CWS
CYBERWERKSUITE

ISMS Measurement Catalogue

Forty-eight measures for an ISO/IEC 27001 management system — the headline formula for each, and what the number actually tells you.

No dashboard and no maturity model. The formulas themselves, the four traps that make them lie, and the rules that keep a ratio honest when an auditor recalculates it.

CyberWerkSuite · ISO/IEC 27001:2022 Clause 9.1 · Annex B of ISO/IEC 27004:2016 is informative — it offers measurement examples, not mandatory KPIs. Every formulation here is our own; we do not reproduce the annex.

48	36	12	DE / EN
Measures	Subjects in Annex B	Added for 2022 and 2024	Both editions

CyberWerkSuite

cyberwerksuite.com

Dr. Sait Yalazay

CISO · DPO · Author | CISM · CIPP · AAISM · LA 27001, 27701, 22301, 42001

Architect of Automated Compliance Systems for NIS2, GDPR, ISMS, BCM, DORA, Cloud Security (C5), Tisax & AI Act

Governance, resources, audit and improvement

Each measure in one line: the formula, what the number tells you, and whether it measures performance, effectiveness or both - the typing is ours, argued from Clause 7.2 and 7.3. B-numbers cite the construct in Annex B of ISO/IEC 27004:2016; CWS numbers are ours. “Plus n more” means the construct carries further derived ratios - the headline one is printed. Thresholds are deliberately absent and the reason comes after the list. This group: how the management system itself is resourced, steered, audited and corrected.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
B.2 PERFORMANCE	**Resources allocated divided by resources used, per budget line, over one budget period**	Whether the resources budgeted for security were actually used, and where they were not
B.3 PERFORMANCE	**Policies reviewed in the period divided by policies in force, as a percentage**	Whether policies are reviewed at the planned interval or after a significant change
B.4 PERFORMANCE	**Reviews held divided by reviews scheduled · plus 1 more**	Whether top management turns up to the reviews it owns
B.5 EFFECTIVENESS	**Count of high and medium risks above the acceptance threshold · plus 1 more**	How much risk sits above the accepted level, and whether it is being looked at
B.6 PERFORMANCE	**Audits performed divided by audits planned, as a percentage**	Whether the audit programme that was planned was delivered
B.7 PERFORMANCE	**Improvement actions meeting time, cost and quality divided by actions due in the period**	Whether improvement actions land on time, on cost and to requirement
B.8 EFFECTIVENESS	**Sum of the cost of every incident in the period, then the average per incident and category**	What the absence of security costs, period by period
B.9 PERFORMANCE AND EFFECTIVENESS	**Incidents that triggered an improvement action divided by all incidents**	Whether incidents change anything, or are only closed
B.10 PERFORMANCE	**Actions not implemented divided by actions planned to date · plus 2 more**	Whether corrective actions land when planned, and whether slippage has a reason

People and access

Training coverage and currency, how people behave when tested, and who still has rights they should not.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
B.11 PERFORMANCE	**Staff in ISMS roles trained divided by those required to be trained · plus 1 more**	How much of the workforce has had awareness training, and how much is still current
B.12 PERFORMANCE	**Staff who completed this year's general awareness training divided by all staff in scope**	Compliance with the annual awareness training requirement
B.13 PERFORMANCE	**Personnel who have signed divided by those planned to sign by that date, plus the trend**	Whether people completed awareness training and signed the user agreement with it
B.14 EFFECTIVENESS	**Sampled recipients passing a knowledge test on the campaign topics divided by those sampled**	Whether the content of an awareness campaign was understood
B.15 EFFECTIVENESS	**Clicked divided by tested, lower better, then a weighted sum of the rates · plus 2 more**	Whether staff react correctly to a simulated social-engineering attempt
B.16 PERFORMANCE	**Passwords complying with policy divided by registered passwords, against the previous ratio**	Whether the passwords in use meet the policy, assessed by inspection
B.17 PERFORMANCE AND EFFECTIVENESS	**Passwords not cracked within the test budget divided by all passwords, read as a trend**	How many passwords survive an automated cracking attempt
B.18 PERFORMANCE	**Critical systems with a periodic access-rights review divided by all critical systems**	Whether access rights on critical systems are reviewed systematically

