The CISO in Practice

A workbook for boards, supervisors and security leaders — European edition

Content

Preface and reading guide 2

Editorial framework 2

Preface and reading guide 5

Chapter 1 — The CISO role: definition and foundations 6

Chapter 2 — What a CISO does: the task landscape 14

Chapter 3 — Core tasks in practice I: steering and setting the framework 21

Chapter 4 — Core tasks in practice II: organising resilience 31

Chapter 5 — What a CISO must be able to do 47

Chapter 6 — What the board may expect 54

Chapter 7 — Positioning in the governance structure 60

Chapter 8 — Mandate and independence 66

Chapter 9 — Organisation, team building and span of control 73

Chapter 10 — Tasks that do not belong with the CISO 80

Chapter 11 — Remuneration: market indications in Europe 84

Chapter 12 — The CISO and stakeholders 89

Chapter 13 — The relationship with the board: the board compact 94

Chapter 14 — Profile and perception: partner rather than obstacle 99

Chapter 15 — Common mistakes and anti-patterns 104

Chapter 16 — Professional associations and networks in Europe 109

Chapter 17 — The workbook toolkit 113

Chapter 18 — Four 90-day plans 124

Appendix A — Glossary 130

Appendix B — Regulatory overview: NIS2, DORA and national transposition 132

Appendix C — Standards and frameworks 134

Appendix D — Sources and further reading 136

Preface and reading guide

Editorial framework

This framework sets out who the book is for, how it speaks and how it deals with certainty. It applies to every chapter.

Audience and reading routes

Reader	What they are looking for	Suggested route
Executive board member	What do I expect, what do I provide, how do I steer?	Ch. 1, 6, 7, 8, 13, 17.2
Supervisory board or audit committee member	How do I test whether security is properly anchored?	Ch. 1, 6, 7, 8, 15, 17.2
Aspiring CISO	Am I ready, what lies ahead?	Ch. 1–5, 17.1, 18.2
Serving CISO	How do I become more effective and better positioned?	Ch. 3–4, 8, 12–15, 17
Security manager	How do I grow into the CISO role?	Ch. 2–5, 9, 17.1

Language, tone and terminology

- British English, as is common in European professional publishing.
- Businesslike, direct and accessible. Short sentences, active voice.
- No marketing language (“game-changer”, “best-in-class”) and no empty jargon.
- European governance differs between countries. This book uses neutral terms:

Term in this book	Meaning	Examples across Europe
Board	The highest executive body	Executive board, management board, *Vorstand*, *directie*, executive committee
Supervisory body	The body that supervises the board	Supervisory board, *Aufsichtsrat*, *raad van commissarissen*, non-executive directors in a one-tier board, audit committee
Regulator	External supervisory authority	National cybersecurity authority, sector regulator, data protection authority

Term in this book	Meaning	Examples across Europe
Works council	Employee representation with consultation or consent rights	*Betriebsrat*, *ondernemingsraad*, *CSE*; rights differ by country

Labels for certainty

Label	Meaning	Example
Requirement	Follows from law, regulation or a widely accepted standard	Under NIS2, the management body approves cybersecurity risk-management measures and oversees their implementation
Good practice	Broad professional consensus, not mandatory	The CISO has a direct escalation line to the board
Context	The right choice depends on size, sector or maturity	A CISO reporting to the CIO can work in a small, IT-driven organization
Advice	The author's reasoned view	Put the mandate in writing before the first working day

Organization size and sectors

Category	Employees (indicative, aligned with the EU SME definition)	Typical CISO arrangement
Small	10–49	Shared or virtual CISO, a few days a month
Medium-sized	50–249	Part-time or full-time CISO, 0–2 FTE team
Large	250–5,000	Full-time CISO with own team and functional line to IT
Multinational or heavily regulated	> 5,000 or under intensive supervision	CISO function with divisional or country CISOs

Sectors with distinct emphasis: **public sector** (political accountability, national baselines), **healthcare** (patient safety, availability, national healthcare standards), **finance** (DORA, prudential supervision), **industry** (OT security, safety, supply chains) and **commercial/tech** (speed, product security, customer assurance).

