MANAGEMENT GUIDE / 2027 EDITION

Demonstrable compliance in 2027

From complying to proving it, without adding complexity.

A management guide for board members, CISOs, IT managers, privacy officers and compliance officers

01

Policy

What applies, and why?

02

Access

Who may do what, and for how long?

03

Use

Does it work in daily practice?

04

Evidence

Can we show it today?

A 2027 regulatory calendar, a four-layer model, a self-assessment and a quarterly roadmap.

EXECUTIVE SUMMARY

In 2027, compliance is about evidence

Having a policy is no longer enough. Supervisors, auditors and customers want to know whether you can show that your measures work every day.

The Dutch Cybersecurity Act (Cyberbeveiligingswet, Cbw) and the Critical Entities Resilience Act (Wwke) both took effect on 15 August 2026. That makes 2027 the first full year in which the Dutch implementation of NIS2 and CER applies. DORA is now established practice in the financial sector. At the end of 2027, the AI Act's high-risk rules and the main obligations of the Cyber Resilience Act follow.[1][3][4][5]

At their core, all these frameworks ask the same question: can you demonstrate who had access, what was shared, which policy applied and when action was taken? This guide helps you answer that question without extra bureaucracy. Start with five decisions.

Decision	What you record
Scope	Which laws apply to your organisation, and to which services and supply chain partners.
Ownership	One owner per control, with a mandate and a fixed place on the board agenda.
Backbone	One GRC or ISMS environment where policy, risks, controls and evidence come together.
Exchange	One fixed, controlled route for sharing sensitive information with external parties.
Evidence rhythm	How often you test effectiveness, and how quickly evidence must be available to an auditor.

In this guide

01 The issue 02
02 What changes in 2027 03
03 The compliance paradox 04
04 Complexity and shadow IT 05
05 Policy 06
06 Access 07
07 Use 08
08 Evidence 09
09 The evidence chain 10
10 Self-assessment 11
11 Roadmap 2027 12
12 The role of Msafe 13

Reading guide: board members read pages 1 to 5 and the roadmap on page 12. The worksheet on page 11 is intended for the owner of a document flow.

01 / THE ISSUE

From complying to proving it

The core question is shifting. No longer "do we comply?", but "can we show that every day, with objective evidence?".

What is demonstrable compliance?

Demonstrable compliance is the extent to which an organisation can show, with objective evidence, that its measures work. The question is not whether a policy exists, but whether you can reconstruct what happened: which control applied, who had access, which action was taken and with what result.

That evidence consists of logs, audit trails, reports and recorded decisions. The more of it is created automatically in daily work, the less time you spend collecting it afterwards.

Why it is a board issue

The Dutch Cybersecurity Act explicitly places final responsibility with the board. Board members must approve the measures, oversee their implementation and complete training themselves.[1] DORA takes a similar line for financial institutions.[3]

Evidence is therefore no longer a task for IT or compliance alone. The board must be able to explain which risks it accepts, and why.

Who asks for evidence

Evidence is not only for the supervisor. Customers, insurers and supply chain partners increasingly ask for it too, for example in tenders and supplier assessments. Organisations with their evidence in order also save time in sales.

Who asks	Typical question	Evidence that convinces
Supervisor	Are the measures appropriate, and do they work?	Risk analysis, decisions, test results and incident files.
Auditor	Does this control work over the whole period?	Logs and reports per control, with date and owner.
Customer or partner	How do you handle our data?	Certification, processing agreements and an audit trail per transfer.
Board	Which residual risk do we accept?	A current overview per control, with open items and decisions.

02 / REGULATION AND TIMELINE

What changes in 2027

2027 is not a year of new laws, but of testing. The rules are in place. Now the question is whether they work in practice.

