DOCUMENT 04 / 05 · THE PROGRAM

30 / 60 / 90 Day Plan.

Your practical, week-by-week path to a working IR 2.0 program.

Designed to be achievable alongside the day job. Each task is small enough to finish in an afternoon and load-bearing enough to compound. Three checkpoints — at days 30, 60, and 90 — mark the work that has actually moved the program forward.

SERIES	DOCUMENT	VERSION	LICENSE
IR 2.0	04 of 05	1.3 · 2025	CC BY 4.0

HOW TO USE THIS

Don't try to do everything at once. Focus on one task per day. *Consistency beats intensity.* Check items off as you complete them; carry incomplete items forward without renegotiating the rest of the schedule.

30 Foundation.

"Get your house in order" — assess current state, baseline documentation, quick wins.

DAYS 1 – 30

WEEK 01 Assessment

- D 01 Download a cyber-insurance application — your free gap assessment.
- D 02 Complete the insurance checklist. Every "No" is a project.
- D 03 Inventory current security tools. What you have, what's missing.
- D 04 Identify IR stakeholders: IT, Legal, HR, Comms, executive sponsor.
- D 05 Document current backup status. Backed up? Tested? Immutable?

WEEK 02 Quick wins

- D 06–7 Enable MFA on all admin accounts, email, and VPN.
- D 08 Verify EDR coverage — every endpoint has an agent and is reporting.
- D 09 Test one backup restoration. Document time, success, issues.
- D 10 Build the emergency contact list — personnel, vendors, legal, broker.

WEEK 03 Documentation

- D 11–12 Draft the IR One-Pager — severity levels, roles, escalation triggers.
- D 13 Define incident severities (P1 / P2 / P3 / P4 or Critical → Low).
- D 14 Document IR communication channels (Slack, Teams, email DL).
- D 15 Draft comms templates — internal, customer, press.

WEEK 04 Validation

- D 16–17 Review IR One-Pager with stakeholders. Get feedback and buy-in.
- D 18 Schedule first tabletop drill for days 45 – 60. Send invites.
- D 19 Open the shared evidence folder for insurance documentation.
- D 20 Brief the executive sponsor. Frame gaps as risk items.

CHECKPOINT · DAY 30

IR One-Pager drafted · Big 3 controls verified · insurance gaps identified · first tabletop scheduled.

60 Playbooks & Practice.

"From plan to practice" — build the first playbooks and run the first drill.

DAYS 31 – 60

WEEK 05 First playbook

D 21–23	Build Playbook #1 — Endpoint Quarantine + Identity Revoke.
D 24	Document manual endpoint-isolation steps in your EDR.
D 25	Document manual identity / session revocation in your IdP.

WEEK 06 More playbooks

D 26–27	Build Playbook #2 — Phishing Burst Response.
D 28–29	Build Playbook #3 — SaaS Consent Kill.
D 30	Review playbooks with the technical team. Steps accurate?

WEEK 07 Tabletop prep

D 31–32	Develop tabletop scenario (suggest: ransomware on file server). Write inject cards.
D 33	Prepare materials — scenario brief, role cards, timeline.
D 34	Send pre-reads. Remind participants of date and time.
D 35	Dry-run with one colleague. Adjust timing and injects.

WEEK 08 Execute & learn

D 36–37	Run the first tabletop (60–90 min). Document observations.
D 38	Conduct debrief. Capture lessons and improvements.
D 39	Update One-Pager and playbooks based on findings.
D 40	Brief sponsor on results — gaps, remediation, momentum.

CHECKPOINT · DAY 60

Three playbooks documented · first tabletop completed · lessons captured · IR program actively improving.

90 Automation & Improvement.

"From manual to automated" — first Calm Loop and a continuous-improvement cadence.

DAYS 61 — 90

WEEK 09 Automation planning

D 41–42	Identify first automation candidate — alert enrichment workflow.
D 43	Document the manual steps it replaces. Measure current time.
D 44	Define Reversibility Score for each automated action.
D 45	Draft RS policy — RS 1/2 auto-execute · RS 3+ require approval.

WEEK 10 First automation

D 46–48	Build first automation — alert → enrich → ticket → notify.
D 49	Test in non-prod or with low-severity alerts first.
D 50	Document trigger, steps, expected output, rollback procedure.

WEEK 11 Metrics

D 51	Define IR KPIs — MTTD, MTTR, incident type, false-positive rate.
D 52	Set up basic metrics tracking (a spreadsheet is fine to start).
D 53	Establish baseline metrics from recent incidents.
D 54–55	Build remaining playbooks — Stolen Credential · Data Exfil.

WEEK 12 Continuous improvement

D 56	Schedule quarterly tabletop drills for the next 12 months.
D 57	Create blameless post-incident review template.
D 58	Update insurance documentation with new evidence.
D 59	Build 90-day summary for the executive sponsor.
D 60	Celebrate. The foundation is built.

CHECKPOINT · DAY 90

Five playbooks live · first automation in production · metrics baseline established · quarterly drill cadence on the calendar · insurance-ready documentation.

DAYS 91 – 180 · WALK

- Deploy SIEM if not already in place
- Build more automated Calm Loops
- Expand playbook coverage to 80%+
- Integrate threat-intelligence feeds

DAYS 181 – 365 · RUN

- AI-assisted triage in production
- Chaos engineering / live-fire drills
- Full Calm Loop automation
- Continuous improvement culture