Rob Bickel Agency · Managed Software Services

The Software Estate Risk Scorecard

A 34-point assessment of ownership, recoverability, security, lifecycle, cost, and AI across the applications your business runs on.

For COOs, CFOs, CIOs, and the people who keep the systems running

robbickel.com

2026 edition

In brief

Most assessments of business software stop at security. This one starts from ownership, because that is where the other risks come from. An application with an accountable owner tends to get patched, backed up, documented, and reviewed. An application without one tends to drift, however well it was built.

The scorecard has **34 items in six dimensions**. Each is scored 0, 1, or 2, and each is cross-referenced to the frameworks your auditors, insurers, and customers already use: NIST Cybersecurity Framework 2.0, CIS Critical Security Controls v8.1, ISO/IEC 27001:2022, ITIL 4, DORA and Google SRE practice, TOGAF, the NIST AI Risk Management Framework, and ISO/IEC 42001. The full crosswalk is in the appendix.

It takes about an hour with a business leader and the most technical person who knows your systems in the same room.

It produces a baseline, not a grade. The point is to know where you stand and what to fix first, then to measure progress against your own last score.

It highlights four critical items that deserve attention whatever your total.

How to use this scorecard

Choose the scope. Score either your whole software estate or a single business-critical application. If you are unsure where to start, score the application that would hurt most if it stopped working tomorrow: billing, order fulfilment, scheduling, or whatever your customers would notice first. Then score the next one.

Bring two perspectives. A business owner knows what the application must do and what it costs. A technical lead knows how it actually runs. Scoring together surfaces the gaps between those two views, and those gaps are often the most important finding.

Score honestly. Every item uses the same three levels:

0 · Absent. It does not exist, or nobody is sure.

1 · Exists, unproven. It exists, but is informal, incomplete, out of date, or has not been tested.

2 · Owned and proven. It exists, someone is accountable for it, and it has been tested or reviewed in the last 12 months.

“Nobody is sure” scores 0. Uncertainty is itself the finding.

About the bands. The score bands on the results page reflect professional judgment, not an empirically validated threshold. No published research supports a universal cut-off, and Gartner has argued in a research note titled “Technical Debt Benchmarks Are a Waste of Time” that comparisons against other companies mislead.[1] Use your score as a baseline and re-score every six to twelve months.

Dimension 1 · Ownership

Ownership is the foundation. The best evidence on key-person risk comes from open-source research: a 2016 study of 133 popular projects found that **65 percent depended on two or fewer people**,[2] and a study of 1,932 projects found that of those that lost their key developers, **only 41 percent survived, all because someone new took ownership**.[3] With a median tenure of **4.6 years in computer and mathematical occupations**,[4] most business applications will outlive their builders' time at the company.

TOGAF's starting artifact, the Application Portfolio Catalog, exists "to identify and maintain a list of all the applications in the enterprise."[5] Many mid-sized companies cannot produce one. That is where this dimension begins.

Item		Score
O1 ★	Every business-critical application has a named business owner and a named technical owner.	0 1 2
O2	A current inventory of applications, integrations, and scheduled jobs exists, ranked by business criticality.	0 1 2
O3	At least two people can change and deploy each critical application.	0 1 2
O4 ★	Admin accounts, domains, cloud billing, and code repositories are held by company accounts, not by individuals or contractors.	0 1 2
O5	Every supplier-built or supplier-run application has a written support and ownership agreement.	0 1 2

Dimension 2 · Operations and recoverability

This dimension separates applications that run from applications that are run. The strongest evidence concerns backups. In a Sophos study of 2,974 organizations hit by ransomware, attackers attempted to compromise backups in **94 percent** of attacks. Where backups were compromised, the **median recovery cost was $3 million, against $375,000** where they were not.[6] Veeam's 2025 research found that while 98 percent of organizations had a ransomware playbook, **only 44 percent included backup verification**.[7] Both are vendors that sell recovery products, but CISA's vendor-neutral guidance says the same: "Maintain offline, encrypted backups of critical data, and regularly test the availability and integrity of backups."[8]

One point is worth knowing. In the CIS Controls, testing data recovery (safeguard 11.5) sits in Implementation Group 2, above the baseline set that CIS calls essential cyber hygiene.[9] NIST CSF 2.0, by contrast, builds testing into the outcome itself: "Backups of data are created, protected, maintained, and **tested**."[10] Item R3 deliberately sets the higher bar.