The European legal frame

NIS2 (Directive (EU) 2022/2555) makes cybersecurity an explicit responsibility of the management body. Member states had to transpose it by 17 October 2024; transposition progressed unevenly, and several

member states adopted their laws later. The examples in this book come mainly from the Netherlands and Belgium:

Country	Law	Status
Netherlands	Cybersecurity Act (*Cyberbeveiligingswet*) and Cybersecurity Decree	In force since 15 August 2026
Belgium	NIS2 Act of 26 April 2024	In force since 18 October 2024; CyberFundamentals as reference framework
Other member states	National transposition laws	Check the current status with the national cybersecurity authority

DORA (Regulation (EU) 2022/2554) has applied to the financial sector since 17 January 2025 and takes precedence over NIS2 for financial entities. Appendix B gives an overview.

What differs from the Dutch edition

Topic	Dutch edition	European edition
Legal frame	Dutch and Belgian law	NIS2 and DORA as common frame; NL and BE as worked examples; pointers for other member states
Governance terms	Dutch structures (RvB, RvT, OR)	Neutral terms covering one-tier and two-tier boards
Remuneration	Dutch and Belgian vacancy data	Same anchors, plus factors that explain differences between countries; no figures where data is lacking
Networks	Dutch and Belgian associations	European bodies plus national examples
Sector standards	BIO2, NEN 7510	Presented as examples of national baselines

Sources and currency

- Legislation, remuneration figures and association data carry a source and a reference date. Reference date: 5 October 2026.
- Remuneration figures are **market indications**: always a range, never a single figure.

- Practice examples are composites of recognizable situations; organization's are fictional unless a public source is cited.
- Where practice differs by country or sector, the text says so.

Preface and reading guide

This workbook is about a role that many organization's are still trying to place. Almost every organization of any size now has someone with the title CISO, yet what that person may do, must do and is able to do varies widely. Since NIS2, cybersecurity has also become an explicit responsibility of the board across the European Union. The position of the CISO is therefore no longer an internal matter. It is a governance matter.

The book is written from practice. It does not explain how a firewall works. It explains how a CISO makes sure an organization genuinely governs its information risks: with a clear mandate, honest information for the board, good relationships with the line, and without becoming the person who makes everyone else's work harder.

This European edition is based on the Dutch original. The examples remain largely Dutch and Belgian, because that is where the author's experience lies, but the framework is European: NIS2 and DORA apply in every member state, and the questions of mandate, position and influence are the same from Lisbon to Helsinki.

Who this book is for

- **Board members and supervisory body members** who want to know what they may expect from a CISO, and what the CISO needs from them.
- **Aspiring CISOs and security managers** who want to know what the role demands and whether they are ready.
- **Serving CISOs** who want to strengthen their position, mandate and effectiveness.

The suggested reading routes per audience are in the editorial framework.

How the book is structured

Part I describes the role, the tasks and the skills. Part II covers governance: expectations, position, mandate, organization, boundaries and remuneration. Part III deals with relationships, influence and perception, including common mistakes and professional networks. Part IV contains the toolkit and four 90-day plans. Four appendices provide a glossary, a regulatory overview, a list of standards and the sources.

Every chapter closes with a workbook section: summary, reflection questions, checklist, practical exercises, template, and dos and don'ts. Readers who use the book as a workbook can get to work chapter by chapter.

How the book deals with certainty

Recommendations are labelled where useful as **Requirement**, **Good practice**, **Context** or **Advice**. Legislation and remuneration figures carry a source and reference date. Where public data is lacking, the text says so and marks any estimate as such.

