anchor@anchor-cyber:~$ cat ir-plan-structure.md

ANCHOR CYBER SECURITY LLC

IR Plan Structure Reference

NIST SP 800-61 Rev 2 — required plan sections, four-phase response lifecycle, and tabletop exercise scenario types for IR planning and testing.

$ ir-plan --phases

Four-Phase Response Lifecycle — NIST SP 800-61 Rev 2

NIST SP 800-61 structures incident response as four phases. The phases are a lifecycle, not a strict sequence — detection and analysis continue throughout containment, and lessons learned feed back into preparation.

Phase 1 Preparation § 3.1

- Establish and document the IR policy, plan, and procedures before an incident occurs
- Define roles and responsibilities: IR lead, executive sponsor, legal, PR, IT, affected business units
- Maintain and test the call tree and escalation path — verify contact info quarterly
- Pre-authorize external resources: IR retainer, forensics firm, legal counsel, cyber insurer hotline
- Identify and inventory critical systems, data flows, and crown-jewel assets
- Establish and baseline logging for key systems; verify log completeness before an incident reveals gaps
- Conduct tabletop exercises at minimum annually; update the plan after each exercise
- Maintain offline or out-of-band copies of the IR plan and contact lists

Phase 2 Detection & Analysis § 3.2

- Establish an initial incident severity rating (P1/P2/P3 or equivalent) at first detection
- Document all observations with timestamps from the moment detection begins — this becomes evidence
- Determine the attack vector, affected systems, and scope of compromise before concluding analysis
- Distinguish between an incident and an event: an event is any observable occurrence; an incident is one that violates policy or causes harm
- Use indicators of compromise (IoCs) to expand scope — adversaries rarely stop at one system
- Notify appropriate internal stakeholders per the escalation matrix based on severity
- Preserve volatile evidence (running processes, memory, network connections) before containment changes system state
- Engage legal counsel before communicating externally about the incident

Phase 3 Containment, Eradication & Recovery § 3.3

- **Containment:** isolate affected systems while preserving forensic evidence; make isolation decisions with business continuity in mind
- Choose short-term containment (network segmentation, blocking) vs. long-term containment (reimaging, credential rotation) based on dwell-time confidence
- **Eradication:** identify and remove all attacker artifacts — malware, persistence mechanisms, backdoor accounts, scheduled tasks
- Confirm eradication is complete before beginning recovery; re-infection during recovery is the most common failure mode
- **Recovery:** restore systems from known-good backups or clean builds; apply patches before bringing systems back online
- Monitor restored systems more intensively post-recovery for signs of re-compromise
- Issue external notifications on the legally required schedule — do not wait for full eradication before notifying regulators if timelines require earlier action
- Document every containment and eradication action taken with timestamps

Phase 4 Post-Incident Activity § 3.4

- Conduct a lessons-learned meeting within two weeks of incident resolution — while events are fresh
- Produce a written post-incident report covering: timeline, root cause, impact, actions taken, and recommendations
- Update the IR plan, detection rules, and runbooks to close gaps revealed by the incident
- Track all recommendations as formal remediation items with owners and deadlines
- Retain all incident documentation per the organization's retention policy (check regulatory requirements — HIPAA, PCI DSS, SOC 2 each have specifics)
- Debrief the executive sponsor and board if the incident was material

$ ir-plan --required-sections

Required IR Plan Sections — what auditors and insurers expect to see

SECTION	REQUIRED BY	WHAT IT MUST CONTAIN
Purpose & Scope	All frameworks	What the plan covers, which systems and data types are in scope, who it applies to
Roles & Responsibilities	HIPAA · SOC 2 · NIST	IR team members, decision authority, backup contacts, external resource contacts
Incident Classification	NIST · SOC 2	Severity tiers (e.g., P1–P3), criteria for each tier, and who is notified at each level
Detection & Reporting Procedures	All frameworks	How employees report suspected incidents, where reports go, initial triage steps
Containment & Eradication Procedures	All frameworks	Specific steps for common incident types (ransomware, data breach, BEC, unauthorized access)
Communication Plan	HIPAA · PCI DSS · SOC 2	Internal escalation matrix, external notification contacts (regulator, insurer, legal), customer notification templates
Breach Notification Timelines	HIPAA · GDPR · state laws	Regulatory deadlines by data type and jurisdiction; who drafts and approves notifications
Evidence Preservation	Legal · forensics	Log retention policy, chain of custody, forensic imaging procedures
Recovery Procedures	All frameworks	Restoration steps, backup verification, system hardening before reconnection
Testing & Review Schedule	HIPAA · SOC 2 · NIST	How often the plan is tested (tabletop, simulation), who reviews updates, version control

$ ir-plan --tabletop-scenarios

Tabletop Exercise Scenario Types

Tabletop exercises test decision-making and communication, not technical response. A well-run tabletop takes 2–4 hours, uses injects to evolve the scenario, and ends with a structured debrief — not just a retrospective discussion.

Ransomware

- Activation and initial isolation decisions
- Backup viability and restoration timeline
- Regulatory notification triggers
- Ransom payment decision authority

Business Email Compromise

- Wire transfer recall procedures
- Scope of mailbox compromise
- Vendor and partner notification
- Ongoing fraud detection gap

Data Breach / Exfiltration

- Scope determination and data classification
- Notification obligation triggers by jurisdiction
- Forensic preservation vs. remediation tension
- Customer and regulator communication

Insider Threat

- HR and legal involvement from minute one
- Evidence preservation without alerting subject
- Access revocation timing
- Scope of data access review

Supply Chain / Vendor Compromise

- Third-party notification and access revocation
- Lateral movement scope assessment
- Contract and SLA implications
- Alternate vendor activation

Phishing Campaign

- Credential reset scope decisions
- MFA bypass or device compromise assessment
- Employee communication and awareness
- Email filtering gap remediation

Sources: NIST SP 800-61 Rev 2 (Computer Security Incident Handling Guide), NIST SP 800-84 (Testing Exercises). Anchor Cyber Security LLC.

exit 0