For R6, DORA defines five software delivery measures, including change fail rate and failed deployment recovery time.[11] If nobody can say what they are for a critical application, that is an ownership finding.

Item		Score
R1	Automated backups run for each critical application and its data.	0 1 2
R2	Backups are protected, and an isolated or offline copy exists.	0 1 2
R3 ★	A restore has been tested in the last quarter, and the time it took is known.	0 1 2

Item		Score
R4	The application could be rebuilt from scratch using documented procedures or infrastructure-as-code.	0 1 2
R5	Monitoring alerts a named person, and each alert has a written runbook.	0 1 2
R6	The team can report change fail rate and failed-deployment recovery time.	0 1 2
R7	Changes are assessed, approved, and recorded, and configuration is managed.	0 1 2
R8	Recurring incidents get a root-cause review that leads to a change.	0 1 2

Dimension 3 · Security posture

The security items focus on the hygiene that ownership makes possible. Verizon's 2025 Data Breach Investigations Report, covering 12,195 confirmed breaches, found **credential abuse was the leading way in, at 22 percent** of breaches where the entry point was known, and **third-party involvement doubled to 30 percent**.[12] Its 2026 edition reports that the exploitation of vulnerabilities became the top initial access route, at 31 percent.[13] Sophos's 2025 ransomware study, whose sample is weighted toward mid-sized organizations of 100 to 5,000 employees, independently found **exploited vulnerabilities to be the most common root cause, at 32 percent**.[14]

Mid-sized companies are not too small to matter. The UK government's *Cyber Security Breaches Survey* found that **67 percent of medium-sized businesses** identified a breach or attack in the previous 12 months in its 2025 edition.[15]

Item		Score
S1	Multi-factor authentication protects every externally exposed application and all admin access.	0 1 2
S2	When someone leaves, their access, including API keys, tokens, and shared accounts, is revoked the same day.	0 1 2
S3	Secrets are kept out of source code, stored in a vault, and rotated.	0 1 2
S4	Vulnerability management covers application dependencies and libraries, not only servers and laptops.	0 1 2
S5	Suppliers are listed, ranked by criticality, and included in incident planning.	0 1 2

Dimension 4 · Lifecycle and supportability

Unsupported software is a baseline failure, not an advanced concern. CISA's catalogue of *Bad Practices* lists the use of unsupported or end-of-life software as dangerous for all organizations.[16] CIS safeguard 2.2, part of the essential-hygiene baseline, treats unsupported software as unauthorized unless there is a documented exception with mitigations.[17] NIST CSF 2.0 frames the outcome as "Software is maintained, replaced, and removed commensurate with risk."[10]

The open-source components inside applications age quietly. Black Duck's 2025 analysis of 965 commercial codebases, audited mostly during acquisitions, found **90 percent contained components more than four years out of date**.[18]

Item L4 brings in the TIME model, attributed to Gartner and widely used in application portfolio management: each application is classified as **Tolerate, Invest, Migrate, or Eliminate**, based on business value and technical fit.[19]

Item		Score
L1 ★	Every critical application's operating system, runtime, and framework is vendor-supported, and end-of-support dates are recorded.	0 1 2
L2	Any unsupported software has a documented exception, mitigations, and an accepted owner of the risk.	0 1 2
L3	Third-party components are updated on a schedule, and none is more than four years out of date.	0 1 2
L4	Each application has a TIME classification, reviewed at least annually.	0 1 2
L5	Cloud and SaaS dependencies have a documented exit path.	0 1 2