Reference date

The content is current to 5 October 2026. Legislation, standards and labour-market data change; Appendix D lists what should be checked again for a new printing.

Chapter 1 — The CISO role: definition and foundations

Part I — Foundations and craft

The CISO is the officer who, on behalf of the board, makes information security governable: risks visible, choices explicit, measures assigned and effectiveness demonstrable. The CISO is therefore not the owner of all security, but of the question whether the organization governs its security well.

1.1 What a CISO is — and is not

Working definition (Advice). The Chief Information Security Officer is the most senior officer for information security, who advises the board on information risk, sets and monitors the security framework, coordinates and tests its implementation by the line, and reports independently on the state of security and residual risk.

Four elements of this definition shape the rest of the book:

1. **On behalf of the board.** The CISO derives authority from the board, not from IT. Without that anchoring, the role is a title without effect.
2. **Setting and monitoring the framework.** The CISO decides *what* is good enough; the line decides how and implements.
3. **Coordinating and testing.** The CISO often steers functionally, not hierarchically. Influence is the main instrument.
4. **Reporting independently.** The CISO must be able to deliver uncomfortable news without the line manager being able to stop it.

What a CISO is not (Good practice):

- Not the most senior system administrator or the “firewall boss”.
- Not the person who personally accepts every risk. Risk acceptance belongs to the owner of the process or system.
- Not the internal auditor. The CISO tests in order to steer; internal audit tests independently of steering.
- Not a guarantee that incidents will not happen. Complete prevention does not exist; see the limits of control in 1.6.

The title versus the role. In practice, people with very different tasks carry the title CISO. A “CISO” at a 60-person company who also manages the firewall does something different from a CISO at a bank with an 80-person department. This book therefore assesses the **role** (what someone does and may do), not the title.

1.2 Strategic, tactical and operational

The CISO role operates on three levels. The balance shifts with organization size, but a CISO who spends more than half of their time on operational work is in effect performing a different role.

Level	Key question	Typical activities	Output	Time allocation small / medium / large (indicative)
Strategic	Which risks do we accept, and where do we invest?	Strategy, risk appetite, board advice, positioning, regulators	Security strategy, board report, risk appetite statement	20% / 35% / 50%
Tactical	How do we translate strategy into programmes and frameworks?	Policy, control framework, roadmap, budget, metrics, supplier policy, architecture principles	Policy, roadmap, KPI/KRI set, annual plan	35% / 40% / 35%
Operational	Does it work, and what is happening now?	Incident coordination, risk assessments, reviews, project advice, awareness delivery	Incident report, risk analysis, advice, test results	45% / 25% / 15%

Context. In a small organization, operational work is unavoidable. That is acceptable as long as the CISO deliberately reserves strategic time and the board knows that operational involvement limits independence.

Practice examples

- *Small (35 employees, accountancy firm).* A virtual CISO works four days a month. One day per quarter is reserved for the management team and risk appetite; the rest goes to MFA roll-out, supplier questions and a phishing exercise.
- *Medium-sized (180 employees, logistics).* The CISO attends the weekly IT meeting (tactical), the monthly management meeting (strategic), and temporarily coordinates incidents (operational) before an external SOC partner takes over.
- *Large (3,000 employees, municipality).* The CISO leaves operational work to a security manager and the SOC, and spends half of their time on the executive, the municipal secretary, chain partners and accountability under the national public-sector baseline.

1.3 The CISO alongside related roles

Confusion between roles is the most common cause of “responsibility without authority”. The table shows the typical demarcation (**Good practice**; titles and arrangements vary).

