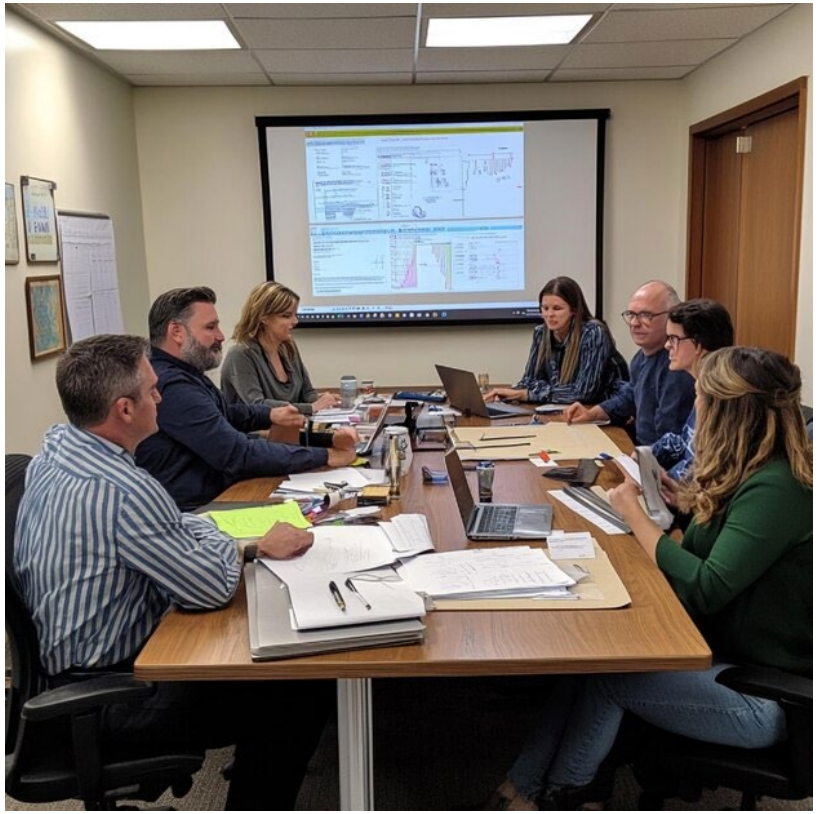
RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK RESPONSE PLANNING

This module is an overview on developing a high maturity risk response plan



INCIDENT RESPONSE PLANNING

- Operational backbone for containing, mitigating, and recovering from disruptive events
  - IRP is not a static document
  - It is a living, continuously exercised capability that blends technical execution, decision-making discipline, organizational coordination, and regulatory alignment
- A well-designed IRP ensures that when an incident occurs
  - Even under conditions of stress and uncertainty
    - Teams respond with speed, clarity, and coherence
    - High-maturity incident response minimizes damage, reduces recovery time, and prevents recurrence

STRATEGY COMPONENTS

- Threat scenario catalogs
  - Enumerate and characterize probable or high-impact incident types
  - Unlike generic threat lists, scenario catalogs are contextualized to the organization’s technology stack, business model, and regulatory exposure
  - Examples
    - Cyber: Ransomware, credential theft, insider exfiltration, command-and-control activity
    - Operational: Storage array collapse, message-queue saturation, orchestration failure
    - Cloud: Region outages, IAM misconfiguration, API rate limit exhaustion
    - Data integrity: Corrupted datasets, failed ETL pipelines, unauthorized data manipulation
    - Third-party: SaaS outage, vendor breach, supply-chain compromise

STRATEGY COMPONENTS

- Threat scenario catalogs
  - Each scenario includes
    - Likelihood
    - Affected assets
    - Early warning KRIs
    - Containment strategies
    - Escalation requirements
    - Expected recovery pathways

STRATEGY COMPONENTS

- Impact pathways
  - Describe how an incident propagates across systems and business services
    - Enables responders to anticipate secondary and tertiary effects
  - Example:
    - A credential compromise → privileged escalation → database exfiltration → downtime → customer impact → regulatory exposure
  - Mapping these pathways supports
    - Prioritized containment
    - Isolation strategies
    - More accurate business impact forecasting
    - Better-tuned KRIs and escalation triggers

