NEWMIND PARTNERS

NEWMIND RESEARCH · BENCHMARK REPORT 11

TECHNICAL DEBT BENCHMARK 2026

What published research says technical debt costs, how much developer time it takes, how old systems raise security risk, what the EU CRA, NIS2, DORA and the US SEC rule now expect, what the debt is worth in wages, and the playbooks and worksheets to pay it down.

Edition 1
Desk-research edition

October 2026
Published

Licence
Single company use

CONTENTS

What's inside

01	About this edition	5
02	Executive summary	7
PART A · MARKET EVIDENCE		
03	What technical debt is, and why it is hard to count	9
04	Tech debt as a share of the technology estate	10
05	The new-product budget that goes to old problems	11
06	The cost of poor software quality in the US	12
07	A prediction of rising severity	13
08	The market for paying debt down	14
09	Reading the market numbers together	15
10	Hours in the developer week spent on debt	16
11	Maintenance, bad code and what developers say holds them back	17
12	Technical debt as the top frustration at work	18
13	AI coding tools and delivery performance	19
14	Trust in AI-generated code	20
15	The people who pay the debt down are in short supply	21
16	Hard-to-fill ICT vacancies, and why	22
17	Legacy systems in UK central government	23
18	Funding: the gap the UK review names	24
19	US federal IT: most of the budget keeps the lights on	25
20	The federal systems most in need of modernisation	26
21	Lessons from public-sector reviews	27
22	What breach data says about old weaknesses	28
23	Breach trends: third parties, exploitation, ransomware	29
24	Known exploited vulnerabilities: the public list	30
25	Where exploited vulnerabilities cluster	31
26	End of support: Windows and SQL Server	32
27	End of support: .NET and Python	33
28	An end-of-support calendar	34
29	How security turns debt into interest	35
PART B · REGULATION		
30	The rules: an overview	36
31	EU Cyber Resilience Act: scope and dates	37
32	Cyber Resilience Act: reporting exploited vulnerabilities	38

33	Cyber Resilience Act: support periods and fines	39
34	NIS2: risk management for essential and important entities	40
35	NIS2: incident reporting deadlines	41
36	DORA: legacy systems in financial services	42
37	US SEC: cybersecurity disclosure rule	43
38	SEC: the four-business-day incident filing	44
39	What the rules ask of a debt programme	45

PART C · THE NEWMIND MODEL

40	The NEWMIND model: method and inputs	46
41	The NEWMIND model: wage inputs	47
42	The NEWMIND model: what debt time costs a team	48
43	The NEWMIND model: measuring your own share	49
44	The NEWMIND model: what reclaimed time is worth	50
45	The NEWMIND model: when a debt programme pays back	51
46	The NEWMIND model: limits	52

PART D · PLAYBOOKS

47	How to use the playbooks	53
48	Playbook: measure debt before you fund it	54
49	Playbook: build a legacy register	55
50	Playbook: ring-fence a debt budget	56
51	Playbook: modernise or retire a legacy system	57
52	Playbook: plan ahead of end of support	58
53	Playbook: patch exploited weaknesses first	60
54	Playbook: use AI coding tools without adding debt	61
55	Playbook: map the rules to your systems	62
56	Playbook: rehearse incident reporting	63
57	Playbook: make the case to the board	64

PART E · SELF-ASSESSMENT TOOLKIT

58	Self-assessment: KPI sheet	66
59	Self-assessment: debt maturity score	67
60	Scenario tables: debt cost and payback	68
61	Reference grid: wage cost of programme hours	70
62	Worksheet: hours on technical debt	71
63	Worksheet: legacy register	72
64	Worksheet: debt budget and board case	73
65	Worksheet: keep, fix, replace or retire	74
66	Worksheet: end-of-support calendar	75

67	Worksheet: exploited-vulnerability log	76
68	Worksheet: AI coding tools review	77
69	Worksheet: rules, systems and reporting	78

REFERENCE

70	Sources by type	79
71	Method and limits	82
72	Glossary	84
73	Sources	85

Figures from third-party research carry a numbered source (full list in the Sources chapter). Everything else is labelled as NEWMIND analysis or model.

