COMPUTER IMPRESSIONS · 2026

Legacy System Risk Scorecard

Quantify risk exposure across five categories to build a business case for modernization

LOW RISK | MODERATE RISK | HIGH RISK | CRITICAL RISK

How to Use This Scorecard

For each risk indicator, mark **YES** if this risk is currently present in your organization, **PARTIAL** if it exists but is being addressed, or **NO** if this risk is managed. **More YES answers = greater risk exposure.** Transfer your category counts to the Risk Summary, circle your risk level on the Heat Map, and complete the Business Case section to quantify the cost of inaction.

Executive Track Strategic risk indicators for CTO, CIO, and senior leadership — focused on business impact, operational exposure, and board-level risk.

Operational Track Technical risk indicators for IT Directors, Managers, and technical leads — focused on systems, processes, and implementation-level gaps.

1 Operational Fragility

Unplanned downtime, manual recovery, fragile deployments, and hidden dependencies

Mark YES for each risk that is currently present in your organization.

EXECUTIVE TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Critical business processes depend on systems that are poorly documented or understood by only a few people.				
We have experienced unplanned downtime or operational disruptions in the past 12 months.				
Recovery from a system failure requires manual intervention or specialized individual knowledge.				
Maintenance windows and change freezes are driven by system fragility — not business need.				
Leadership cannot get an accurate picture of system health without asking the technical team directly.				

OPERATIONAL TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Production systems lack automated monitoring or alerting for critical failure conditions.				

Risk Indicator	YES	PARTIAL	NO	Notes
We have no tested, documented recovery procedure for our most critical system.				
Configuration drift between environments creates unpredictable behavior in production.				
Emergency patches or hotfixes have been applied without proper testing or documentation.				
Incident resolution time has increased or stabilized at an unacceptable level over the past year.				
System interdependencies are undocumented and are discovered only when something breaks.				

2 Institutional Knowledge Risk

Bus-factor exposure, undocumented systems, and knowledge loss from departures

Mark YES for each risk that is currently present in your organization.

EXECUTIVE TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
The departure of one or two individuals would create a critical operational or technical crisis.				
We cannot onboard a new technical leader in a reasonable timeframe using existing documentation.				
Key vendor or system relationships are managed by individuals, not the organization.				
We have experienced operational disruption due to knowledge loss from a departure in the past three years.				

OPERATIONAL TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Critical systems have no runbooks, operating procedures, or troubleshooting guides.				
System configurations exist only in the minds of current staff — not in written documentation.				
Tribal knowledge about why systems were built the way they were is not captured anywhere.				

Risk Indicator	YES	PARTIAL	NO	Notes
New team members take significantly longer than expected to become productive with key systems.				
There is no formal process for capturing and transferring institutional knowledge when roles change.				
Documentation, when it exists, is outdated and not maintained on any regular schedule.				

3 Security & Compliance Exposure

Unpatched vulnerabilities, audit findings, access control gaps, and regulatory risk

Mark YES for each risk that is currently present in your organization.

EXECUTIVE TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Our legacy systems have known security vulnerabilities that have not been fully remediated.				
We have received audit findings related to technology controls in the past 24 months.				
We cannot demonstrate consistent compliance with current regulatory requirements across all systems.				
Cyber insurance renewal has required disclosure of legacy system risks or resulted in coverage limitations.				

OPERATIONAL TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Legacy systems are running end-of-life operating systems or unsupported software versions.				
Access controls in legacy systems cannot enforce least-privilege or role-based access.				
Audit logging is absent or incomplete in systems that handle sensitive or regulated data.				
Security patches have been deferred due to system fragility or compatibility concerns.				
Our incident response plan has not been tested against a realistic scenario in the past 12 months.				

Risk Indicator	YES	PARTIAL	NO	Notes
Data classification and access governance are not consistently applied across all legacy systems.				

4 Opportunity Cost

Delayed initiatives, reporting gaps, manual workarounds, and constrained development

Mark YES for each risk that is currently present in your organization.

EXECUTIVE TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Strategic initiatives have been delayed or cancelled because legacy systems could not support them.				
We are unable to provide the reporting and analytics that leadership or the board requires.				
Customer-facing limitations exist because our systems cannot support modern expectations.				
We are slower to respond to market opportunities than competitors with more modern infrastructure.				

OPERATIONAL TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Manual workarounds exist because legacy systems cannot be integrated with modern tooling.				
Data is regularly extracted, transformed, and loaded between systems through manual processes.				
New feature or capability requests are routinely blocked by legacy system constraints.				
Development velocity has declined due to the complexity and fragility of existing systems.				
More than 60% of IT effort is consumed by maintenance rather than new capability development.				
Technical debt backlogs have grown faster than the team can address them.				