Role	Core responsibility	Line (three lines)	Relationship to the CISO
CISO	Governability of information security: framework, advice, testing, reporting	2nd line (sometimes hybrid)	—
Security manager	Running the security programme and operational security tasks	1st or 2nd line, depending on design	Often reports to or deputizes for the CISO
SOC manager	Detection, monitoring and first response	1st line	Operational; supplies data for KPIs and incident information
IT manager	Availability and management of IT services, including technical controls	1st line	Owner of many controls the CISO tests
CIO	Information provision and IT strategy	1st line (executive)	Key partner; potential conflict of interest if a hierarchical line exists
Risk manager / CRO	Enterprise risk management across all risk types	2nd line	Sets the methodology; CISO contributes information risk
Compliance officer	Compliance with laws, regulations and internal rules	2nd line	Overlap on NIS2, DORA, GDPR; agreements needed
DPO	Monitoring GDPR compliance, independent by law	2nd line (statutory position)	Close cooperation; the DPO may not be instructed by those who determine the processing
Internal audit	Independent testing of design, existence and operation	3rd line	Also tests the CISO function

Sector differences

- **Finance (Requirement/Good practice):** supervisors generally expect a clear second-line information security function, separate from IT. DORA reinforces that expectation.

- **Public sector:** the CISO often works alongside a CIO or information manager. National baselines (for example BIO2 in the Netherlands) require a designated responsible officer and accountability towards the executive and elected bodies.
- **Healthcare:** national healthcare security standards (for example NEN 7510 in the Netherlands) require demonstrably assigned responsibility. Smaller institutions often combine CISO and privacy roles, with the risk of an overly broad remit (see Chapter 10).
- **Industry:** OT security often sits with engineering or operations. The CISO needs functional authority over the framework without taking over safety responsibility.
- **Commercial/tech:** product security often sits with the CTO; the CISO sets the framework and tests.

1.4 Responsibility, accountability, mandate and ownership

Four concepts are often used interchangeably. Without separating them, you get a CISO who is held to account for everything and decides nothing.

Concept	Definition	Question it answers	Example
Responsibility	The duty to carry out a task	Who does it?	IT operations patches the servers
Accountability	The duty to answer for the result, even when others carry it out	Who is held to account?	The CIO answers for the patch backlog
Mandate	The formal authority to decide, instruct or escalate	Who may decide?	The CISO may have an internet-facing system without MFA disconnected in case of acute risk
Ownership	The role that decides on an asset, process or risk and bears the consequences	Whose is it?	The director of care is owner of the EHR risk and accepts residual risk

Key rule (Good practice). Accountability requires a mandate. Holding someone accountable for an outcome they may not decide on is not governance but risk-shifting.

How it is usually assigned well

- The **board** is ultimately accountable for information security as a whole (**Requirement** under NIS2 for entities in scope).
- **Process and system owners** own their risks and accept residual risk within the risk appetite.
- **IT and other implementers** are responsible for implementing and maintaining controls.
- The **CISO** is accountable for the quality of the framework, the accuracy and timeliness of risk information, and timely escalation. The CISO is *not* accountable for the absence of incidents.

Example of misassignment. After a ransomware incident, the supervisory board asks why "the CISO did not prevent this". The records show the CISO reported the outdated VPN environment three times as a high risk, that replacement was postponed twice, and that nobody formally accepted the risk. The failure lies in governance, not with the CISO. The lesson: always record risk acceptance with an owner, by name and date.

1.5 The three lines and the tension between advice and assurance

The three lines model (IIA, revised in 2020 as the "Three Lines Model") distinguishes execution, support and oversight, and independent assurance.

Line	Role	Who (security context)	Typical CISO relationship
1st line	Owns and manages risks in daily operations	Business, IT, OT, development, supplier management	The CISO advises, supports and sets requirements
2nd line	Sets frameworks, supports, monitors and challenges	CISO, risk management, compliance, DPO	Position of the CISO in most mature models
3rd line	Independently tests design and operation of 1st and 2nd lines	Internal audit, external audit	Also tests the CISO function

Where the CISO stands. In mature and regulated organizations, the CISO sits in the second line (**Good practice**; in finance often a **Requirement** in supervisory practice). In smaller organizations the CISO is often hybrid: advising, setting frameworks and also implementing. That works as long as the board knows where independence ends.