Page numbers refer to the full report.

CHAPTER 01

About this edition

This is Edition 1 of the NEWMIND Technical Debt Benchmark. It is a desk-research edition: it contains no original survey data and no peer quartiles. It is built on official legal texts, official statistics, public sector reviews, product owners' lifecycle pages, and vendors' and consultancies' own published research, each fetched, saved and checked for this edition.

What this edition contains

- **Market evidence**: what CIOs and analysts publish on the size and cost of technical debt, from McKinsey[1], CISQ[2], Forrester[3] and MarketsandMarkets[4], each tagged as a consultancy or vendor claim.
- **Developers**: time spent on debt and maintenance from Stripe[5], Stack Overflow[6] and the DORA research programme[7], with EU skills data from Eurostat[8].
- **Public sector**: legacy systems in UK central government[9] and US federal agencies[10].
- **Security**: breach data from Verizon[11], the CISA catalogue of known exploited vulnerabilities[12], and end-of-support dates from Microsoft[13] and the Python project[14].
- **Regulation**: the EU Cyber Resilience Act[15], NIS2[16], DORA[17] and the US SEC cyber disclosure rule[18], with dates from the official texts only.
- **A transparent model**: what debt time costs a team in wages and when a debt programme pays back, from US wage statistics[19], labelled 'Market research model · based on published benchmarks'.
- **10 playbooks**: measure debt before you fund it, build a legacy register, ring-fence a debt budget, modernise or retire a legacy system, plan ahead of end of support, patch exploited weaknesses first, use AI coding tools without adding debt, map the rules to your systems, rehearse incident reporting, make the case to the board.
- **Self-assessment toolkit**: a KPI sheet, a debt maturity score, scenario tables, a wage cost reference and 8 blank worksheets (hours on technical debt, legacy register, debt budget and board case, keep, fix, replace or retire, end-of-support calendar, exploited-vulnerability log, ai coding tools review, rules, systems and reporting).

What it does not contain yet

No original survey data. Edition 1 is desk research. NEWMIND ran no survey for it and publishes no peer quartiles by company size, sector or region. A later edition may add a survey of firms; this one does not claim it.

Who it is for

CIOs and CTOs, heads of engineering and architecture, CISOs, and the finance, risk and legal leads who fund modernisation or answer for its risks.

You will recognise these signals

- Every change to a core system takes longer than the team estimated
- Products past their end of support still run in production, and no one has a list
- Security fixes wait because the system around them is too fragile to touch

- The board asks what the CRA, NIS2 or DORA mean for old systems and no one owns the answer

What to measure

- Share of developer time spent on maintenance and debt, by team
- Systems past or near their end of support, with an owner and a date
- Known exploited vulnerabilities open in your estate, and their age
- Budget ring-fenced for debt reduction, against what was spent
- Lead time for a change on your oldest systems against your newest

How to read the numbers

- **Official figures** carry a numbered source and their population: which organisations, which country, which period. Figures from different sources use different definitions, so they are shown side by side, never added up.
- **Vendor and consultancy figures** are tagged 'vendor claim' or 'consultancy claim'. They are printed as published and not independently tested.
- **Models** are transparent: every formula and input is printed so you can replace it with your own data.
- **Dates**: legal dates come only from the official texts and are stated against 11 October 2026. Where the report reads what a rule means for a firm, it says so: 'In NEWMIND's reading'.
- **Currency**: US dollars throughout. EU fines are quoted in euros, as the texts state them.

From benchmark to your numbers

A NEWMIND feasibility audit measures your own organisation in 3–4 weeks and delivers:

- A register of your legacy systems with support dates, owners and risk
- The share of engineering time your debt takes, measured on your own data
- A ranked plan to keep, fix, replace or retire each system, with the cost of each
- A map of your systems against the CRA, NIS2, DORA and SEC duties that apply to you

Licence: single company use. Please cite as: NEWMIND Research, Technical Debt Benchmark 2026, Edition 1. NEWMIND PARTNERS has no affiliation with any vendor, consultancy or firm named in this report.

