such as raw alert counts or total policy count.

21 / GOVERNANCE OPERATING MODEL

A lightweight cadence that keeps risk visible

CADENCE	FORUM	PURPOSE	OUTPUT
Weekly	Security operations	Critical vulnerabilities, incidents, urgent exceptions, control failures	Owners + immediate actions
Monthly	Security leadership	Risk register, roadmap, metrics, exceptions, cross-team blockers	Decisions + owners + due dates
Quarterly	Executive / steering	Top business risks, maturity progress, major commitments, investment	Risk acceptance + priorities
Annually	Program strategy	Risk appetite, objectives, policy framework, major testing plan	Next-year roadmap

CLIENT LEADERSHIP

Own business risk decisions, priorities, resourcing, policy approval, and acceptance authority.

CYRAVEX ADVISORY

Provide independent analysis, roadmap guidance, risk framing, architecture/security advice, and executive-ready reporting within scope.

Flexible support without pretending to replace internal ownership

FRACTIONAL SECURITY ADVISOR

Recurring senior guidance: monthly risk review, 90-day roadmap, architecture decisions, security questionnaires, policy/control guidance, executive reporting, and remediation prioritization.

FOCUSED ADVISORY PROJECT

Time-boxed maturity assessment, risk baseline, architecture review, incident-readiness exercise, control roadmap, or customer-security readiness engagement.

ENGAGEMENT RULE	PRACTICE
Scope	Define objectives, decisions, deliverables, cadence, and hours.
Ownership	Client retains final business, legal, and risk decisions.
Evidence	Recommendations should reference verified information and stated assumptions.
Escalation	Emergency/incident support is included only when explicitly contracted.
Boundaries	No legal advice, audit attestation, or certification issuance unless separately provided by qualified parties.

23 / CONCLUSION

Build a security program that can be operated, evidenced, and improved

The illustrative organization can materially improve security without launching a large transformation. The key is to make risk ownership explicit, standardize high-value controls, verify that those controls work, and give leadership concise information for decisions.

CYRAVEX SECURITY

Security Advisory engagements combine practical risk management, technical context, program design, architecture guidance, and executive communication to help organizations improve security without unnecessary complexity.

Discuss Security Advisory | cyravex.com

This document is a fictional sample deliverable and contains no real client data.