15 Aug 2026
IN FORCE

Dutch Cybersecurity Act and Critical Entities Resilience Act. Registration with the NCSC is mandatory.[1][2]

11 Sep 2026
IN FORCE

Cyber Resilience Act reporting obligation for manufacturers of products with digital elements.[5]

2 Dec 2027
SCHEDULED

AI Act: obligations for stand-alone high-risk AI systems (Annex III).[4]

11 Dec 2027
SCHEDULED

Cyber Resilience Act: most obligations start to apply.[5]

Framework	Status November 2026	What you must be able to show in 2027
Cbw (NIS2)	In force since 15 August 2026 for over 8,000 organisations in 18 sectors.[1]	Duty of care in practice, timely reporting (24 hours, 72 hours, final report within one month) and board involvement.[13]
Wwke (CER)	In force since 15 August 2026; around 500 organisations are designated as critical entities.[1]	Resilience of services, including physical and supply chain resilience.
DORA	Applicable since 17 January 2025 in the financial sector.[3]	ICT risk management, incident reporting, resilience testing and control over ICT service providers.
AI Act	Transparency obligations apply; high-risk rules postponed by the Digital Omnibus.[4]	A register of AI applications and preparation for 2 December 2027 (Annex III) and 2 August 2028 (Annex I).
CRA	Reporting obligation since 11 September 2026.[5]	In procurement: requirements for suppliers of software and connected products.
GDPR	Remains the basis for all processing of personal data.[6]	Accountability: appropriate security and a complete record of processing activities.

Reference date 2 November 2026. Check the current state of laws and regulations before making decisions. This guide is not legal advice.

03 / THE COMPLIANCE PARADOX

More reporting, less resilience

The pitfall of stricter rules is that organisations respond with more documents and more complex processes. That does not make them safer, only slower.

> "You can't innovate in an organisation that spends all its time avoiding tomorrow's fine. We've forgotten that compliance is meant to make us better, not just safer."
>
> THIJS VAN DER LINDEN, COO OF MSAFE

The boardroom mechanism

Avoiding loss weighs more heavily than the ambition to win. Fines, data breaches and reputational damage are concrete. Under NIS2, fines for essential entities can reach 10 million euros or 2% of worldwide annual turnover.[13] Innovation, by contrast, feels uncertain.

The result is a culture of risk avoidance instead of risk management. A digital form of bureaucracy emerges: processes that mainly exist to prove that they exist.

What goes wrong

- Attention shifts from detection to documentation.
- New technology gets stuck in the pilot phase.
- Budget goes to audits instead of prevention.
- Employees look for workarounds around processes that are too heavy.

The lesson from security

A system can be fully compliant and still vulnerable. Following rules is necessary, but not sufficient. Security teams therefore steer on effectiveness, not on documents. That principle works for compliance too.

KPMG's Chief Ethics and Compliance Officer Survey shows that compliance officers at large Dutch companies expect more supervision, with data quality, privacy and cybersecurity at the top of their agenda.[11]

Decision question: which report in your organisation only exists because it always has, and which evidence is created naturally in the work?

04 / COMPLEXITY AND SHADOW IT

Make the secure route the easiest one

Compliance rarely fails because there is no policy. It fails because policy becomes too complicated in practice.

62%

of the breaches studied involved a human element, such as an error, misuse or social engineering.

Verizon DBIR 2026[8]

£750,000

fine for the Police Service of Northern Ireland, after the accidental publication of data on 9,483 officers and staff.

ICO, October 2024[9]

How shadow IT emerges

As soon as employees have to work with cumbersome processes, extra steps and separate portals, they look for a faster route. A private cloud, an unmanaged link or a free transfer service feels efficient. The organisation loses sight of access, logging and retention periods. The UK NCSC therefore explicitly names shadow IT as a risk.[10]

People are not the problem

The high share of human action does not mean employees are the problem. It means that processes requiring perfect human behaviour remain vulnerable. In the PSNI incident, the data sat in a hidden tab of a spreadsheet. The regulator stressed that simple procedures could have prevented the incident.[9]

What boards can do

- Measure how many steps the secure route takes, and compare it with the insecure one.
- Ask departments which tools they use outside IT, without sanctions.
- Only prohibit once an equally easy alternative is in place.
- Link awareness to the process, not to an annual e-learning.

Decision question: if an employee has to share a large file with an external party today, which route will they really choose?

05 / LAYER 1: POLICY

Start with the purpose of the control

Policy only works when it is measurable. Not the checklist, but the reason behind a control determines its impact.

