THREATNEXIS · 90-DAY RISK PROGRAM SPRINT TRA

How to Build a Repeatable Risk Assessment Program in 90 Days — Without Hiring a Ne

Phase 1 Tasks Done	Phase 2 Tasks Done	Phase 3 Tasks Done	Total Risks Logged	Critical / High Risks
0	0	0	10	4
of 14 tasks	of 14 tasks	of 14 tasks	in register	need action

PHASE COMPLETION TRACKER

Phase 1 — Foundation (Days 1–30)	0%	
Phase 2 — Execute (Days 31–60)	0%	
Phase 3 — Sustain (Days 61–90)	0%	

HOW TO USE THIS WORKBOOK

✅ Phase 1 Checklist	Work through Days 1–30 tasks. Mark each 'Done' to update the dashb
✅ Phase 2 Checklist	Work through Days 31–60 tasks. Complete all Phase 1 items before st
✅ Phase 3 Checklist	Work through Days 61–90 tasks. This phase creates program repeatal
⚡ Risk Register	Log identified risks during Phase 2. Likelihood × Impact auto-calculate
🗂️ Asset Inventory	Build your asset inventory in Phase 1, Week 3. Used in risk register.
👥 Roles & RACI	Assign named individuals to each role before Day 30.

PREMIUM TOOLKIT: Complete template pack · Assessment playbook · Findings report · PowerPoint d

ACKER

w Team

oard.

tarting.

bility.

s.

deck · threatnexis.

Phase 1 — Foundation [Days 1–30]

Task ID	Task Description	Status	Owner	Target Date
P1-001	Executive sponsor identified and commitment confirmed	Not Started		
P1-002	Risk Assessment Charter drafted	Not Started		
P1-003	Risk Assessment Charter signed by executive sponsor	Not Started		
P1-004	Scope statement written and reviewed by IT & business owners	Not Started		
P1-005	Stakeholder map completed — all owners identified and notified	Not Started		
P1-006	90-day calendar built, distributed, and calendar invites accepted	Not Started		
P1-007	documented (Likelihood × Impact	Not Started		
P1-008	documented (NIST SP 800-30	Not Started		
P1-009	(Financial, Operational,	Not Started		
P1-010	+ Operations + one Business Unit	Not Started		
P1-011	with classification and criticality	Not Started		
P1-012	All roles assigned with named individuals	Not Started		
P1-013	Stakeholder interview template finalized and reviewed	Not Started		
P1-014	Risk register template built and reviewed	Not Started		

COMPLETION	14 tasks done		

Wk 1
Wk 1
Wk 1
Wk 1
Wk 1
Wk 1
Wk 2
Wk 2
Wk 2
Wk 3
Wk 3
Wk 4
Wk 4
Wk 4

Phase 2 — Execute [Days 31–60]

Task ID	Task Description	Status	Owner	Target Date
P2-001	All stakeholder interviews scheduled (one per system in	Not Started		
P2-002	Interview 1 completed and notes documented	Not Started		
P2-003	Interview 2 completed and notes documented	Not Started		
P2-004	Interview 3 completed and notes documented	Not Started		
P2-005	All remaining interviews completed and notes documented	Not Started		
P2-006	STRIDE analysis applied to each in-scope asset	Not Started		
P2-007	Threats and vulnerabilities identified and documented per	Not Started		
P2-008	Threat actor types documented for each finding	Not Started		
P2-009	All risks scored using documented methodology (L × I)	Not Started		
P2-010	Control effectiveness rated for each risk (None / Low / Moderate / S	Not Started		
P2-011	Residual risk scores calculated for all findings	Not Started		
P2-012	Risk priorities assigned (P1–P4) based on residual scores	Not Started		
P2-013	Risk register draft completed — all required fields populated	Not Started		
P2-014	Risk owners assigned for all findings and confirmed with	Not Started		
COMPLETION		14 tasks done		

Wk 5
Wk 5
Wk 5
Wk 5
Wk 5
Wk 6
Wk 6
Wk 6
Wk 7
Wk 7
Wk 7
Wk 7
Wk 8
Wk 8

Phase 3 — Sustain [Days 61–90]

Task ID	Task Description	Status	Owner	Target Date
P3-001	Findings report executive summary written (1 page)	Not Started		
P3-002	Full findings report completed (scope, methodology, findings,	Not Started		
P3-003	Executive briefing deck built from findings report	Not Started		
P3-004	Executive briefing delivered to leadership team	Not Started		
P3-005	Board-level presentation scheduled (if applicable)	Not Started		
P3-006	All P1 and P2 remediation owners confirmed and accepted	Not Started		
P3-007	Target remediation dates set for all P1 and P2 findings	Not Started		
P3-008	Quarterly risk register review meetings scheduled (4 quarters	Not Started		
P3-009	Risk exception process documented	Not Started		
P3-010	Assessment playbook written so another person could run Cycle 2 from this document	Not Started		
P3-011	Cycle 2 scope defined in writing	Not Started		
P3-012	Cycle 2 kickoff date scheduled on organizational calendar	Not Started		
P3-013	Program KPIs defined and baseline values recorded	Not Started		
P3-014	Program formally declared operational — Day 90 milestone	Not Started		