The tension between advice and assurance. The CISO must be both partner and tester. That is not a design flaw, but it requires conscious switching.

Aspect	Advisory role	Assurance role
Purpose	Help make a good choice	Establish whether the choice and its implementation meet requirements
Attitude	Engaged, solution-oriented	Independent, critical, factual
Timing	Beforehand and during	Afterwards and periodically
Risk when overdone	Co-designing the solution, then testing your own work	Being seen as the police, being excluded

Handling the tension (Advice)

1. Make explicit which role you are in: "I'm advising now; in Q3 I will test how it works."

2. Do not design solutions you will later have to approve. Provide requirements and criteria; let the line make the design.
3. Have the operation of critical controls also tested by the third line or an external party, especially where you advised.
4. Leave risk acceptance with the owner; the CISO advises on acceptance but does not sign.

Practice examples

- *Medium-sized (care provider, 900 employees).* The CISO advises on the procurement of a new rostering system and provides a set of requirements. At delivery, the CISO commissions an external penetration test instead of testing himself, because he was closely involved in the design.
- *Large (insurer).* The first line has its own business information security officer per division; the second-line CISO sets the framework and tests by sampling. Internal audit annually audits the ISMS, including the CISO function.
- *Small (software company, 40 employees).* The CTO is also the CISO. The board has an external party carrying out an annual review, so there is still an independent view.

1.6 NIS2 as a board-level framework, and the limits of control

NIS2 places ultimate responsibility firmly with the management body. For entities in scope, the management body must approve the cybersecurity risk-management measures, oversee their implementation and have sufficient knowledge; members can be held liable (**Requirement**). Each member state implements this through its national law, for example the Dutch Cybersecurity Act since 15 August 2026 and the Belgian NIS2 Act since 18 October 2024.

For the CISO this means three things:

1. **The board has its own interest in a good CISO.** The CISO is the instrument through which board members fulfil their legal duty. That is a strong argument for mandate and access.
2. **The CISO cannot take over the board's responsibility.** The board can delegate but cannot shift ultimate responsibility. A CISO charter must not suggest otherwise.
3. **Board knowledge is a CISO task.** The CISO organizes board training and makes sure papers enable the board to genuinely assess, not merely sign.

The limits of control (Advice). A CISO can guarantee a clear framework, honest risk information, timely escalation and a prepared organization. A CISO cannot guarantee that no incident will occur, that suppliers will work flawlessly, or that others' budget decisions will turn out well. Failing to make this distinction turns the CISO into a scapegoat and gives the board false reassurance.

Workbook — Chapter 1

Summary

- The CISO makes information security governable on behalf of the board; the role sets frameworks, advises, coordinates and tests.
- The balance between strategic, tactical and operational work shifts with size; a structurally operational CISO is in effect doing a different job.

- Separate responsibility, accountability, mandate and ownership; accountability without mandate is unworkable.
- The CISO preferably sits in the second line; in small organizations a hybrid role works if it is deliberate and transparent.
- NIS2 makes the board ultimately responsible; the CISO makes that responsibility workable but cannot take it over.

Reflection questions

1. If you describe your role in one sentence, is it a title or a mandate from the board?
2. What percentage of your time went to operational work last month, and did the board choose that?
3. For your three largest risks, do you know exactly who the owner is and when residual risk was accepted?
4. In which current project are you both adviser and tester, and how do you safeguard that?
5. After a major incident, what would the board expect you to have done, and is that written down?

Checklist: is the role clearly defined?