Record policy, risk register, controls and owners in one GRC or ISMS environment. Map your controls to frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework. That way one set of measures covers several laws, instead of building separate administration for each law.[7]

For each control, define three things: the purpose, the standard and the evidence. A control without a definition of evidence is an intention. A control without a purpose becomes a checkbox.

Make classification usable

A classification with eight levels will not be used. Three or four levels, each with a concrete sharing rule, work better than a perfect scheme nobody knows.

Make exceptions temporary

Every exception gets an owner, a reason and an end date. A permanent exception is in effect new policy, and should be decided as such.

Decision question	What you record	Evidence
Which information is critical?	Classification with up to four levels and examples per level.	Published guideline and periodic sample check.
How long do we retain it?	Retention periods per type of information and per route.	Automatic deletion and a log entry per deletion.
What must not leave?	Excluded file types and data, with an exception process.	Technical block and register of exceptions.
Who decides when in doubt?	Information owner per domain, with a deputy.	Recorded decisions with date and rationale.

Tip: use fixed IDs per control (for example POL-03) across all your systems. That lets you trace every log entry directly to the measure it belongs to.

06 / LAYER 2: ACCESS

Let access rights move with people

Access that is no longer needed should expire automatically. Manual revocation almost always gets forgotten in practice.

Decide who may access which information, internally and externally. Single Sign-On and MFA are the standard. With automatic provisioning via SCIM, accounts are created, changed and removed as soon as someone joins, changes role or leaves.

The same principle applies to external recipients: access belongs to a purpose and a term, not to a person indefinitely.

Verify the recipient

A wrong email address is one of the most common causes of data breaches. An extra verification step for the recipient, such as a code sent to their phone, makes the difference between a mistake and an incident.

Test the expiry

Check not only whether access is granted, but also whether it expires. A sample of expired links and departed employees provides strong evidence.

Moment	Measure	Evidence
Joiner	Account via SSO and SCIM, rights based on role.	Provisioning log with date and role.
Mover	Old rights expire on a change of role.	Change log and periodic access review.
Leaver	Account blocked within the agreed period.	Deprovisioning log and sample check.
External recipient	Verification, expiry date and revocable access.	Audit trail per transfer and per recipient.
Administrator	Separate admin accounts with MFA and logging.	Admin log and quarterly review.

07 / LAYER 3: USE

Choose the route by control need

This is where most risks arise: in daily collaboration with customers, suppliers, auditors and supply chain partners.

Every route has its own strength. Email suits communication, a collaboration platform suits internal work. Sharing sensitive information with external parties requires a route that manages access, term and logging centrally.

Choose ways of working that fit seamlessly into daily work. If an employee can share securely from their own email client, they have no reason to fall back on an attachment or a free service.

Don't make large files the exception

Construction drawings, medical images and due diligence files are often too large for email. That is exactly where workarounds arise. Make sure the secure route handles large files too.

Train recognisable trade-offs

Practise with real situations: a request from an unknown address, an auditor in a hurry, a file with special categories of personal data. That works better than general rules.

Route	Primary use	Control question
Email attachment	Communication, copy in mailbox	What happens after sending, and who forwards it?
Collaboration platform	Working on documents together	Who keeps track of guest access, and for how long?
Secure file transfer	Sensitive exchange with external parties	Which expiry date, verification and audit trail apply?
Free transfer service	Not approved	Why did employees choose this route, and what was missing?

Decision question: which document flows with external parties currently run through a route that leaves you no evidence afterwards?

08 / LAYER 4: EVIDENCE

From log entry to usable file

An audit trail only has value when the incident team or the auditor can use it to reconstruct the transfer.

Make sure every relevant action automatically leaves a trace: who sent what, to whom, when it was opened and when access expired. Make that evidence exportable to your SIEM or GRC environment, so it does not stay stuck in separate systems.

Decide in advance which questions you want to be able to answer within an hour. That forces choices about logging, retention and access to the logs themselves.

Practise reconstruction

Choose one fictitious transfer and reconstruct it with the incident team. Whatever is missing becomes an improvement item with an owner.