CHAPTER 02

Executive summary

The published evidence agrees on the direction, if not the size: technical debt takes a large share of technology budgets and developer time, old and unsupported systems keep growing as a share of estates, and attackers use the weaknesses they leave. In the EU, the CRA, NIS2 and DORA now turn part of that debt into a legal duty. The cost can be priced from your own wages, and the toolkit shows how.

20% to 40%

Of the value of the technology estate, CIOs' estimate of their tech debt in McKinsey's survey

CONSULTANCY CLAIM [1]

13.5 of 41.1 hours

Weekly hours on technical debt, out of a developer's working week, in Stripe's survey (means)

VENDOR CLAIM [5]

28%

Share of UK central government systems that are legacy, as estimated for 2024 by the UK government's review [9]

Ten findings

01 CIOs put debt at a fifth to two fifths of their estate

In McKinsey's survey, CIOs estimated that tech debt amounts to 20% to 40% of the value of their entire technology estate before depreciation CONSULTANCY CLAIM [1]. The population is 50 CIOs of financial-services and technology companies with revenues above $1 billion.

02 Debt takes money meant for new products

The same CIOs reported that 10% to 20% of the technology budget dedicated to new products is diverted to resolving issues related to tech debt CONSULTANCY CLAIM [1], and 60% felt their organisation's tech debt had risen perceptibly over the past three years CONSULTANCY CLAIM [1].

03 About a third of a developer's week goes on debt

In Stripe's survey, respondents estimated that the average developer at their company spends 13.5 hours a week addressing technical debt, out of a working week of 41.1 hours (both means) VENDOR CLAIM [5]. That is 32.8% of the week by NEWMIND arithmetic, the default share in the model.

04 Developers name debt as their top frustration

Technical debt is the top frustration at work for professional developers, according to 63% of respondents to Stack Overflow's 2024 survey who answered the question VENDOR CLAIM [6].

05 AI coding tools do not pay debt down on their own

Google's DORA research programme estimated that as AI adoption increased, delivery throughput decreased by 1.5% and delivery stability fell by 7.2% VENDOR CLAIM [7]; 39% of respondents reported little to no trust in AI-generated code VENDOR CLAIM [7].

06 Legacy is a growing share of government estates

The UK government's digital review estimates that legacy makes up 28% of systems in central government departments in 2024, up from 26% in 2023, according to the review [9]; 28% of red-rated legacy systems lack remediation funding [9].

07 Old weaknesses are a leading way in

Verizon's 2025 breach report names exploitation of vulnerabilities, at 20%, among the leading initial attack vectors, and says such exploitation has surged by 34% VENDOR CLAIM [11]. CISA's catalogue of known exploited vulnerabilities lists 1,739 entries in its version of 8 October 2026, according to the published file [12].

08 Support has already ended for common Microsoft products

Microsoft support for Windows 10 Home and Pro ended on 14 October 2025, Pacific Time, according to its lifecycle page [13]. Extended support for SQL Server 2016 ended on 14 July 2026 and for Windows Server 2016 ends on 12 January 2027, according to the same lifecycle pages [20,21].

09 EU rules now reach old products and legacy systems

Under the EU Cyber Resilience Act, the reporting duties of Article 14 have applied since 11 September 2026, and the rest of the Regulation applies from 11 December 2027, as the Regulation states [15]. DORA has applied since 17 January 2025 and requires financial entities, at least yearly, to conduct a specific ICT risk assessment on all legacy ICT systems [17].

10 Debt time is worth pricing

At the US mean wage for software developers [19], 32.8% of the time of a team of 20 developers is about $972,000 a year in wages, before benefits (NEWMIND model). Chapter 42 sets out the formula and the inputs to replace with your own.

What to do on Monday

1. Fill in the KPI sheet for your organisation (full report, chapter 58).
2. Measure the hours your teams spend on debt (full report, chapter 62).
3. List your legacy systems with an owner and a support date (full report, chapter 63).
4. Plan for every product past or near its end of support (full report, chapter 52).
5. Price the debt time of one team with your own wages (full report, chapter 42).
6. Write the business case for a first debt programme (full report, chapter 57).