Premises, suppliers and independent review

Entry control and maintenance, security terms in third-party agreements, and whether the planned reviews actually happen.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
B.19 PERFORMANCE	**An ordinal scale of the entry-control mechanism in use, cumulative levels, not a ratio**	What entry-control mechanism exists, and how strong it is
B.20 EFFECTIVENESS	**Unauthorised entries this period divided by the previous period figure, read as a trend**	Whether physical controls keep unauthorised people out of facilities holding systems
B.21 PERFORMANCE	**Completed events divided by planned events, with the gap between scheduled and actual dates**	Whether scheduled maintenance happens when it was scheduled
B.31 PERFORMANCE	**Average share of the required security requirements addressed per agreement**	How far required security requirements appear in third-party agreements
B.32 PERFORMANCE	**Addressed divided by required security requirements, averaged per agreement, plus the trend**	Whether agreements covering personal information carry the required requirements
B.36 PERFORMANCE	**Independent reviews conducted divided by independent reviews planned**	Whether the planned independent reviews of security are actually carried out
B.37 PERFORMANCE	**Systems with a valid assessment or penetration test date divided by all systems in inventory**	How much of the estate is genuinely in scope of assessment or penetration testing

Operations: change, malware, availability

The largest group, split across two pages. Where most organisations already have data and read it wrongly.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
B.22 PERFORMANCE	**New installations with change and hardening evidence divided by installations in the period**	Whether new systems go in through change management and the hardening baseline
B.23 EFFECTIVENESS	**Incidents caused by malicious software divided by attacks blocked - an odds ratio, not a share**	How well the protection stack stops malicious code, judged by what got through
B.24 PERFORMANCE	**Systems carrying obsolete signatures divided by all systems**	How many systems carry out-of-date anti-malware signatures
B.25 EFFECTIVENESS	**Actual end-to-end availability divided by maximum availability, agreed downtime excluded**	Whether each service delivers the availability it promised
B.26 PERFORMANCE	**Count of border-firewall rules with no hits in the sampling period, a count not a ratio**	How much of the border ruleset is dead weight

Operations: logs, configuration, vulnerabilities, incidents

The evidence trail, the baseline behind it, and whether incidents are resolved and learned from.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
B.27 PERFORMANCE	**Log files reviewed in the required period divided by all log files in scope**	Whether the critical log files that must be reviewed are actually reviewed
B.28 PERFORMANCE	**Devices configured correctly divided by all devices, by device type, once all is defined**	Whether devices stay configured the way policy says they should be
B.29 PERFORMANCE	**Critical systems tested since their last major release divided by all critical systems**	Whether critical systems have been tested since their last major release
B.30 EFFECTIVENESS	**Severity value of each open vulnerability multiplied by affected systems, then aggregated**	How much unpatched exposure the estate is carrying
B.33 EFFECTIVENESS	**Count of incidents exceeding their category resolution target, against the set threshold**	Whether incidents are resolved inside the target time for their category
B.34 EFFECTIVENESS	**Average of the last two periods divided by the average of the last six, all and by category**	Where incident volume is heading, overall and by category
B.35 PERFORMANCE	**Events formally treated by the response team divided by events reported in the period**	Whether security events are reported at all, and formally handled when they are

CyberWerkSuite extension, first half

Twelve constructs for subjects that had no measurement example in 2016: the eleven controls introduced by ISO/IEC 27002:2022, and the climate determination added to ISO/IEC 27001:2022 by Amendment 1 in 2024. None is presented as an ISO example.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
CWS.1 PERFORMANCE AND EFFECTIVENESS	**Sources ingested divided by sources in the source register · plus 1 more**	Whether named sources are really ingested, and whether intelligence changes anything
CWS.2 PERFORMANCE	**Discovered cloud services with a valid inventory entry divided by all discovered · plus 4 more**	Whether every cloud service is known and covered, and leavers were shut down properly
CWS.3 EFFECTIVENESS	**Critical services restored inside their objective divided by those tested · plus 3 more**	Whether critical services can really be restored inside their recovery objectives
CWS.4 PERFORMANCE AND EFFECTIVENESS	**Critical areas with continuous monitored detection divided by critical areas · plus 1 more**	Whether premises holding systems are monitored, and whether anyone answers the alarm
CWS.5 PERFORMANCE	**Asset classes covered by the configuration baseline divided by those in scope · plus 2 more**	Whether the configuration baseline covers what is installed, and how fast drift is fixed
CWS.6 PERFORMANCE	**Sensitive data types with a documented disposal method divided by all of them · plus 1 more**	Whether each sensitive data type has a disposal method, and whether data is deleted

CyberWerkSuite extension, second half

Masking, leakage, monitoring, filtering, secure development and the climate determination.

