Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Governance and risk

- [ ] Name executive, IT, cybersecurity, privacy and business owners.
- [ ] Define decision rights, escalation thresholds and risk-acceptance authority.
- [ ] Create an integration risk register with owners and target dates.
- [ ] Classify issues as Day 1, short-term or longer-term priorities.
- [ ] Establish a reporting cadence for leadership and the board.
- [ ] Track inherited vulnerabilities and technical debt through a remediation plan.

Technology and application visibility

- [ ] Complete the application inventory before close when feasible.
- [ ] Inventory infrastructure, cloud platforms, applications and databases.
- [ ] Document each application's owner, cost, users, data and business purpose.
- [ ] Identify unsupported systems, shadow IT and undocumented integrations.
- [ ] Map critical systems, data flows and operational dependencies.
- [ ] Confirm administrators, vendors and key-person dependencies.
- [ ] Document contracts, renewal dates and life cycle status.

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Target operating model and platform conversion

- [ ] Define the combined organization's target technology architecture.
- [ ] Classify applications as retain, migrate, consolidate, replace or retire.
- [ ] Assign an owner and target date to each conversion decision.
- [ ] Identify systems affected by identity, domain and email changes.
- [ ] Develop migration, testing, rollback and decommissioning plans.
- [ ] Define temporary coexistence requirements and exit dates.
- [ ] Update support responsibilities, procedures and user training.
- [ ] Validate the target environment before retiring legacy systems.

Licensing and vendor optimization

- [ ] Inventory purchased, assigned, active and unused licenses.
- [ ] Identify overlapping and underused applications.
- [ ] Review renewal dates, minimum commitments and termination rights.
- [ ] Identify capabilities already included in enterprise agreements.
- [ ] Quantify temporary dual-licensing costs.
- [ ] Establish dates for cancelling redundant subscriptions.
- [ ] Confirm data-retention requirements before terminating platforms.
- [ ] Track expected savings and confirm that they are realized.

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Identity and access

- [ ] Inventory employee, contractor, administrator, service and vendor accounts.
- [ ] Disable dormant, former-employee and unnecessary accounts.
- [ ] Require multifactor authentication for remote and privileged access.
- [ ] Review privileged access and remove excessive permissions.
- [ ] Rotate administrative, service-account and sensitive credentials.
- [ ] Establish secure onboarding, transfer and termination procedures.
- [ ] Avoid broad trust until minimum security requirements are satisfied.

Social engineering and fraud

- [ ] Warn employees that phishing and impersonation risk increases during integration.
- [ ] Publish authorized integration, HR, finance and IT contacts.
- [ ] Independently verify payment and banking changes.
- [ ] Prohibit employees from sharing passwords or MFA codes.
- [ ] Verify unusual requests through a separate trusted channel.
- [ ] Prepare for executive impersonation, voice cloning and deepfakes.
- [ ] Test phishing, help-desk impersonation and payment-fraud scenarios.

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Data protection and migration

- [ ] Inventory and classify sensitive and regulated data.
- [ ] Confirm authorization to combine, transfer and retain the data.
- [ ] Encrypt data in transit and at rest.
- [ ] Restrict and monitor migration-team access.
- [ ] Validate data completeness, accuracy and permissions after migration.
- [ ] Maintain tested backups and rollback plans.
- [ ] Remove residual data from retired systems and temporary storage.

Compliance and regulatory obligations (1 of 2)

- [ ] Identify all applicable laws, regulations, industry standards and contractual security requirements.
- [ ] Map each obligation to the relevant legal entity, business process, data type, system, location and owner.
- [ ] Obtain current assessments, attestations, certifications, audit reports, regulator correspondence and open findings.
- [ ] Identify required reporting, renewal, examination and notification dates that occur during integration.
- [ ] Determine whether the transaction or change of control requires notice, consent, reassessment or contract amendment.

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Compliance and regulatory obligations (2 of 2)

- [ ] Define PCI DSS scope, payment channels, service providers and compliance-validation responsibilities where applicable.
- [ ] Identify covered defense contracts, FCI, CUI, required CMMC level and in-scope systems where applicable.
- [ ] Review HIPAA, GLBA, privacy, breach-notification and sector-specific obligations based on the acquired company's operations and data.
- [ ] Evaluate whether migrations, network connections, identity changes or vendor changes alter compliance scope.
- [ ] Preserve audit evidence, system diagrams, data-flow maps, risk acceptances and remediation records.
- [ ] Map inherited requirements to the target control environment and document control owners.
- [ ] Track compliance gaps, temporary exceptions and remediation milestones through stabilization.

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

Practical IT and cybersecurity integration risk checklist

Use this checklist to assign ownership, document decisions and track risk from pre-close through stabilization.

Third parties and incident readiness

- [ ] Inventory vendors with system or data access.
- [ ] Review security obligations, notification terms and audit rights.
- [ ] Remove unnecessary vendor access and rotate shared credentials.
- [ ] Align incident-response, legal, privacy, insurance and communication procedures.
- [ ] Confirm that required logs reach the designated monitoring platform.
- [ ] Monitor identities, endpoints, email, networks, cloud services and data transfers.
- [ ] Test ransomware recovery and conduct an integration-focused incident exercise.

How Wipfli can help

Wipfli brings together cybersecurity, technology, risk advisory and compliance capabilities to support organizations through every stage of integration — from pre-close assessment through stabilization.

Contact us to learn more

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.