01 / PREVENTION AND DETECTION

Ransomware Readiness Guide

A practical guide to prevention, protected backups, tested recovery, and business continuity for business leaders and IT teams.

If a critical system went offline today, could your team restore trusted access and resume essential work? Use this guide to identify gaps, assign owners, and focus your next review.

Start with the systems that matter most

Inventory firewalls, VPN gateways, identity systems, servers, storage, backup platforms, virtualization hosts, and core network devices. Record owners, support status, exposure, critical data, vulnerabilities, controls, and dependencies. Prioritize by business impact and likelihood, then assess the risk remaining after controls.

Review your core defenses

- ☐ **Secure access.** Use multifactor authentication, limit privileged access, and review remote access paths.
- ☐ **Patch exposed systems.** Prioritize internet-facing devices and applicable vulnerabilities in CISA’s Known Exploited Vulnerabilities Catalog.
- ☐ **Verify active protection.** Confirm endpoint protection and firewall security services are licensed, enabled, current, and monitored.
- ☐ **Look beyond signatures.** Evaluate behavior-based protection and endpoint detection and response (EDR); consider XDR and SIEM based on your environment.
- ☐ **Assign response ownership.** Define who reviews alerts, escalates incidents, and approves automated containment actions.

Keep updates and patches separate

Automatic signatures, reputation feeds, and threat intelligence updates improve detection. They do not fix software vulnerabilities. Apply firmware, operating system, and application patches through a controlled process, then verify completion.

Use the checkboxes to guide discussion. Mark an item complete only when the responsible owner can show supporting evidence.

02 / BACKUP PROTECTION

Protect your recovery options

A backup is useful only if it survives the incident and can restore clean, usable systems and data.

Build from the 3-2-1 baseline

Three copies of data. Two media types or independent storage systems. One copy offsite. Add at least one offline or appropriately configured immutable copy. Protect backup credentials separately and restrict access to consoles, encryption keys, retention policies, and deletion controls.

Synchronization and replication can carry malicious changes into another location. Keep historical recovery points, monitor failed jobs, and verify clean data before restoration. Maintain trusted installation images and offline recovery instructions.

Ask these questions before choosing cloud protection

Planning area	Microsoft Azure	Amazon Web Services
Backup service	Azure Backup for supported workloads	AWS Backup for supported workloads
Deletion resistance	Evaluate immutable vaults, soft delete, and multi-user authorization	Evaluate Vault Lock and logically air-gapped vaults
Disaster recovery	Azure Site Recovery for supported replication and failover needs	AWS Elastic Disaster Recovery for supported recovery needs
Administrative isolation	Separate roles and restrict vault access; evaluate recovery region	Separate accounts and restrict IAM; evaluate cross-region copies

Features depend on workload, region, service configuration, and retention settings. A logically air-gapped cloud vault is not a physically offline copy. Validate support, bandwidth, recovery time, licensing, and cost before selecting a design.

Test the full restore process

- ☐ Recover both individual files and a complete application or server, including dependencies.
- ☐ Document elapsed recovery time, the restored recovery point, data validation, and any failures.
- ☐ Have security personnel validate results. Assign corrective actions and retest when needed.

03 / RECOVERY AND CONTINUITY

Plan your recovery

Complete this worksheet with business owners and IT. Targets need management approval, a funded design, and test results that show whether they can be met.

Recovery time objective (RTO): Maximum acceptable time to restore a business service.
Recovery point objective (RPO): Maximum acceptable data loss, measured in time.

Recovery planning worksheet

Service and owner	RTO target	RPO target	Dependencies and last restore test
Identity / authentication Owner: _____	_____	_____	_____ _____
Core business application Owner: _____	_____	_____	_____ _____
Shared files / sensitive data Owner: _____	_____	_____	_____ _____
Other critical service Owner: _____	_____	_____	_____ _____

Service names are prompts, not a prescribed restoration sequence. Determine the order from your own dependencies. Blank targets must be defined and validated; this worksheet makes no recovery-time promise.

Make the plan usable during an outage

- ☐ Keep emergency contacts, escalation paths, and recovery instructions available offline.
- ☐ Define who can declare an incident, coordinate containment, preserve evidence, and authorize restoration.
- ☐ Plan temporary business workarounds and communications if email or identity services are unavailable.
- ☐ Rehearse the response and restore only into an environment your response team has validated.

Choose one immediate action

Our most important gap: _____

Accountable owner: _____ Due date: _____

04 / ONGOING READINESS

Make readiness a routine

Use this suggested review schedule to keep controls, people, and recovery plans current. Adjust frequency to your risk, system changes, and response agreement.

Suggested cadence	Review and evidence
Daily or continuously	Review critical alerts and backup failures according to your response agreement. Escalate to a named owner.
Monthly	Report on patch and firmware status, subscription health, endpoint coverage, signature age, and unresolved exceptions.
Quarterly	Test file and full application or server recovery. Run phishing simulations; record outcomes and corrective actions.
Annually	Conduct technical security assessments and appropriately scoped penetration testing. Provide employee awareness and hands-on technical training.
After major changes	Recheck scope, asset dependencies, recovery targets, backup coverage, and incident response procedures.

These frequencies reflect CKSS's advisory recommendations and planning guidance. They are not universal CISA requirements. Keep up with vendor and CISA security advisories between scheduled reviews.

Turn unanswered questions into a plan

CKSecurity Solutions helps organizations evaluate security risk, plan cloud solutions, and strengthen security programs through advisory services and practical documentation resources. Discuss your environment and recovery needs with CKSS to identify the next steps that fit your organization.

Schedule a consultation
443.459.1589 | info@cksso.com
cksecuritysolutions.com

Sources and scope

Adapted from CKSS's Ransomware Prevention, Recovery & Business Continuity advisory dated October 24, 2026.

CISA and partners: #StopRansomware Guide
Microsoft Learn: Azure Backup overview
AWS: Logically air-gapped vaults

General educational guidance, October 2026. Tailor implementation to your systems and applicable obligations. This guide does not establish compliance, certify security, or guarantee prevention or recovery.