MEASURE TYPE	THE FORMULA, IN ONE LINE	WHAT THE NUMBER TELLS YOU
CWS.7 PERFORMANCE	**Non-production datasets masked or pseudonymised before provisioning divided by those in scope**	Whether production data reaches test and analytics environments in masked form
CWS.8 PERFORMANCE	**Assets with leakage controls active and tuned divided by assets in scope · plus 1 more**	Whether sensitive-data assets are covered, and whether the alerts are worth reading
CWS.9 EFFECTIVENESS	**Alerts triaged within the target time divided by alerts, by severity · plus 2 more**	Whether events reach one place, are triaged in time, and thresholds are still tuned
CWS.10 PERFORMANCE	**Assets with filtering enforced divided by assets in scope for filtering · plus 2 more**	Whether endpoints and networks really use the filtering service, and who gets around it
CWS.11 PERFORMANCE	**Process components present divided by those your policy defines · plus 3 more**	Whether a secure development process exists, developers are trained and code is checked
CWS.12 PERFORMANCE	**Binary yes or no: recorded in the context analysis, plus months since it was last reviewed**	Whether climate relevance was determined and recorded, and requirements captured with it

CWS
CYBERWERKSUITE

ISMSSuite

a tool from **CyberWerkSuite** · the ISO/IEC 27001 edition of NIS2**Suite**

THE ISO/IEC 27001:2022 EDITION OF THE CYBERWERKSUITE PLATFORM

The list you have just read, already running.

A list of formulas is a starting point only if something computes them. This is where these forty-eight live: each with the target you set, its frequency, owner and evidence source, feeding the management review instead of a spreadsheet nobody owns.

Control assessment

More than 300 assessable controls, mapped to the 93 of Annex A — assessed once, with the 2022 attribute scheme, gap severity and maturity calculated and the reasoning kept behind every score.

Statement of Applicability

A living SoA that stays in sync with the assessment and with the risk treatment plan — the document auditors ask for first.

Policy generation

Audit-ready policies in German and English, generated from your own answers, clause-level and exportable as PDF and Word.

Risk engine

Risks derived from real gaps, scored in a configurable matrix, with treatment decisions, owners and deadlines tracked to closure.

Measurement, Clause 9.1

These forty-eight measures built in, each with the target you set, its frequency, owner and evidence — results feed the management review, not a slide.

Management review pack

Clause 9.3 inputs assembled: performance trends, nonconformities, audit results and objective fulfilment, board-ready in one click.

Internal audit

Audit programme, findings register and corrective actions — the loop that keeps the evidence current all year.

Multi-standard

One control set, several obligations: ISO/IEC 27001:2022, NIS2 and the Implementing Regulation assessed from the same evidence base.

300+	93	48	DE / EN
Controls assessed	Annex A controls	Measures	Bilingual output

See the ISO 27001 edition at cyberwerksuite.com

Assessment · SoA · policies · measurement · management review
Also available as the 40-hour CISE programme

MADE IN GERMANY

Thorough, reliable — and ready long before the auditor asks.

CyberWerkSuite

cyberwerksuite.com

“We have KPIs” is not “we measure”

In almost every audit there is a moment when the metrics slide comes out. Ten percentages, eight of them green. Then one question tips it over.

Over what period, and what is in the denominator?

The question that ends most metrics presentations

- The answer is rarely a number. It is usually a sentence beginning “the system pulls that automatically”.
- And it ends with the discovery that two runs of the same quarter give different results.

Not wrong — unsettleable

WHY THAT MATTERS MORE THAN ACCURACY

A metric that cannot be reproduced is not a bad metric, it is not a metric. An auditor cannot verify it and a board cannot decide on it. Clause 9.1 requires that you measure; it does not say what. The list you have just read is what we measure, and why.

A measure is settled when its window, its counting unit and its acceptance rule are written down — before the first collection.

The time window and the counting unit

Two of the four traps are arithmetic. They look pedantic until the first time a number moves for the wrong reason.

The time window

TRAP 1

“Share of systems at current patch level” is not a measure until it is settled **when** you count: a cut-off date, a monthly average, or a rolling thirty days. The same estate yields three different percentages. All three are correct. None is comparable to the others, and nobody notices.

The counting unit

TRAP 2

Numerator and denominator must count the same unit, matched on the same identifier. Provider A delivers nine cloud services under a current contract; provider B delivers one under a stale contract. **Provider-based** currency is 1/2 = 50 %. **Service-based** currency is 9/10 = 90 %. Both are legitimate. Neither is a version of the other — and whoever swaps them reports an improvement that did not happen.

Same data, two verdicts. The unit is fixed in writing before the first collection, not after the first result.

The zero that is not a zero

The other two traps are about meaning. These are the ones that reach the management review intact and do the damage there.

