

TEN560

Disaster Recovery Audit Project Timeline

Customer planning guide for Ten560 led and self directed audits

Purpose

This guide helps your organization choose between a Ten560-led disaster recovery audit and a self-directed audit completed with the Ten560 toolkit. It shows the expected work, customer responsibilities, milestones, and conditions that commonly extend delivery. Final commitments are established only in an executed Statement of Work.

Planning Summary

Delivery Approach	Estimated Labor	Expected Calendar Time
Ten560-led audit	32 to 48 hours	2 to 3 calendar weeks
Self-directed audit	64 to 96 hours	4 to 6 calendar weeks
Delayed self-directed audit	Work varies	6 to 10 calendar weeks or longer

Why self-directed work takes longer. Ten560 begins with experience performing infrastructure reviews, interpreting technical evidence, interviewing stakeholders, and connecting individual findings to the larger recovery picture. Internal teams usually complete the audit alongside normal operational duties. Context switching, approvals, vendor responses, evidence gathering, and unfamiliar portions of the review commonly double both the labor required and the elapsed calendar time.

These ranges assume one primary location, fewer than 20 on-premises servers, a manageable cloud environment, available stakeholders, and no active incident or major remediation project.

Delivery Schedule

Workstream	Ten560-led Schedule	Self-directed Schedule
Project setup	Week 1: kickoff, scope, contacts, access, and testing boundaries	Weeks 1 to 2: assign owners, confirm scope, gather access, and schedule work
Interviews	Weeks 1 to 2: leadership, department, facilities, and technical interviews	Weeks 2 to 4: schedule and complete interviews around normal workloads
Site and technology review	Weeks 1 to 2: on-site inspection and technical evidence collection	Weeks 2 to 5: inspect facilities, systems, cloud services, identity, and dependencies
Recovery validation	Weeks 2 to 3: backup evidence review and representative restore testing	Weeks 3 to 6: obtain approvals, prepare safe tests, execute restores, and document results
Hazard research	Weeks 1 to 2: public-source research and evidence verification	Weeks 2 to 5: research, document sources, and validate planning assumptions
Analysis and reporting	Weeks 2 to 3: analyze findings, prepare report, and conduct executive briefing	Weeks 5 to 8: reconcile evidence, score findings, write recommendations, and obtain review

Milestones

Milestone	Ten560-led Target	Self-directed Target
Scope and owners confirmed	Business Day 1	Business Days 1 to 2
Initial evidence assembled	Business Days 1 to 3	Business Days 2 to 6
Interviews completed	Business Days 2 to 5	Business Days 4 to 10
Technical review completed	Business Days 5 to 8	Business Days 10 to 16
Restore testing completed	Business Days 6 to 10	Business Days 12 to 20
Draft findings reviewed	Business Days 10 to 13	Business Days 20 to 26
Final report completed	Business Days 12 to 15	Business Days 24 to 30

Estimated Labor by Phase

Self-directed estimates are exactly twice the corresponding Ten560-led estimates for planning purposes.

Audit Phase	Ten560-led	Self-directed
Pre-engagement planning and document request	2 to 3 hours	4 to 6 hours
Kickoff and management interviews	2 to 4 hours	4 to 8 hours
Department and business-impact interviews	3 to 6 hours	6 to 12 hours
On-site facility and technology inspection	4 to 6 hours	8 to 12 hours
Server, network, cloud, identity, and dependency review	4 to 7 hours	8 to 14 hours
Backup configuration and evidence review	3 to 5 hours	6 to 10 hours
Representative restore testing	3 to 6 hours	6 to 12 hours
FEMA and other public-source hazard research	2 to 4 hours	4 to 8 hours
Security and malicious-event preparedness review	2 to 4 hours	4 to 8 hours
Findings analysis, scoring, and recommendations	3 to 5 hours	6 to 10 hours
Final report preparation	5 to 8 hours	10 to 16 hours
Executive presentation and factual corrections	2 to 3 hours	4 to 6 hours

Individual phase maximums should not be added to create a guaranteed project total. Some activities overlap, while missing documentation, failed restore tests, additional locations, or unexpected complexity may add work outside the baseline.