STRATEGY COMPONENTS

- Decision trees (contain, isolate, failover)
  - Decision trees guide responders through branching choices based on observed conditions
  - Use cases
    - Contain: Quarantine compromised endpoints, revoke tokens
    - Isolate: Remove components from the network, segment traffic
    - Failover: Trigger DR site activation, route traffic to secondary cluster
  - Decision trees reduce decision fatigue and ensure consistent, policy-aligned responses
  - They document SOP decision making logic

STRATEGY COMPONENTS

- Communication matrices
  - A communication matrix defines who communicates what, to whom, when, and through which channels
  - Includes
    - Incident Commander notifications
    - Legal/compliance updates for regulated events
    - Executive escalations
    - Customer and external stakeholder communications
    - Media responses (rare but essential in severe events)
  - Communication matrices prevent
    - Conflicting messages
    - Delays in decision-making
    - Regulatory non-compliance

STRATEGY COMPONENTS

- Runbooks and playbooks
  - Runbooks capture low-level technical steps
  - Playbooks capture higher-level sequences and decision logic
  - Example playbooks
    - “Suspicious Privilege Escalation”
    - “Ransomware Detected”
    - “Container Node Failure”
    - “Data Integrity Compromise”

STRATEGY COMPONENTS

- Runbooks and playbooks
  - Example runbook steps
    - Revoke temporary IAM tokens
    - Snapshot affected volumes
    - Apply firewall rule
    - Trigger automated SOAR routine
  - Runbooks and playbooks together ensure repeatability, automation, and operational consistency

STRATEGY COMPONENTS

- Clearly defined coordination roles
  - Incident commander
    - Owns the operational response
    - Approves containment and eradication actions
    - Manages cross-team coordination
  - Communications lead
    - Handles internal and external messaging
    - Keeps executives and regulators informed
    - Aligns communications with legal standards
  - Technical lead
    - Directs hands-on technical staff
    - Manages investigation and triage
    - Coordinates with SMEs across teams
  - Clear role definition eliminates confusion during crises and ensures unity of effort

STRATEGY COMPONENTS

- RACI Tables
  - RACI (Responsible, Accountable, Consulted, Informed) ensures that:
  - Responsibility boundaries are explicit
  - Decision-makers are identified
  - No task is “owned by nobody” under pressure
  - Stakeholders receive the right level of communication
  - RACI modeling is essential for minimizing coordination failures.

SCENARIO-BASED IRP DEVELOPMENT

- Scenario-driven planning
  - Cstomizes response strategies to different categories of incidents
  - Not all incidents behave the same, and responses must be tailored accordingly
- Cybersecurity incidents
  - Examples: malware infections, credential compromise, DDoS attacks
  - Considerations
    - Evidence preservation for forensics
    - Threat intelligence integration
    - Regulatory reporting for breaches
    - Eradication without losing root cause evidence

SCENARIO-BASED IRP DEVELOPMENT

- Infrastructure failures
  - Examples: database corruption, storage failures, orchestration system collapse
  - Considerations
    - Rapid failover and redundancy
    - Data recovery from validated snapshots
    - Architectural review to prevent recurrence
- Cloud provider disruptions
  - Examples: cloud region outage, IAM misconfiguration, API throttling
  - Considerations
    - Multi-region failover
    - Automated infrastructure rehydration
    - Dependency mapping for distributed systems
    - CSP (Cloud Service Provider) SLAs and escalation

SCENARIO-BASED IRP DEVELOPMENT

- Data integrity events
  - Examples: corrupted ETL pipelines, unauthorized changes to datasets
  - Considerations
    - Isolation of suspect pipelines
    - Identification of “last known good state”
    - High-trust restore procedures
    - Validation before services resume
- Third-party outages
  - Examples: SaaS provider downtime, vendor breach
  - Considerations
    - Contractual obligations + SLA enforcement
    - Rapid invocation of contingency vendors
    - Risk acceptance vs. operational workaround decisions
    - Monitoring of vendor-provided status and updates
  - Scenario-based strategies improve response precision and reduce recovery times

HIGH-MATURITY IR PLAN

- Cross-functional rehearsal (tabletop + live-fire)
  - Tabletop exercises (TTX)
    - Execs, engineers, risk teams walk through scenarios to evaluate decision-making
  - Live-fire exercises
    - Simulated attacks or controlled faults (e.g., chaos engineering) test real operational resilience
  - Benefits
    - Builds reflexes
    - Identifies blind spots
    - Strengthens team coordination
    - Validates playbooks and automation