Keep reporting deadlines achievable

Under NIS2, significant incidents require an early warning within 24 hours. Under the GDPR, you report a personal data breach within 72 hours. Fast evidence is the difference between a substantiated report and an estimate.[6][13]

Time	Fictitious exercise file EX-2027-01
09:00	An employee shares a file with an external adviser, with verification and expiry date.
09:04	The recipient verifies and downloads the file.
11:30	The employee reports that an attachment was not intended for this recipient.
11:34	Access revoked; the audit trail shows one download at 09:04.
12:15	The privacy officer assesses the reporting obligation based on the export file.

Exercise scenario, not a customer case.

09 / THE EVIDENCE CHAIN

One measure, multiple frameworks

Organising evidence per law creates double work. Organising evidence per control answers several laws at once.

A usable line of evidence always follows the same chain:

Obligation
What does the law or customer require?

Risk
What can go wrong?

Measure
Which control limits it?

Effectiveness
Has the control been tested?

Evidence
Where is the trail?

Decision
Who accepts the residual risk?

Example: external file transfer

Measure	Supports, among others	Evidence
Encrypted transfer with recipient verification	GDPR Art. 32, Cbw duty of care, ISO/IEC 27001 A.5.14	Configuration and audit trail per transfer.
Role-based and time-bound access	ISO/IEC 27001 A.5.15 and A.5.18, DORA ICT risk management	Provisioning logs and expired links.
Logging of all actions	ISO/IEC 27001 A.8.15, Cbw reporting obligation, GDPR Art. 5(2)	Exportable logs per file and recipient.
Central retention periods	GDPR storage limitation, sector-specific retention duties	Policy setting and deletion log.

Indicative mapping for illustration. The correct mapping depends on your scope and risk analysis.[6][7]

How to work with the chain

Start with the measure, not the law. Record which obligations each measure supports, and refer to the same control from every framework. When a law changes, you update the reference instead of building a new process.

Let the chain end with a decision. A gap in the evidence is not a disaster, as long as someone with a mandate consciously accepts the residual risk or schedules an improvement. That decision is evidence too.

10 / SELF-ASSESSMENT

What can you demonstrate today?

Use the worksheet for one document flow. An unknown answer is an item to investigate, not a pass.

Mark each criterion: A = in place and tested; B = in place, effectiveness not yet sufficiently demonstrated; C = missing or unknown. Record the evidence reference, owner and follow-up date in your management file.

Control point	A	B	C
1. The applicable laws and their 2027 deadlines have been established.	○	○	○
2. Every control has an owner, a purpose and a definition of evidence.	○	○	○
3. The board has approved the measures and completed training.	○	○	○
4. Joiner, mover and leaver processes for accounts run automatically.	○	○	○
5. External access always has an expiry date and can be revoked.	○	○	○
6. There is one approved route for sensitive exchange with external parties.	○	○	○
7. Every external transfer can be reconstructed with an audit trail.	○	○	○
8. Reporting processes meet the 24 and 72 hour deadlines and have been practised.	○	○	○
9. Suppliers have been assessed on security, location and logging.	○	○	○
10. Evidence for an auditor is available within one working day.	○	○	○

Don't use a total score as reassurance

Set priorities based on risk and dependencies. A single C on point 7 can weigh more than three Bs elsewhere. Agree in advance which shortcomings are critical and who may accept a residual risk.

Document flow / owner / date

Own worksheet for internal management. This is not a validated audit, legal standard or statement of compliance.

11 / ROADMAP 2027

Four quarters to demonstrable

Start small enough to learn and concrete enough to assess the outcome. Round off the year before the December deadlines.

Q1

Define

Scope and baseline

- Establish which laws apply and their deadlines.
- Choose one critical document flow.
- Complete the worksheet on page 11.
- Appoint owners per control.

Q2

Set up

Route and controls

- Set up one approved route for external exchange.
- Automate SSO, MFA and SCIM.
- Set retention periods and expiry dates centrally.
- Train on recognisable situations.

Q3

Test

Effectiveness and evidence

- Reconstruct a fictitious transfer.
- Practise the 24 and 72 hour deadlines.
- Connect logs to your GRC environment.
- Assess suppliers, including CRA requirements.