CHAPTER 03

What technical debt is, and why it is hard to count

Technical debt is the extra work an organisation will have to do later because of a shortcut, an ageing component or a design that no longer fits what the business needs. Like financial debt it has a principal (the work to fix it) and interest (the time, incidents and risk it costs every week it stays).

It is hard to count because no ledger records it. Every figure in this report comes from one of four places: what executives estimate in surveys, what developers say about their own week, what official bodies find when they audit public systems, and what vendors publish about their markets. Each is a different lens, and none of them is a measurement of your estate.

Four kinds of debt this report covers

KIND	WHAT IT LOOKS LIKE	WHERE THE EVIDENCE SITS
Code and design debt	Hard-to-change code, missing tests, tangled dependencies	Chapter 10 to chapter 14
Legacy systems	Old platforms, outdated languages, scarce skills	Chapter 17 to chapter 21
Unsupported software	Products past their vendor's end-of-support date	Chapter 26 to chapter 29
Security exposure	Known vulnerabilities left unpatched	Chapter 22 to chapter 25

What this means

- Treat any single headline number as one lens, not as the size of your problem.
- Your own inventory, hours and incident data matter more than any benchmark. Chapter 58 lists what to track.
- This edition is desk research. NEWMIND ran no original survey; where we add arithmetic, it is labelled NEWMIND analysis or model.

Definition and categories: NEWMIND analysis.

CHAPTER 04

Tech debt as a share of the technology estate

In a McKinsey survey of 50 CIOs of financial-services and technology companies with revenues above $1 billion, carried out in July 2020, CIOs estimated that tech debt amounts to 20% to 40% of the value of their entire technology estate before depreciation CONSULTANCY CLAIM [1].

20%–40%

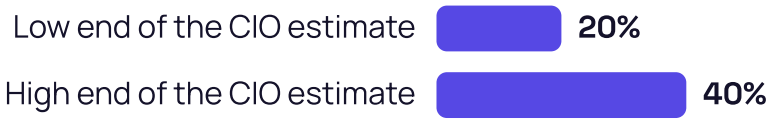
of estate value, as estimated by 50 CIOs

CONSULTANCY CLAIM [1]

50

CIOs in the sample, financial services and technology only [1]

Tech debt as a share of estate value, CIO estimate, 2020, %



Source: McKinsey, CIO survey of 2020 CONSULTANCY CLAIM [1]. Chart: NEWMIND.

How to read it

The figure is an estimate given by executives, not an audit. The sample is small and drawn from two sectors with large, long-lived estates, so it says more about large financial and technology firms than about a mid-sized company in another sector.

What this means

- A range this wide tells you the CIOs themselves were unsure. Use it to start a conversation, not to set a budget.
- Value 'before depreciation' is a gross figure; few companies hold their estate in a register at that value. Chapter 63 gives a simpler starting point.

Reading and implications: NEWMIND analysis.

CHAPTER 05

The new-product budget that goes to old problems

The same 50 CIOs reported that 10% to 20% of the technology budget dedicated to new products is diverted to resolving issues related to tech debt CONSULTANCY CLAIM [1].

10%–20%

of the new-product technology budget diverted to tech-debt issues, CIO report

CONSULTANCY CLAIM

1

60%

of the CIOs felt their tech debt had risen perceptibly over the past three years

CONSULTANCY CLAIM

1

Why the diversion matters more than the stock

A stock of debt is abstract. A share of this year's budget that never reaches new products is concrete: it is time and money a team planned for growth and spent on repair. That is the number most finance teams can act on, because it already sits inside an approved budget.

The question was asked in 2020. The survey does not say how the diverted share has moved since, so this report does not project it forward. Chapter 40 shows how to put a value on the same idea with your own hours and public wage data.

