THE TWELVE

The security metrics every examiner, insurer and board asks for first — with the target that counts as 'good' in 2026.

Start here at any maturity. These twelve are the insurable baseline, the NYDFS certification core, the SEC Item 1C evidence, and what a CISO's first 100 days should baseline. Everything else phases in later.

#	Metric	What it actually means	Good =	What they'll ask
1	**MFA — enforced for all users on all systems**	Enforced, not enabled. Includes email, remote access, admin, backup console.	**100%**	'Is MFA enforced everywhere? Show me the export.'
2	**EDR on every endpoint and server**	Agent checked in within 24 h; denominator from your inventory, not the console.	**≥ 98%**	'What % of devices have EDR? Servers too?'
3	**Immutable or offline backups**	A copy a compromised admin cannot delete; separate credentials.	**100% of critical data**	'Can a domain admin delete your backups?'
4	**Restore test — full, recent**	Full restore of critical systems, dated, with time-to-recover.	**Tested ≤ 6 months**	'When did you last restore, and how long did it take?'
5	**Critical/high vulnerabilities fixed within SLA**	Critical ≤ 15 days, high ≤ 30; on in-scope assets.	**≥ 90%**	'What's your patch SLA and are you meeting it?'
6	**KEV vulnerabilities open > 7 days**	CISA Known Exploited — the ones being used this week.	**0**	'Anything on the KEV list still open?'
7	**Internet-facing high/critical exposures**	Exposed RDP/SMB, EOL appliances, KEV on the perimeter.	**0**	'What does an external scan show right now?'
8	**Tier 1–2 vendors assessed with current evidence**	Critical vendors with an assessment and attestation inside cadence.	**100%**	'Who has your data, and when did you last check them?'
9	**Notifications on time**	Regulator, insurer, customer and contractual notices inside their windows.	**100%**	'Did you meet every clock last incident?'
10	**Incidents by severity — trended**	Confirmed incidents per quarter, same definitions every quarter.	**Trend down**	'How many incidents, and is it getting better?'
11	**Mean time to respond (MTTR)**	Detection → containment for confirmed incidents; the protection level you pay for.	**< 4 h (critical)**	'How fast do you contain?'
12	**Program maturity — trended**	Framework-based score, independently sampled, shown as a line not a number.	**+0.5 / yr**	'How do you know the program is improving?'

Three rules that keep them honest

1. The denominator comes from your inventory, never from the tool producing the number. 2. Publish the definition and keep it stable — trend is the asset. 3. Every red or amber gets one sentence, not a slide.

ciso.diy · Get the full 86-metric library with formulas, sources, targets and framework mappings (MET-01), or the 37-control insurance readiness self-assessment these twelve come from (INS-01). · Not legal advice.

Get your first twelve numbers in an afternoon

Where each number comes from, and the trap that makes it quietly wrong.

#	Source (export this)	Compute	The trap
1	IdP / M365 / Google: authentication-method and enforcement report; user list	enforced ÷ all accounts	Counting 'enabled' as enforced; leaving out shared and service mailboxes
2	EDR console device list with last-seen; CMDB or discovery count	healthy agents ÷ inventory count	Using the EDR console as the denominator
3	Backup console: immutability / retention-lock flag per repository; credential separation	isolated data sets ÷ critical data sets	A cloud backup with the same admin password
4	Restore-test log (make one if it doesn't exist): date, systems, time to recover	most recent full restore date	File-level restores counted as full
5	Vulnerability scanner: findings with first-seen / closed dates by severity	closed within SLA ÷ closed	Risk-accepting to clear the queue; changing the SLA
6	Scanner findings joined to CISA KEV feed	count open > 7 days	Assets outside scan scope
7	External scan (EASM / Shodan / microsec.tools) of your public ranges	count high/critical	'That host isn't ours' — check the ranges
8	Vendor inventory with tiers; assessment and attestation dates	current ÷ Tier 1–2 vendors	Downgrading tiers to hit the number
9	Incident register + clock log (discovery, determination, notice sent)	on time ÷ required	Late 'determination' to reset the clock
10	Incident register by severity per quarter	count, same definitions	Changing severity definitions
11	Incident tickets: detection and containment timestamps	median (contain − detect)	Redefining 'contained'
12	Framework self-assessment (CSF 2.0, CIS, ISO) — same one each year; an assessor samples it	weighted domain average, trended	Self-scoring drift with no independent check

What to do with the numbers

Red on 1, 2, 3 or 4 is a cyber-insurance decline in 2026 and the first finding in any exam — fix those before anything else; most are configuration, not spend.

Put the twelve on one page for the board with a target, the latest value, a trend arrow and one sentence per red or amber. Change the set once a year, not once a quarter.

Keep the exports. They are the evidence behind NYDFS 500.17(b), SEC Item 1C, the CCPA cybersecurity audit, SOC 2 and the insurance application — the same twelve, five audiences.