HIGH-MATURITY IR PLAN

- Automated playbooks for rapid initial actions
  - SOAR platforms execute
    - Log enrichment
    - Endpoint isolation
    - Credential revocation
    - Firewall rule deployment
    - Suspicious user lockouts
    - Triage information gathering
  - Automation reduces MTTD and MTTR, especially in high-volume environments

HIGH-MATURITY IR PLAN

- Decision checkpoints with predefined criteria
  - Checkpoints ensure escalation and containment decisions are made consistently and timely
  - Examples
    - "If containment efforts fail after 10 minutes → escalate to Incident Commander."
    - "If data integrity is uncertain → failover to last known good snapshot."
  - Checkpoints reduce inconsistency and avoid unnecessary delays

HIGH-MATURITY IR PLAN

- Regulatory alignment (NIST, ISO 27035, FFIEC)
  - High-maturity IR plans align to recognized frameworks
    - NIST SP 800-61 (Computer Security Incident Handling Guide)
    - NIST CSF – Respond & Recover domains
    - ISO 27035 (Information Security Incident Management)
    - FFIEC guidance for financial operations resilience
  - Alignment ensures
    - Compliance
    - Audit readiness
    - Consistency with industry norms

HIGH-MATURITY IR PLAN

- Integration with GRC systems
  - IR integrates with GRC platforms for
    - Incident documentation
    - Root cause analysis tracking
    - Evidence management
    - Remediation monitoring
    - Lessons learned ingestion
    - Automated risk register updates
  - This creates a closed-loop incident-to-risk feedback mechanism

INCIDENT LIFECYCLE

- NIST/ISO incident lifecycle
  - Gold standard for incident handling across cybersecurity, IT operations, and organizational resilience
    - Continuous, adaptive loop, not a linear sequence
    - Each phase builds the capability to respond faster, more effectively, and with greater precision
    - Ensures that incidents are handled systematically, from preparation and detection, through containment and recovery, to lessons learned and strategic improvements
  - Phases
    - Preparation
    - Detection and Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Review

PREPARATION

- Build tools, access pathways, and communication channels
  - Incident responders require rapid access to
    - SIEM dashboards
    - Cloud consoles
    - Endpoint detection systems
    - Ticketing and GRC platforms
    - Forensic tools (memory analysis, log extractors)
    - Network segmentation and firewall controls
    - Identity management portals

PREPARATION

- Build tools, access pathways, and communication channels
- Preparation includes
  - Pre-loading required tools on secured laptops
  - Ensuring responders have elevated just-in-time access
  - Establishing dedicated communication channels
    - For example: “War Room” Slack/Teams channels, secure voice bridges

PREPARATION

- Define playbooks and escalation paths
  - Playbooks define what actions to take
    - Escalation paths define who must take them and when
  - Elements include
    - Automated first-response actions
    - Technical and non-technical decision trees
    - Required notifications (legal, compliance, PR, regulators)
    - Trigger points for escalating severity levels

PREPARATION

- Conduct simulation exercises
  - Simulation builds muscle memory and identifies gaps
  - Types
    - Tabletop exercises (TTX) to execute scenario walkthroughs
    - Blue team drills to perform defensive validation
    - Red team engagements to perform adversarial testing
    - Purple team exercises for joint attack/defense improvement
    - Chaos engineering to assess controlled faults in distributed systems

DETECTION AND ANALYSIS

- Pre-authorize emergency actions
  - Responders often cannot take urgent actions like shutting down a compromised node without approvals
- Preparation includes
  - Pre-authorizing critical actions during SEV-1 events
  - Creating exception procedures for emergency situations
  - Ensuring legal and compliance sign-off in advance
  - This prevents delays that could significantly expand the blast radius

DETECTION AND ANALYSIS

- Detect anomalies
  - Detection sources include
    - SIEM correlation rules for privilege escalation anomalies
    - IDS/IPS for network intrusion signatures
    - APM tools for latency spikes, microservice failures
    - Cloud logs (e.g., CloudTrail, Azure Activity Logs) for suspicious role changes
    - KRI breaches for alerts for early risk indicators
  - High-maturity environments blend
    - Signature-based detection
    - Behavioral analytics
    - Machine learning anomaly detection

DETECTION AND ANALYSIS

- Confirm and classify the incident
  - Before triggering full IR, responders validate
    - “Is this a real incident?”
    - “What severity should be assigned?”
    - “Which playbook applies?”
  - Classification decisions affect
    - Escalation paths
    - Communication requirements
    - Resource allocation