What this means

- Ask each product team what share of last quarter's work went to fixing what already existed. Compare it with what was planned.
- If the gap is large, the debt is already being paid; the decision is whether to pay it on purpose. Chapter 50 sets out how.

Reading and implications: NEWMIND analysis.

CHAPTER 10

Hours in the developer week spent on debt

Stripe and Harris Poll surveyed more than 1,000 developers and more than 1,000 C-level executives in the United States, the UK, France, Germany and Singapore VENDOR CLAIM [5]. Asked how many hours each week the average developer at their company spends on addressing technical debt, developers gave a mean of 13.5 hours, against an average developer week of 41.1 hours VENDOR CLAIM [5].

13.5 h

a week on technical debt, mean of developers' estimates for the average developer at their company

VENDOR CLAIM [5]

41.1 h

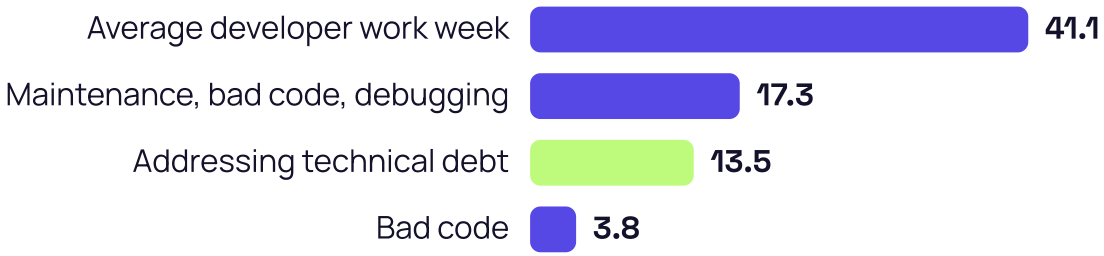
average developer work week, mean across all countries

VENDOR CLAIM [5]

32.8%

of that week, NEWMIND arithmetic on the two means; Stripe does not print this share

The developer week as Stripe reported it, September 2018, hours



Source: Stripe, The Developer Coefficient, September 2018 VENDOR CLAIM [5]. Chart: NEWMIND.

Limits you must keep with the number

- **Self-reported.** These are estimates of a colleague's week, not timesheets.
- **Dated.** The survey was published in September 2018, before AI coding assistants were common.
- **Five countries, by the methodology page.** The report's introduction says six; the methodology lists five. This report follows the methodology.
- **The share is ours.** 32.8% is 13.5 divided by 41.1, a NEWMIND calculation. Chapter 40 uses it as a model input, labelled as such.

CHAPTER 73

Sources

Each entry gives the date that applies to it: when a law was adopted or came into force, when a document was published, or, for live web pages and datasets, when it was accessed (11 October 2026). Figures quoted are short, attributed and linked; no paywalled tables and no third-party charts are reproduced.