Dimension 5 · Cost

The cost of software arrives mostly after launch. Robert Glass's widely cited synthesis puts maintenance at **40 to 80 percent of total software cost, averaging about 60 percent**, and most of that is enhancement, the system keeping pace with the business.[20] McKinsey's 2020 survey of 50 CIOs found technical debt estimated at **20 to 40 percent of the value of the entire technology estate**.[21]

Licence waste is the most visible symptom. Zylo, a vendor of SaaS management software, reported in its 2025 index that average licence utilization was **about 47 percent**, meaning roughly half of paid licences went unused.[22]

Item		Score
C1	The annual cost of each critical application is known, including licences, hosting, support, and people's time.	0 1 2
C2	Licence utilization is known for the 20 largest software subscriptions.	0 1 2
C3	Technical debt is estimated for each critical application, with a budget to reduce it.	0 1 2
C4	A budget for planned change exists, separate from break-fix.	0 1 2

Dimension 6 · AI components

This is where most estate assessments are silent and where risk is growing fastest. In Microsoft and LinkedIn's 2024 Work Trend Index, **78 percent of people who use AI at work bring their own tools**.[23] IBM's 2025 *Cost of a Data Breach* study found that **63 percent of breached organizations had no AI governance policy or were still developing one**.[24]

AI components also have a lifecycle that is set by someone else. Anthropic commits to at least 60 days' notice before retiring a model; OpenAI commits to at least six months for generally available models and as little as two weeks for previews.[25] An AI feature without an owner stops working on a known date.

The NIST AI Risk Management Framework makes each item below concrete. GOVERN 1.6 calls for mechanisms "to inventory AI systems." GOVERN 1.7 calls for safe decommissioning. MANAGE 3.2 requires that pre-trained models "are monitored as part of AI system regular monitoring and maintenance."[26] ISO/IEC 42001 builds a certifiable management system around the same expectations.[27]

Item		Score
A1	An inventory of AI components exists, including AI features in applications and tools staff have built.	0 1 2
A2	Each AI component has a named owner and documented responsibilities.	0 1 2
A3	Model versions are pinned, vendor retirement notices are monitored, and a fallback exists.	0 1 2
A4	The outputs of AI components are monitored after deployment.	0 1 2

Item		Score
A5	AI-generated code is reviewed and security-tested before it reaches production.	0 1 2
A6	Each AI feature can be switched off or retired without breaking the process it supports.	0 1 2
A7	A written policy covers which AI tools staff may use and with what data.	0 1 2

Your results

Dimension	Items	Your score	Maximum	Percent	Band
Ownership	5		10		
Operations and recoverability	8		16		
Security posture	5		10		
Lifecycle and supportability	5		10		
Cost	4		8		
AI components	7		14		
Total	**34**		**68**		

Owned · 75 percent or more of the maximum. The dimension has owners and proven practices. Keep it that way with a scheduled review.

Exposed · 40 to 74 percent. Things work, but some of it depends on individuals or luck. One departure, failed change, or vendor notice could become expensive.

Unowned · below 40 percent. Treat the dimension as a business risk, not an IT task. Start with the critical items and the owner question.

Critical items. Whatever your total, a score of 0 on any of the four items marked ★ (**O1** named owners, **O4** company custody of accounts, **R3** tested restore, **L1** supported software) deserves action this quarter. Each one is a single point of failure that a good total can hide.

Reading your score

A scorecard is useful only if it changes what happens next. Three patterns are common.

Low Ownership, decent everything else. The practices exist because of one or two capable people. That is a strength today and a concentration risk tomorrow. Start with O1, O3, and O4: name the owners, give each critical application a second person, and move every account into company custody.

Good Ownership, low Recoverability or Lifecycle. The applications have owners who are fully occupied keeping them running. The gap is capacity, not accountability. Prioritize a tested restore (R3) and a supported-software plan (L1 and L2), then build the runbooks that let other people respond.