"0 %" can mean	What it actually is	How it is reported
Measured and genuinely zero	**A result**	0 %, with the population stated
The population does not exist here	**Not applicable**	not_applicable — neither 0 % nor 100 %, and never green
Nothing was collected	**Not assessed**	not_assessed — an admission, not a score
The population exists, no event fell in the window	**Not triggered**	not_triggered — the control was not exercised

Performance is not effectiveness

TRAP 4 — CLAUSE 7.2 AGAINST 7.3

"98 % of staff completed the training" is performance. Whether they act differently in a phishing test is effectiveness. Both are legitimate and they answer different questions. The failure mode is not measuring the wrong one — it is measuring only the first and calling it assurance. Every measure in the list is typed as one or the other, or both.

Do not copy a threshold

A band printed in a document written for someone else measures that someone else. It is the most-copied and least-defensible part of any measurement programme — which is why this list gives you the formulas and not the bands.

1

Measure first, band second

Take a baseline before you set a threshold. A band chosen before the first measurement is a wish; a band chosen after the first result is a negotiation.

2

Band the population you actually care about

One band across a mixed estate hides exactly the systems you built the measure for. Band by criticality class and report the classes separately.

3

Keep the acceptance rule apart from the target

The target says where you want to be. The acceptance rule says what counts as passing. They are not the same sentence, and confusing them is how a tolerance quietly becomes a target.

4

Test the threshold on the raw value

Round for display only. A result that passes or fails at the same printed figure depending on the rounding is not a measurement, it is a coin.

A ratio is only as honest as the rules behind it

One rule set, applied to every measure in the list, published with the results. Without it every number is arguable, and every argument is won by whoever is more senior.

Rule	What it means in practice
Window	State the period. Count each item once, by unique identifier.
Subset	For coverage and success ratios the numerator is a subset of the denominator population. Trends and non-normalised weighted totals are the exceptions, and they are marked where they occur.
Zero denominator	No population at all means not_applicable. A population with no event in the window means not_triggered. No data collected means not_assessed. None of the three is 0 % or 100 %, and none is green.
Rounding	Test the threshold on the raw value; round only for display.
Exceptions	Every exception carries a reason, an owner and an expiry date. An exception without an expiry is a decision nobody made.
Provenance	Separate what the standard states, what is your reading of it, and what is your own threshold. Three different things, three different labels.

What is in force, and how we cite it

Any statement about the status of a standard carries the date it was checked, because the answer changes without notice.

ISO/IEC 27004:2016 is the edition in force

SECOND EDITION · NO AMENDMENT, NO CORRIGENDUM PUBLISHED

Checked on 13 September 2026. A third edition is in development as ISO/IEC DIS 27004 and is **not published**. Work from the 2016 edition, and build your programme so that each measure carries a mapping line to ISO/IEC 27002:2022 — then a new edition means checking the mapping, not rebuilding the programme.

Annex B is informative

A CONFORMITY FACT, NOT A COPYRIGHT ARGUMENT

It offers measurement examples, not mandatory metrics. What is required is Clause 9.1: that you measure — not that you measure these. Any line reading “ISO requires 36 metrics” is false, and in an audit it costs credibility.

How we cite

OUR OWN EDITORIAL RULE

Construct numbers and clause references are citations. Every formula and every line of interpretation in this deck is CyberWerkSuite wording; we do not reproduce the text of the annex. For the standard itself you need your own copy, from ISO, IEC, DIN Media or your national standards body. The twelve CWS measures are ours and are marked as ours.

CWS
CYBERWERKSUITE

Measurement

From a metric to evidence

Clause 9.1 measurement, built into the system that produces the evidence — and taught to the people who have to run it.

YOU HAVE THE LIST. THE WORK IS WHAT COMES AFTER IT

Forty-eight formulas are the easy part. Setting the bands, agreeing the counting units and defending the numbers in the room is the work.

✓ **Certified ISMS Expert (CISE)**	Forty hours of ISO/IEC 27001:2022 implementation on your own organisation — gap analysis, ISO 27005 risk, the 93 controls, the SoA, then Clause 9.1 measurement and internal audit
✓ **Implementation and audit support**	We run the gap analysis, write the documents and define the measures with you — then sit beside you on the day of the audit
✓ **ISMSSuite**	Over 300 assessable controls on the 93 of Annex A, a living SoA, generated policies, a risk engine — and these measures feeding the management review

For people who have to produce evidence, not opinions

Talk to us · no charge for the intake call cyberwerksuite.com/trainings

OR RUN IT YOURSELF — STEP BY STEP

ISMSSuite cyberwerksuite.com

Assessment, SoA, policies, risk and **Clause 9.1 measurement** in one system.

Measure what you intend to change — and be able to show it.

CyberWerkSuite cyberwerksuite.com