1. McKinsey Digital, Tech debt: Reclaiming tech equity, published 6 October 2020 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-debt-reclaiming-tech-equity
2. CISQ, The Cost of Poor Software Quality in the US: A 2022 Report (press release), published 6 December 2022 https://www.it-cisq.org/press-releases/12-06-22/
3. Forrester, Technology & Security Predictions 2025 (press release via Business Wire), published 22 October 2024 https://via.tt.se/pressmeddelande/3664452/forresters-technology-and-security-predictions-2025-tech-leaders-will-triple-the-adoption-of-aiops-to-reduce-technical-debt
4. MarketsandMarkets, Application Modernization Services Market, global forecast to 2031, published 29 October 2025 https://www.marketsandmarkets.com/Market-Reports/application-modernization-services-market-149625724.html
5. Stripe, The Developer Coefficient (survey with Harris Poll), published 14 September 2018 https://stripe.com/files/reports/the-developer-coefficient.pdf
6. Stack Overflow, 2024 Developer Survey: Professional Developers, accessed 11 October 2026 https://survey.stackoverflow.co/2024/professional-developers
7. Google Cloud, Announcing the 2024 DORA report, published 23 October 2024 https://cloud.google.com/blog/products/devops-sre/announcing-the-2024-dora-report
8. Eurostat, Employed information and communications technology (ICT) specialists (dataset isoc_sks_itspt), published 17 April 2026 https://ec.europa.eu/eurostat/api/dissemination/statistics/1.0/data/isoc_sks_itspt?geo=EU27_2020&unit=PC_EMP&lang=EN
9. UK Department for Science, Innovation and Technology, State of digital government review, published 21 January 2025 https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review
10. U.S. Government Accountability Office, GAO-25-107795, Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems, published 17 July 2025 https://www.gao.gov/products/gao-25-107795
11. Verizon, 2025 Data Breach Investigations Report (news release), published 23 April 2025 https://www.verizon.com/about/news/2025-data-breach-investigations-report
12. CISA, Known Exploited Vulnerabilities Catalog (version 2026.10.08), published 8 October 2026 https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
13. Microsoft Learn, Windows 10 Home and Pro lifecycle, accessed 11 October 2026 https://learn.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro
14. Python Developer's Guide, Status of Python versions, accessed 11 October 2026 https://devguide.python.org/versions/
15. Regulation (EU) 2024/2847 (Cyber Resilience Act), Official Journal of the European Union, adopted 23 October 2024 https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
16. Directive (EU) 2022/2555 (NIS2 Directive), Official Journal of the European Union, adopted 14 December 2022 https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
17. Regulation (EU) 2022/2554 (Digital Operational Resilience Act), Official Journal of the European Union, adopted 14 December 2022 https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
18. SEC final rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 FR 51896 (official PDF), published 4 August 2023 https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16194.pdf
19. U.S. Bureau of Labor Statistics, Occupational Employment and Wage Statistics, national estimates (May 2025), accessed 11 October 2026 https://www.bls.gov/oes/
20. Microsoft Learn, SQL Server 2016 lifecycle, accessed 11 October 2026 https://learn.microsoft.com/en-us/lifecycle/products/sql-server-2016
21. Microsoft Learn, Windows Server 2016 lifecycle, accessed 11 October 2026 https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2016

© 2026 NEWMIND PARTNERS. Licensed for use within one company. NEWMIND PARTNERS AG, Luzern, Switzerland · NEWMIND PARTNERS Inc., Sheridan, Wyoming, USA · hi@newmindpartners.com

END OF SAMPLE

Get the full report

This sample includes the cover, contents, about page, executive summary, the opening of Part A on what technical debt is, what CIOs estimate it is worth and the budget it takes, the developer hours it uses, and the sources cited in them. The full report continues with analyst and services market figures, developer frustration, AI coding tools and skills, legacy systems in UK and US government, breaches, known exploited vulnerabilities and end-of-support calendars, the EU CRA, NIS2, DORA and the US SEC rule, the NEWMIND model, ten playbooks and the self-assessment toolkit.

Full report

newmindpartners.com/benchmark-technical-debt.html#report

NEWMIND PARTNERS

NEXT STEP

TURN THIS BENCHMARK INTO DEBT YOU PAY DOWN.

You now know what is published on the cost of technical debt, its security risk and the rules that reach it. NEWMIND PARTNERS measures your own debt, then designs, builds and tests the work that pays it down.

01

Feasibility audit

In 3–4 weeks we map your estate on your data (read-only): the legacy systems, their support dates and owners, the time your teams spend on debt, and the rules that apply to you. Then we compare every option: keep, fix, replace or retire.

02

Design

We rank the debt by cost and risk, write the plan and the budget for each system, and map it against the CRA, NIS2, DORA and SEC duties that apply to you.

03

Build and run

Our senior engineers modernise or replace the systems, connect them to the tools you already use, and can run them in production with monitoring.

04

Prove it

Baseline on day one, then the measured change in hours on debt, lead time and incidents, reported every month.

Start with a feasibility audit

Find out which debt costs you most, which systems carry the most risk, and the business case to fix them. No commitment.

Start a feasibility audit →

newmindpartners.com/pre-audit.html · hi@newmindpartners.com · Luzern, Switzerland · Sheridan, Wyoming, USA