- ☐ There is a written role description or CISO charter adopted by the board
- ☐ The CISO has a direct reporting or escalation line to the board
- ☐ Risk ownership is assigned by name for each critical process or system
- ☐ Risk acceptance is recorded in writing by the owner, not by the CISO
- ☐ The demarcation with CIO, risk, compliance, DPO and audit is recorded
- ☐ The board knows whether the CISO works in the second line or hybrid, and what that means
- ☐ The operation of controls is (also) tested by an independent party
- ☐ It has been established whether the organization is in scope of NIS2 and in which category

Practical exercises

1. **Time analysis (1 hour).** Classify your diary for the last four weeks as strategic, tactical or operational. Compare with the indication in 1.2 and discuss the gap with your line manager.
2. **Role demarcation (2 hours).** Complete the matrix below for your organization and review it with the CIO, risk manager and DPO.
3. **Ownership scan (half a day).** Take the ten largest information risks. For each, note the owner, the last acceptance date and who implements. Every empty cell is a governance action.
4. **NIS2 board test (1 hour).** Formulate three questions the board must be able to answer to meet its duty, and test whether current reporting provides those answers.

Template: role demarcation matrix

Topic	CISO	CIO / IT	Risk	Compliance	DPO	Internal audit	Business owner
Adopting the informatio	Drafts	Consulted	Consulted	Consulted	Consulted	Informed	Board adopts

Topic	CISO	CIO / IT	Risk	Compliance	DPO	Internal audit	Business owner
n security policy							
Risk methodology	Applies for information security	Informed	Sets framework	Consulted	Consulted	Informed	Informed
Risk acceptance	Advises	Consulted	Monitors framework	Informed	Consulted for personal data	Informed	Accepts
Implementing technical controls	Sets requirements, tests	Implements	—	—	—	Tests periodically	Informed
NIS2 incident notification	Coordinates content	Supplies data	Informed	Checks deadline and form	Consulted for data breach	Informed	Board informed
Testing ISMS operation	Monitors	Provides evidence	Informed	Consulted	—	Tests independently	Informed

Adapt names and roles to your organization; empty or duplicate "Accountable" cells are the topic for discussion.

Dos and don'ts

Do	Don't
Put role, mandate and escalation line in writing	Accept a title without the matching rights
State explicitly whether you are advising or testing	Design solutions you will later have to approve
Have risks accepted by the owner	Sign for risk acceptance yourself "because nobody else will"
Make the board aware of its NIS2 responsibility	Suggest the CISO takes that responsibility over
Reserve time for strategic work	Let operational firefighting fill your diary
State what you can and cannot guarantee	Promise an incident-free organization

Examples by organization size

Size	Typical arrangement	Main point of attention
Small	Virtual or shared CISO, or IT manager/CTO with CISO tasks	Ensure a minimal independent test, such as an annual external review
Medium-sized	Part-time or full-time CISO, hybrid 1st/2nd line	Record which operational tasks are temporary and when they move to IT
Large	Full-time second-line CISO with own team	Secure the functional line to first-line security and direct access to the board
Multinational / regulated	Group CISO with divisional or country CISOs	One framework, local room, and a clear relationship with regulators per country

Chapter 2 — What a CISO does: the task landscape

The CISO profession consists of fourteen core tasks, grouped into four clusters: steering, protecting, preparing and organizing. No CISO performs all fourteen with equal intensity; the art is to choose deliberately which tasks remove the most risk now, and to agree that with the board.

2.1 Fourteen core tasks at a glance

The column “CISO role” shows how the CISO relates to the task (**Good practice**):

- **Owner:** the CISO delivers the result and is accountable for it.
- **Framework-setting:** the CISO sets requirements and method; others implement.
- **Coordinating:** the CISO brings parties together and safeguards coherence.
- **Advisory:** the CISO provides input; someone else decides.

#	Core task	Cluster	Purpose	CISO role	Key output	Main stakeholders
1	Information security governance	Steering	Roles, decision-making and accountability are clearly assigned	Owner	Governance structure, CISO charter, meeting structure	Board, supervisory body, CIO, risk
2	Security	Steering	Multi-year direction	Owner	One-page strategy,	Board, CIO,