Cybersecurity Risk Management Checklist

8 Jun 2026 / Jason Wayne

Complete

Score	7 / 10 (70%)	Flagged items	1	Actions	0

Name of inspector	Jason Wayne
Position / role of inspector	Senior IT Officer
Date of inspection	08.06.2026
Location	140 Nassau St, New York, NY 10038, USA (40.7112912, -74.0062811)
Assessment cycle / period	
Department or business unit	Sales
Supervisor / CISO name	Tyler Cho

The next sections contain the risk registers. Work through sections in order. For each asset, complete one row per identified threat. Do not leave rows blank.

Likelihood and impact are each rated 1 (rare / negligible) to 5 (near-certain / catastrophic).

Manually multiply likelihood and impact scores to get the risk score: 15–25 critical; 10–14 high; 5–9 medium; 1–4 low.

For any risk scored medium (5) or above, a treatment decision, owner, and due date are crucial to note down before moving to the next asset.

Flagged items

1 flagged

Section 6: Compliance Framework Checks

Is every in-scope asset recorded with at least one identified threat and a completed risk score?

No

Need to conduct a more detailed cybersecurity risk assessment

Section 1: Hardware Assets

1 / 1 (100%)

	Asset / System	Threat Identified	Existing Controls	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Treatment Decision	Owner	Due Date	Notes
1	Employee laptops	Damage to existing laptops	Refresher course to handle laptops carefully	2	4	8	Mitigate			

Section 2: Software and SaaS Assets

1 / 1 (100%)

	Asset / System	Threat Identified	Existing Controls	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Treatment Decision	Owner	Due Date	Notes
1	Saas backup	Client data at risk in an outage	None	4	3	12	Transfer	Third party		

Section 3: Cloud Infrastructure and Hosted Services

0 / 1 (0%)

	Asset / System	Threat Identified	Existing Controls	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Treatment Decision	Owner	Due Date	Notes
1										

Section 4: Data Assets

1 / 1 (100%)

	Asset / System	Threat Identified	Existing Controls	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Treatment Decision	Owner	Due Date	Notes
1	Customer credentials	Hacking	Add protection measures	3	5	15	Mitigate	IT Manager	20.06.2026	

Section 5: Third-Party and Vendor Connections

0 / 1 (0%)

	Asset / System	Threat Identified	Existing Controls	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Treatment Decision	Owner	Due Date	Notes
1										

Section 6: Compliance Framework Checks

1 flagged, 4 / 5 (80%)

Complete this section after all asset sections are filled. These items confirm the register is complete and that this assessment's structure and outputs are consistent with the requirements of applicable compliance frameworks.

Completing this section does not certify compliance with any framework. Note that determination rests with an accredited auditor or certifying body. Mark N/A for any framework that does not apply to this organization.

Is every in-scope asset recorded with at least one identified threat and a completed risk score?	No
Need to conduct a more detailed cybersecurity risk assessment	
Is a treatment decision, owner, and due date recorded for every risk scored medium (5) or above?	Yes
Is the asset identification in this register structured in line with the NIST CSF 2.0 Identify function (ID.AM)?	N/A
Is the risk assessment methodology used in this register structured in line with NIST CSF 2.0 ID.RA and ISO/IEC 27005 (identification, analysis, evaluation, and treatment)?	Yes
Is the controls documentation in this register structured in line with the NIST CSF 2.0 Protect function (PR)?	Yes
Does this completed register produce documentation consistent with ISO/IEC 27001 audit evidence expectations, including risk register entries, treatment records, sign-off, and review timestamps?	N/A
Is the documentation of treatment actions for all PHI-related risks structured in line with HIPAA Security Rule risk analysis requirements? (Mark N/A if HIPAA does not apply)	N/A
Is the documentation of treatment actions for all cardholder data risks structured in line with PCI-DSS requirements? (Mark N/A if PCI-DSS does not apply)	N/A
Is the documentation of treatment actions for access controls, data loss prevention, and incident response structured in line with FINRA requirements? (Mark N/A if FINRA does not apply)	N/A
Is the next scheduled review date recorded and communicated to the relevant risk owner?	Yes

Completion Page

When this assessment is submitted, a timestamped record is automatically saved. Before signing, confirm that all rows are complete.

The completed register, including all scores and treatment records, serves as the primary evidence document supporting ISO/IEC 27001 and NIST CSF audit review.

Completing and submitting this register does not itself certify compliance with any framework.

Inspector sign-off

Jason Wayne
08.06.2026 15:35 PST

Supervisor / CISO sign-off

Tyler Cho
08.06.2026 15:35 PST