What Each Approach Includes

Ten560-led Audit	Self-directed Audit
Ten560 manages the audit sequence, interviews, evidence register, public-source research, technical review, authorized testing, analysis, and report production.	Your organization assigns an internal audit lead and performs the same activities using the purchased workbook and field guide.
Ten560 distinguishes verified facts, stakeholder statements, planning assumptions, and unknowns.	The internal audit lead must apply the same evidence discipline and avoid treating undocumented statements as verified controls.
Ten560 presents prioritized findings and unresolved dependencies to leadership.	The internal team prepares its findings, obtains leadership review, and assigns owners and deadlines.

Customer Responsibilities

- Assign an executive sponsor and one primary technical contact.
- Provide timely access to systems, consoles, documentation, contracts, facilities, and relevant vendors.
- Schedule leadership, department, facilities, and technical participants.
- Approve the systems, data, timing, and safety boundaries for representative restore testing.
- Provide an isolated destination or another approved method for recovery testing.
- Review factual findings promptly and retain responsibility for business priorities and acceptance of risk.

Conditions That Extend the Schedule

Condition	Likely Effect	Required Response
Missing or inaccurate documentation	Adds discovery and validation time	Document the gap and approve additional discovery
Credentials or vendor access unavailable	Stops the affected review	Escalate access or reschedule the task
Backup failures or corrupt recovery points	Adds investigation and retesting	Separate remediation from audit validation
Large data sets or slow recovery infrastructure	Extends restore-test windows	Adjust the sample, window, or scope
Multiple sites, tenants, or business units	Adds interviews and evidence	Revise scope, schedule, and fees where applicable
Safety or production risk	Prevents planned testing	Use an approved alternative or document the limitation
Delayed customer responses	Moves the delivery date	Reset milestones to reflect the dependency
Material incident discovered	May pause the audit	Authorize incident-response work separately

Scope Changes

The following items require written agreement before they are added to a Ten560-led engagement and may materially extend a self-directed project:

- Additional physical locations or materially separate recovery environments.
- More than 20 on-premises servers or an unexpectedly complex cloud estate.
- Restore tests beyond the agreed representative sample.
- Remediation, implementation, incident response, or recovery execution.
- Detailed recovery runbooks, employee training, or facilitated tabletop exercises unless specifically included.
- Regulatory, legal, engineering, life-safety, or insurance opinions outside the technical audit scope.

Completion Criteria

Work Area	Complete When
Evidence collection	Material requested evidence is received, or its absence is documented as a finding.
Interviews	Required roles are interviewed, or their unavailability is documented.
Testing	Authorized tests are completed and results or limitations are recorded.
Research	Public-source evidence, source dates, assumptions, and limitations are recorded.
Report	Findings are risk-ranked and linked to supporting evidence.
Closeout	Leadership review is completed and factual corrections are incorporated.

Important Planning Boundaries

A completed audit identifies readiness gaps and supports decision-making; it does not guarantee recovery, certify compliance, replace emergency or life-safety planning, or provide legal, engineering, or insurance advice. Remediation and implementation are separate work.

For a Ten560-led audit, the executed MSA and SOW control scope, schedule, fees, prepayment, travel expenses, responsibilities, and deliverables. For a self-directed audit, your organization controls the schedule and remains responsible for the accuracy of evidence, safety of testing, conclusions, and corrective actions.

Planning Decision

Choose Ten560-led When	Choose Self-directed When
Leadership wants an independent assessment and a defined delivery schedule.	The organization has capable internal staff and can protect sufficient time for the work.
The internal team lacks time, audit experience, or independence.	The organization accepts a longer schedule and will manage evidence quality internally.
Restore testing, stakeholder coordination, and executive reporting need experienced facilitation.	Budget is more constrained than internal capacity, and leadership will enforce accountability.