DETECTION AND ANALYSIS

- Assess scope, blast radius, and affected systems
  - Assessment includes
    - Identifying compromised or malfunctioning components
    - Determining lateral movement (in cyber contexts)
    - Understanding business service impacts
    - Estimating potential customer exposure
  - This step determines how far the incident has spread and what is at risk next

DETECTION AND ANALYSIS

- Perform high-level triage and evidence collection
  - Triaging involves
    - Capturing logs, memory, and system snapshots
    - Tagging affected systems for forensic review
    - Prioritizing immediate containment actions
    - Preserving evidence for legal/regulatory needs
  - Evidence accuracy is crucial
    - Poor collection can jeopardize investigations or compliance

CONTAINMENT

- Focuses on preventing further damage and enabling root-cause investigation
- Short-term containment
  - Immediate actions that stabilize the environment
    - Lock or disable compromised accounts
    - Isolate infected endpoints
    - Block malicious IPs/domains at the firewall
    - Throttle or disable affected microservices
    - Cut off external data transfers
  - Short-term actions aim to stop the bleeding.

CONTAINMENT

- Long-term containment
  - Implemented once the situation stabilizes
    - Redirecting traffic to redundant instances
    - Applying temporary configuration changes
    - Deploying compensating controls
    - Creating segmented network zones
    - Implementing modified IAM policies
  - Long-term containment maintains functionality while teams prepare for eradication

ERADICATION

- Removes the root cause
  - Ensures the environment is free from malicious artifacts or corrupted components
- Key eradication activities
  - Remove malware or persistence mechanisms
    - Delete malicious binaries
    - Remove scheduled tasks, cron jobs, startup scripts
    - Neutralize command-and-control channels
  - Patch exploited vulnerabilities
    - Apply vendor patches or hotfixes
    - Update IAM roles and permissions
    - Close misconfigured ports or unnecessary services
    - This stops adversaries from re-exploiting the same path

ERADICATION

- Disable malicious identities or processes
  - Rotating passwords and keys
  - Revoking OAuth or API tokens
  - Terminating rogue sessions
  - Disabling compromised service accounts
- Eradication focuses on permanent removal of the threat, not just temporary containment

RECOVERY

- Recovery restores full service and returns systems to a trusted operational state
- Key recovery activities
  - Restore services from backups or replicas
    - Utilize DR replicas, snapshots, or multi-region failover
    - Recover corrupted datasets from known-good backups
    - Restart affected services in clean environments

RECOVERY

- Key recovery activities
  - Validate data integrity
  - Critical for
    - Financial transactions
    - Healthcare records
    - Customer-facing data
    - Security logs used for investigations
  - Validation techniques
    - Checksums
    - Hash comparisons
    - Database consistency checks
    - Business-level reconciliation (e.g., transaction matching)

RECOVERY

- Key recovery activities
  - Enhance monitoring post-recovery
  - Immediately after restoration, organizations increase monitoring to detect
    - Reinfection attempts
    - Post-recovery performance degradation
    - Recurrence of suspicious patterns
  - This “hyper-care” phase ensures that recovery is stable and secure

POST-INCIDENT REVIEW

- Post-incident review (PIR)
  - Transforms incidents into institutional learning opportunities
  - Strengthens long-term resilience
- Identify control failures and systemic weaknesses
  - PIR evaluates
    - Which controls failed or were bypassed
    - Whether escalation was timely
    - Whether automation executed correctly
    - Which organizational gaps slowed response

POST-INCIDENT REVIEW

- Update KRIs, controls, and response plans
  - Outcomes may include
    - Adding new KRIs
    - Adjusting KRI thresholds
    - Strengthening technical controls
    - Revising playbooks
    - Improving communication workflows
  - This ensures the IR program evolves with new insights

POST-INCIDENT REVIEW

- Document the event for compliance and governance
  - Documentation includes
    - Timeline of events
    - Decisions made and rationale
    - Root cause analysis
    - Evidence collected
    - Lessons learned
    - Regulatory notifications made
  - Regulators, auditors, and executive committees require traceability

POST-INCIDENT REVIEW

- Feed insights into future resilience and risk mitigation
  - Outputs integrate into
    - GRC systems
    - Risk registers
    - Strategic risk mitigation plans
    - Training programs
    - Architecture improvements
  - The goal is continuous improvement and prevention of recurrence

Q&A AND OPEN DISCUSSION