Low AI. This is now the most common pattern, including in companies that score well elsewhere. Begin with the inventory (A1) and owners (A2); the rest follows from knowing what exists.

In enterprise architecture terms, the scorecard is a lightweight baseline. TOGAF builds every change on a baseline description of the current state, and keeps delivered systems aligned with the business through architecture change management (Phase H). Re-scoring every six to twelve months, and recording each application's TIME classification as you go, gives a mid-sized company the same discipline without the bureaucracy.

What to do in the next 90 days

1. **Score your three most critical applications**, not just the estate as a whole. The differences between them will tell you where ownership is thin.
2. **Close the critical items.** Name owners, move accounts into company custody, run and time a test restore, and record end-of-support dates.
3. **Classify each application with TIME.** Decide what to invest in, what to tolerate on purpose, what to migrate, and what to retire.
4. **Assign the work.** Each gap needs an owner and a date. Some will sit with your team; some are better carried by a partner.
5. **Re-score in six months** and compare against your own baseline.

Where my team fits

Rob Bickel Agency takes ownership of the applications established, mid-sized companies run on. We provide **after-build ownership** of the applications behind your critical capabilities, so the Ownership, Recoverability, and Lifecycle dimensions stay at 2 rather than drifting back. We own **change management**, so every change is assessed, tested, released, and recorded. And when something critical fails, our **break-fix and urgent consulting** work stabilizes it first, then puts it on the path to ongoing ownership.

If you would like a second opinion on your results, send me your dimension scores and the applications that worry you. I will reply personally with the two or three changes that would reduce your exposure most.

Appendix · Framework crosswalk

NIST CSF 2.0 references are to subcategories. CIS references are to v8.1 safeguards; all listed safeguards are in Implementation Group 1 except 11.5, which is IG2. ISO references are to ISO/IEC 27001:2022 Annex A control titles. AI RMF references are to NIST AI 100-1. TOGAF references are to the Application Portfolio Catalog (APM) and the Architecture Development Method phases.

ID	NIST CSF 2.0	CIS v8.1	ISO 27001 Annex A	Operations, architecture, and AI
O1	GV.RR-02	—	5.9	TOGAF
O2	ID.AM-02	2.1	—	—
O3	GV.RR-03	—	—	—
O4	PR.AA-01, PR.AA-05	5.1	5.17, 5.18	—
O5	GV.SC-05	—	5.19, 5.20	—
R1	PR.DS-11	11.2	8.13	—
R2	PR.DS-11	11.3, 11.4	—	—
R3	PR.DS-11, RC.RP-03	11.5 (IG2)	8.13, 5.30	—
R4	RC.RP-02	11.1	5.30	—
R5	ID.IM-04	—	—	ITIL incident mgmt; SRE
R6	—	—	—	DORA; SRE service level objectives
R7	PR.PS-01	4.1	8.9, 8.32	—
R8	ID.IM-04	—	—	ITIL problem mgmt; SRE postmortems
S1	PR.AA-03	6.3, 6.5	5.17	—
S2	PR.AA-05	5.3, 6.2	5.11, 5.18	—
S3	PR.AA-01	—	5.17	—
S4	PR.PS-02	7.1, 7.2, 7.4	8.8	—
S5	GV.SC-04, ID.AM-04	—	5.19, 5.21	—