COMPLETION	14 tasks done		

Wk 9
Wk 9
Wk 10
Wk 10
Wk 10
Wk 11
Wk 11
Wk 11
Wk 11
Wk 12
Wk 12
Wk 12
Wk 12
Wk 12

RISK REGISTER · Auto-Scoring · NIST

Enter Likelihood (1–5) and Impact (1–5) — Gross Sco

Risk ID	Risk Description	Asset	Likelihood (1–5)	Impact (1–5)	Gross Score (Auto)
R-001	Customer account takeover via credential stuffing — no MFA	Customer Portal	5	4	**20**
R-002	Privilege escalation in Finance ERP via shared admin	Finance ERP	3	5	**15**
R-003	Customer data exposure via misconfigured S3 buckets with	AWS S3	3	5	**15**
R-004	Business email compromise via DMARC policy in p=none mode	Corporate Email	4	4	**16**
R-005	Supply chain breach via unvetted third-party payroll processor	Payroll System	2	5	**10**
R-006					
R-007					
R-008					
R-009					
R-010					

SP 800-30 · L × I Methodology

re, Rating, and Priority auto-calculate

Risk Rating (Auto)	Existing Controls	Residual Risk Rating	Risk Owner	Target Date	Status
Critical	CAPTCHA, partial rate limiting	High			Not Started
High	AD groups only; no privileged access	Critical			Not Started
High	Encryption at rest; no access logging	Critical			Not Started
High	Email filtering; phishing	High			Not Started
Medium	Contractual terms only; no security assessment	High			Not Started
					Not Started
					Not Started
					Not Started
					Not Started
					Not Started

ASSET INVENTORY · Phase 1, Week 3 Delive

Asset ID	Asset Name	Category	Owner	Data Sensitivity	Internet Exposed?
A-001	Customer Web Portal	Application	IT / Dev Team	PII / Financial	Yes
A-002	Finance ERP (SAP/Oracle)	Application	Finance / IT	Financial / PII	No
A-003	AWS S3 Data Lake	Cloud Storage	DevOps	Mixed — some PII	Yes (partial)
A-004	Active Directory / Azure AD	Identity	IT Admin	All Credentials	No
A-005	Corporate Email (M365)	SaaS	IT	Confidential	Yes
A-006	Payroll Processor (Third Party)	Vendor System	HR / Finance	PII / Financial	Via vendor
A-007	Employee Laptops (Fleet ~150)	Endpoint	IT	Mixed	Indirect
A-008					
A-009					
A-010					

erable

Criticality	Notes
Critical	Public-facing; primary revenue system
Critical	Core financial reporting system
High	Legacy migration left 2 buckets public
Critical	Core identity infrastructure
High	Primary phishing attack vector
Critical	Subprocessors unknown
Medium	Remote workforce; AV aging

ROLES & RACI — Assign Names Before Day 30

Role	Existing Title	Named Individual	Key Responsibilities
Risk Program Lead	CISO / IT Manager / vCISO	**[Enter name]**	Owns the program, chairs meetings, presents to board, signs findings report. 4–6 hrs/week
Assessment Analyst	Senior Security Analyst / IT Analyst	**[Enter name]**	Runs interviews, populates risk register, performs threat ID. 10–15 hrs/week (Weeks 5–8)
Executive Sponsor	CIO / CFO / CEO	**[Enter name]**	Signs charter, removes blockers, receives quarterly briefing. 1–2 hours total per cycle
Asset Owner — IT	IT Director / IT Manager	**[Enter name]**	Interview subject for IT systems. Attends one 90-minute interview. Validates asset inventory
Asset Owner — Finance	CFO / Finance Director	**[Enter name]**	Interview subject for financial systems. 90-minute interview commitment
Asset Owner — Operations	COO / Operations Manager	**[Enter name]**	Interview subject for operational systems. 90-minute interview commitment
Asset Owner — HR	CHRO / HR Manager	**[Enter name]**	Interview subject for HR and payroll systems. 90-minute interview commitment
Risk Register Owner	IT GRC / Compliance / Program Office	**[Enter name]**	Maintains register, tracks remediation status, prepares quarterly review. 2–4 hrs/week
Remediation Owners (P1/P2)	Varies — assigned per finding	**[Enter name]**	Own P1/P2 findings. Set and meet remediation dates. Report status