5 Innovation Drag

Competitive disadvantage, talent friction, and inability to adopt modern capabilities

Mark YES for each risk that is currently present in your organization.

EXECUTIVE TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Competitors have deployed AI, automation, or analytics capabilities we cannot currently match.				
We have evaluated and declined technology opportunities because our infrastructure could not support them.				
Our technology constraints are visible to — or cited by — customers, partners, or prospective hires.				
Board or investor questions about technology modernization are difficult to answer with confidence.				

OPERATIONAL TRACK

Risk Indicator	YES	PARTIAL	NO	Notes
Modern integration patterns (APIs, event streams, microservices) are not feasible with current architecture.				
AI or machine learning workloads cannot be supported by current data infrastructure or compute.				
Our technology stack makes it difficult to attract and retain skilled technical staff.				
Vendor support for key system components is being sunset and no migration plan has been defined.				
The team lacks the tooling or process maturity to safely experiment with new technologies.				
Technical staff spend significant time working around system limitations rather than building new value.				

Risk Summary

Count your YES, PARTIAL, and NO responses per category, then use the totals to determine your overall risk level for each.

Risk Category	YES (risk present)	PARTIAL (in progress)	NO (managed)	Total Items	Risk Level (circle one)
1. Operational Fragility				11	Low / Moderate / High / Critical
2. Institutional Knowledge Risk				10	Low / Moderate / High / Critical
3. Security & Compliance Exposure				10	Low / Moderate / High / Critical
4. Opportunity Cost				10	Low / Moderate / High / Critical
5. Innovation Drag				10	Low / Moderate / High / Critical

Risk Heat Map

Circle the risk level for each category based on your YES count percentage.

RISK CATEGORY	LOW RISK 0–25% YES	MODERATE 26–50%	HIGH RISK 51–75%	CRITICAL 76–100%
Operational Fragility	○	○	○	○
Institutional Knowledge Risk	○	○	○	○
Security & Compliance Exposure	○	○	○	○
Opportunity Cost	○	○	○	○
Innovation Drag	○	○	○	○

Circle the risk level that matches your YES count for each category.

Risk Level Interpretation

Low Risk 0–25% YES	Your legacy systems present manageable risk at this stage. Maintain documentation standards, schedule regular security reviews, and monitor for emerging gaps. Consider a targeted modernization assessment to identify any hidden fragility.

Moderate Risk 26–50% YES	Risk exposure is accumulating across one or more categories. Left unaddressed, moderate risk typically becomes high risk within 12–24 months as systems age and staff turn over. A structured risk-sequenced modernization plan is the recommended next step.
High Risk 51–75% YES	Significant operational, security, and competitive risk is present. High-risk organizations typically underestimate total exposure by 30–50% before a formal assessment. Modernization planning should begin now — not after a triggering incident.
Critical Risk 76–100% YES	Critical fragility exists across multiple dimensions. The cost of continued inaction — through incidents, compliance findings, talent loss, and missed opportunities — typically exceeds the cost of modernization within 18 months. Executive escalation and immediate planning are warranted.

Business Case: Cost of Inaction

Use the estimates below to quantify what legacy system risk is costing your organization annually. Organizations that complete this exercise typically find the true cost of inaction is 30–50% higher than initial estimates. These figures build the financial case for presenting modernization as risk reduction — not optional investment.

Annual cost of unplanned downtime and emergency maintenance ($)	Estimated cost of a key knowledge holder departure ($)	Potential regulatory fine or breach exposure ($)	Annual opportunity cost: delayed or cancelled initiatives ($)
Your estimate	*Your estimate*	*Your estimate*	*Your estimate*

TOTAL ESTIMATED ANNUAL COST OF INACTION: $_____

Presenting This to Your Board or CFO

Frame it as risk reduction, not IT spending.	Legacy modernization eliminates quantifiable operational, security, and competitive risk. The question is not whether to spend — it is whether to spend now on planned modernization or later on incident recovery, compliance penalties, and emergency consulting.
Sequence by risk, not by cost.	Prioritize the highest-risk dependencies first. A risk-sequenced modernization plan delivers risk reduction from the first phase and avoids the "big bang" failure mode that gives modernization projects a bad reputation.
Show the compounding effect.	Legacy risk compounds over time as systems age, staff turn over, and regulations tighten. A board that defers modernization this year faces a larger, more expensive problem next year. The cost-of-inaction estimate above grows with each deferral.