L1	PR.PS-02, ID.AM-08	2.2	8.8	—
L2	PR.PS-02	2.2	—	—
L3	PR.PS-02	7.4	8.8	—
L4	ID.AM-08	—	—	TIME; TOGAF Phase H
L5	GV.SC-07	—	5.23	—
C1	GV.RR-03	—	—	TOGAF APM
C2	ID.AM-02	2.1, 2.3	—	—
C3	—	—	—	TOGAF Phase H; TIME
C4	GV.RR-03	—	—	TOGAF Phases G and H
A1	ID.AM-02	—	—	AI RMF GOVERN 1.6; ISO 42001 A.6
A2	GV.RR-02	—	—	AI RMF GOVERN 2.1
A3	—	—	—	AI RMF MANAGE 3.1, 3.2, GOVERN 6.2; ISO 42001 A.10
A4	—	—	—	AI RMF MANAGE 4.1; ISO 42001 A.6
A5	PR.PS-06	—	—	ISO 42001 A.6
A6	—	—	—	AI RMF GOVERN 1.7, MANAGE 2.4
A7	—	—	—	AI RMF GOVERN 6.1; ISO 42001 A.2

Sources and notes

Figures are quoted as published. Vendor research is labelled; it is useful for direction, and its publishers sell related products. TOGAF quotations are from The Open Group's public TOGAF 9 pages.

1. Gartner, "Technical Debt Benchmarks Are a Waste of Time" (research note).
2. Avelino, Passos, Hora, Valente, "A novel approach for estimating truck factors," ICPC 2016. arxiv.org/abs/1604.06766
3. Avelino, Constantinou, Valente, Serebrenik, "On the abandonment and survival of open source projects," ESEM 2019. arxiv.org/abs/1906.08058
4. US Bureau of Labor Statistics, *Employee Tenure*, January 2026, Table 6. bls.gov
5. The Open Group, TOGAF 9, *Application Portfolio Catalog*. pubs.opengroup.org
6. Sophos, *The impact of compromised backups on ransomware outcomes*, survey of 2,974 ransomware victims by Vanson Bourne (vendor). sophos.com
7. Veeam, 2025 ransomware research (vendor), as announced via Business Wire, April 2025. businesswire.com
8. CISA and MS-ISAC, *#StopRansomware Guide*. cisa.gov
9. Center for Internet Security, *CIS Critical Security Controls v8.1*, safeguard 11.5 and Implementation Groups. cisecurity.org
10. NIST, *Cybersecurity Framework 2.0* (CSWP 29), February 2024. nist.gov
11. DORA, *DORA's software delivery metrics*. dora.dev
12. Verizon, *2025 Data Breach Investigations Report*. verizon.com
13. Verizon, *2026 Data Breach Investigations Report*, as reported by Help Net Security. helpnetsecurity.com
14. Sophos, *The State of Ransomware 2025* (vendor). sophos.com
15. UK Department for Science, Innovation and Technology, *Cyber Security Breaches Survey 2025*. gov.uk
16. CISA, *Bad Practices*. cisa.gov
17. Center for Internet Security, *CIS Critical Security Controls v8.1*, safeguard 2.2. cisecurity.org
18. Black Duck, *2025 Open Source Security and Risk Analysis Report* (vendor; based on M&A audits). blackduck.com
19. LeanIX, "Gartner TIME model." leanix.net
20. Robert L. Glass, *Facts and Fallacies of Software Engineering*, Addison-Wesley, 2002.
21. McKinsey & Company, "Tech debt: Reclaiming tech equity," 2020. mckinsey.com
22. Zylo, *2025 SaaS Management Index* (vendor). zylo.com
23. Microsoft and LinkedIn, *2024 Work Trend Index*. microsoft.com
24. IBM and Ponemon Institute, *Cost of a Data Breach Report 2025*. ibm.com

25. Anthropic, *Model deprecations*; OpenAI, *Deprecations*. platform.claude.com; developers.openai.com
26. NIST, *AI Risk Management Framework 1.0* (AI 100-1), Core. airc.nist.gov
27. ISO/IEC 42001:2023, *Artificial intelligence: Management system*. iso.org

Rob Bickel Agency · Managed Software Services

Need an owner for the software your business runs on?

After-build ownership, change management, and urgent break-fix for the applications established, mid-sized companies depend on. I lead every engagement personally, supported by our onshore and nearshore engineers.

bickel.rob@gmail.com

robbickel.com