Q4

Embed

Decision and scale-up

- Discuss the results with the board.
- Record residual risks with an owner.
- Check AI registration before 2 December.
- Extend to the next document flow.

Make the decision explicit each quarter

Close each quarter with a short decision: what is in place, what has been tested, what remains open and who owns it. Over the year, this builds a file that an auditor or supervisor can review without extra work.

Keep the scope manageable. One well-substantiated document flow says more about your maturity than ten half-finished ones. Then use the experience to scale up faster.

Own organisational model for inspiration. Adjust the order to your risks and the deadlines that apply to your sector.

File transfer as a demonstrable measure

Secure file transfer is not a separate IT topic. It is where sensitive documents leave the organisation, and therefore where evidence is needed most.

Msafe Secure File Transfer is built for sharing sensitive files securely with external parties. Employees share from Outlook with the Msafe Connector or in the web application. Recipients collect files with Easy Download: after a one-time verification via their phone number, without an account. Files up to 1 TB are standard, larger on request.[12]

Msafe is certified to ISO/IEC 27001:2022 and hosted in the Netherlands. A tool never makes an organisation compliant automatically: that also takes policy, risk analysis and processes. Msafe provides the controls and the evidence for the exchange route.

Layer	What Msafe supports	What you arrange yourself
Policy	Central retention periods, expiry dates and excluded file types.	Classification, information owners and exceptions.
Access	Single Sign-On via Microsoft Entra ID, SCIM, MFA, recipient verification and revocable access.	Roles, access reviews and leaver process.
Use	Sharing from Outlook, shared spaces where everyone sees what happens to a document, large files.	Working agreements and training per department.
Evidence	Full audit trail per file and recipient, exportable reports and an API.	Integration with GRC or SIEM and the testing rhythm.

Test your own document flow

Book a demo or proof of concept with one document flow from this guide. We will show which evidence you can present to an auditor straight away. **msafe.co/request-a-demo**

Product information provided by Msafe B.V., reference date November 2026. Features and terms may change.

SOURCES AND ACCOUNTABILITY

Background and further reading

Reference date: 2 November 2026. Legislation, supervision and official guidance may change after this date.

This guide provides general information for board members and specialists. The self-assessment model, exercise file and roadmap are Msafe's own working models, not legal standards or validated audits.

Have the application of laws and regulations to your organisation reviewed by your own legal or compliance function. Figures come from the public sources listed.

[1] Dutch government (Rijksoverheid)
Cyberbeveiligingswet and Wet weerbaarheid kritieke entiteiten in force from 15 August 2026, 7 July 2026.

[2] NCSC (Netherlands)
Registration in the entity register via mijn.ncsc.nl.

[3] DORA
Regulation (EU) 2022/2554, applicable since 17 January 2025.

[4] AI Act
Regulation (EU) 2024/1689, amended by the Digital Omnibus on AI (2026): Annex III from 2 December 2027, Annex I from 2 August 2028.

[5] Cyber Resilience Act
Regulation (EU) 2024/2847: reporting obligation from 11 September 2026, most obligations from 11 December 2027.

[6] GDPR
Regulation (EU) 2016/679, Art. 5(2), Art. 32 and Art. 33.

[7] ISO/IEC 27001:2022
Annex A, controls 5.14, 5.15, 5.18 and 8.15.

[8] Verizon
Data Breach Investigations Report 2026.

[9] ICO
£750,000 fine for the Police Service of Northern Ireland, October 2024.

[10] NCSC (United Kingdom)
Shadow IT: guidance.

[11] KPMG
Chief Ethics and Compliance Officer Survey 2025.

[12] Msafe
Product information Msafe Secure File Transfer, November 2026.

[13] NIS2 Directive
Directive (EU) 2022/2555, Art. 23 (reporting deadlines) and Art. 34 (fines).

Msafe B.V.
Linnaeusweg 9a
IJsselstein, the Netherlands

+31 88 88 53 010
info@msafe.co
msafe.co

Published by Msafe B.V. | 2027 edition | © 2026 Msafe B.V. All rights reserved.