RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

SOPS

This section is an introduction to SOPS

- Standard Operating Procedures

SOP

- Standard Operating Procedure
  - Documented, step-by-step set of instructions that describes how to perform specific operational tasks consistently and safely
    - Translates policy and controls into repeatable actions
- In ISACA terms
  - *"A detailed, written instruction to achieve uniformity of the performance of a specific function"*
- For resilience
  - *"A predefined procedure ensuring continuity of critical operations during normal and abnormal conditions"*

SOP

Framework	Role of SOPs	Key Emphasis
ISACA (COBIT / Risk IT / ITAF)	SOPs operationalize **controls** and ensure **governance objectives** are executed consistently. They provide evidence for audit and control assurance.	Control performance, accountability, repeatability
DRI (Professional Practices)	SOPs are core artifacts for **continuity, recovery, and response**. They describe how to restore critical services and maintain resilience during incidents.	Preparedness, operational continuity, resilience assurance
CERT-RMM	SOPs contribute to **process institutionalization**, embedding resilience activities in daily operations.	Process standardization and maturity
ISO 22301 (Business Continuity)	SOPs support the implementation of business continuity and incident response plans.	Documented procedures, version control, periodic review

In short:

→ In ISACA, SOPs = control execution.

→ In DRI, SOPs = resilience in action.

KEY CHARACTERISTICS

Characteristic	Description
Clear and Concise	Uses precise, unambiguous language with defined terms.
Consistent and Repeatable	Produces the same results regardless of who executes it.
Aligned with Policy	Reflects the organization's governance, security, and compliance policies.
Role-Specific	Defines responsibilities and required competencies.
Tested and Validated	Verified through drills, audits, or walkthroughs.
Accessible and Controlled	Easily available to authorized personnel, protected from unauthorized change.
Version-Controlled	Updated regularly with date, version, and approval metadata.
Action-Oriented	Focuses on what to do, how to do it, and in what sequence.
Linked to Metrics	Allows performance monitoring (e.g., time to complete, error rate).
Resilient	Accounts for contingencies and alternate actions in failure scenarios.

SOP EXAMPLES

Domain	SOP Example	Purpose / Description
IT Operations	System Backup and Restore SOP	Defines how to perform regular backups and restore data in the event of corruption or loss.
Incident Response	Cybersecurity Incident Escalation SOP	Outlines how to detect, report, and escalate a suspected security breach.
Business Continuity	Alternate Site Activation SOP	Details how to activate an alternate data center or office in case of outage.
Change Management	Software Deployment SOP	Specifies pre-deployment checks, approvals, rollback steps, and documentation.
Compliance & Audit	Evidence Collection SOP	Defines how audit evidence is gathered, stored, and verified.
Human Resources / Resilience	Emergency Communication SOP	Lists escalation paths and contact hierarchies for crisis communication.
Physical Security	Data Center Access SOP	Establishes procedures for authorized entry and verification.

SOP DEVELOPMENT

- Development
  - Identify the need
  - Triggered by a policy requirement, risk finding, incident, or new control
- Define scope and objectives
  - What task does the SOP cover?
  - What outcome is expected?
- Gather input from SMEs (subject matter experts)
  - Collaborate with process owners, security, operations, and compliance teams
- Draft the SOP
  - Step-by-step instructions, tools, roles, timing, contingencies

SOP DEVELOPMENT

- Review and validate
  - Cross-check accuracy; test through simulations or tabletop exercises
- Obtain approval
  - Formal sign-off from process owner and governance body
- Publish and train
  - Distribute to relevant personnel; ensure accessibility and training

SOP USAGE

- SOPs are used during:
  - Routine operations (e.g., daily monitoring, backups)
  - Incident response (reference during a crisis)
  - Audit or compliance checks (evidence of control performance)
  - Training (onboarding new staff)
  - Identify control weaknesses or gaps
    - Compare current controls to framework expectations or regulatory standards
  - Determine if gaps arise from low maturity (e.g., no ownership, no automation, poor testing)

SOP MAINTENANCE

- Periodic review (quarterly/annual):
  - Ensure procedures remain valid
- Change control
  - Updates must follow formal versioning and approval workflows
- Testing
  - Verify SOP effectiveness through drills or real-world incidents
- Archiving
  - Retain old versions for audit traceability

GOVERNANCE AND REGULATORY ISSUES

Governance / Regulatory Framework	SOP Requirement / Expectation
ISACA COBIT 2019 / ITAF	SOPs demonstrate control implementation and audit evidence for governance objectives.
SOX (Sarbanes–Oxley)	Requires documentation of control activities — SOPs often serve as that documentation.
ISO 22301	Mandates documented business continuity and recovery procedures.
NIST SP 800-61 / 800-34	Require documented incident response and contingency procedures.
DRI Professional Practices 4–6	Require documented response, continuity, and recovery plans — all underpinned by SOPs.
FFIEC / Basel III (Banking)	Mandate operational risk management documentation for key processes.

Regulatory takeaway:
Incomplete, outdated, or untested SOPs can constitute **control deficiencies** under audit or compliance reviews.

BEST PRACTICES

- Link SOPs to policies and risks
  - Every SOP should trace back to a policy statement or control objective
- Keep it simple and usable
  - Avoid dense text
  - Use checklists, flowcharts, and tables
- Use version control and approval logs
  - Record authors, reviewers, dates, and approvals for audit evidence
- Integrate SOPs into training and drills
  - Test and rehearse them to optimize effectiveness

BEST PRACTICES

- Align SOPs with process maturity
  - As processes evolve, SOPs must be revised accordingly
- Digitize and centralize SOPs
  - Store in secure document management or GRC systems with access controls
- Review after every major incident
  - Feed lessons learned back into the SOP (continuous improvement)
- Ensure cross-functional ownership
  - SOPs should reflect operations, risk, IT, and compliance collaboration

SOPS AND PROCESS MATURITY

Process Maturity Level	SOP Characteristics
Level 1 – Ad Hoc	SOPs are informal or nonexistent; actions depend on individual knowledge.
Level 2 – Repeatable	SOPs exist but are not standardized or enforced organization-wide.
Level 3 – Defined	SOPs are documented, standardized, and regularly reviewed.
Level 4 – Managed	SOPs are measured for compliance, effectiveness, and cycle time.
Level 5 – Optimized	SOPs are continuously improved, automated, and aligned to resilience metrics.

As organizations mature, SOPs shift from static documentation to **living control instruments**, integrated with governance tools (e.g., GRC, workflow automation, dashboards).

EXAMPLES OF SOPS BY FUNCTION

Function	SOP Example	Notes on Control Alignment
Cybersecurity	Security Patch Management SOP	Preventive control — ensures timely updates and vulnerability reduction.
Disaster Recovery	Data Center Failover Activation SOP	Corrective control — defines recovery procedures and testing intervals.
Monitoring and Detection	Log Analysis and Escalation SOP	Detective control — defines alert thresholds and escalation rules.
Vendor Risk Management	Third-Party Assessment SOP	Preventive control — ensures due diligence and risk scoring.
Operational Continuity	Critical Function Recovery SOP	Corrective control — defines time objectives (RTO/RPO).
Change Management	Pre-Deployment Review SOP	Preventive control — ensures approvals and rollback procedures.

Q&A AND OPEN DISCUSSION