

Chief Information Security Officer

FF09 IT infrastructure, operations and security · ISCO-08 1330 · CBS 0533 ICT Managers · seniority lead
· Also known as: CISO, Head of Information Security

Holds ultimate responsibility for information security, sets policy and risk appetite and accounts for the security posture to board and supervisors.

The chief information security officer directs the security function of an organisation, allocates resources and decides which risks are accepted. Unlike the security officer, this role has mandate and budget, and unlike the IT director its primary charge is risk control rather than system availability. Selection weighs technical and standards knowledge heavily, while in practice the role fails on executive presence: a CISO must be able to force an investment through and communicate with directors and supervisors during a crisis without dressing up the facts.

Key figures for this profile

26 skills · 4 competencies to measure · 3 knockout skills · centre of gravity: Digital, data and AI 47%, Leadership and organising 20%, Cognitive ability and problem solving 10%

1 Competencies to measure

These are the behavioural and ability constructs in this profile. Each one shows which hrmforce questionnaire measures it.

Competencies to measure	Target level	hrmforce instrument	Assessment method	Behavioural anchor at target level
Accuracy and attention to detail Competency (50-framework): Accuracy	 N5	Big Fifty, 360 Feedback	Personality questionnaire	Sets the standards for completeness and correctness, has samples checked and addresses teams on structural sloppiness.

Competencies to measure	Target level	hrmforce instrument	Assessment method	Behavioural anchor at target level
integrity and dependability Competency (50-framework): Integrity	 N5	Big Fifty (Integrity Scale), 360 Feedback, Structured interview	Personality questionnaire	Sets the organisation's integrity standards, enforces them also with influential parties and explains the resulting choices publicly.
Discipline and keeping commitments Competency (50-framework): Discipline	 N5	Big Fifty, 15PF, 360 Feedback	Personality questionnaire	Anchors the standard for reliable follow through in working agreements and addresses anyone at any level who lets that standard slip.
Stress tolerance Competency (50-framework): Stress resilience	 N5	Big Fifty, 15PF, Mental Resilience (4C)	Personality questionnaire	Keeps the organisation workable in crises, takes decisions under high uncertainty and sets the standard for composed action under pressure.

2 Full skill profile

Every skill in this profile, sorted by weight. The behavioural anchor under each skill belongs to the target level.

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Problem analysis Traces persistent organisational problems back to a few root causes and sets the analysis method that other teams will use.	■■■■■ N5	5	yes	Assessment centre	Competency Check, Ability Scan
V	Strategic thinking Develops scenarios for the whole organisation, weighs uncertainties explicitly and sets the strategic agenda together with the executive board.	■■■■■ N5	5	no	Assessment centre	Ability Scan, Competency Check
K	Governance and compliance Draws up the governance framework of the organisation, defines mandates and oversight arrangements and accounts for compliance to external supervisors.	■■■■■ N5	5	no	Knowledge test	Knowledge test (client-specific)
V	Risk management Builds the risk framework of the organisation, sets risk appetite with the executive team and reports on it to the supervisory body.	■■■■■ N5	5	no	Knowledge test	Knowledge test (client-specific), Competency Check

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Access and identity management Sets the organisation's access policy and accounts for the control of permissions in audits.	■■■■■ N5	5	yes	Work sample test	Knowledge test (client-specific), Work sample test
V	Threat and risk analysis Independently performs a threat analysis on an application, prioritises risks and advises on measures with costs and effect.	■■■■■ N4	5	yes	Work sample test	Knowledge test (client-specific), Work sample test
G	Accuracy and attention to detail Sets the standards for completeness and correctness, has samples checked and addresses teams on structural sloppiness.	■■■■■ N5	4	no	Personality questionnaire	Big Fifty, 360 Feedback
G	integrity and dependability Sets the organisation's integrity standards, enforces them also with influential parties and explains the resulting choices publicly.	■■■■■ N5	4	no	Personality questionnaire	Big Fifty (Integrity Scale), 360 Feedback, Structured interview
V	Accounting to supervisors and stakeholders Accounts for organisational results and incidents to the supervisory board, media or politics and links visible policy adjustments to them.	■■■■■ N5	4	no	Assessment centre	Competency Check, 360 Feedback

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
G	Discipline and keeping commitments Anchors the standard for reliable follow through in working agreements and addresses anyone at any level who lets that standard slip.	■■■■■ N5	4	no	Personality questionnaire	Big Fifty, 15PF, 360 Feedback
G	Stress tolerance Keeps the organisation workable in crises, takes decisions under high uncertainty and sets the standard for composed action under pressure.	■■■■■ N5	4	no	Personality questionnaire	Big Fifty, 15PF, Mental Resilience (4C)
V	Information security in the work process Sets information security policy and monitors organisation wide that processes meet the requirements set.	■■■■■ N5	4	no	Knowledge test	Knowledge test (client-specific)
V	Using cloud platforms Determines the organisation's cloud strategy and decides which workloads are placed where.	■■■■■ N5	4	no	Knowledge test	Knowledge test (client-specific)
K	Information security awareness Designs the organisation's awareness programme, measures its effect and adjusts the approach based on measured results.	■■■■■ N5	4	no	Knowledge test	Knowledge test (client-specific)
V	Policy development Sets the policy course for a domain, connects parties in the chain and has the effects evaluated systematically.	■■■■■ N5	4	no	Portfolio or evidence	Portfolio, Competency Check

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Security incident response Independently limits damage during an incident, preserves evidence and delivers a traceable timeline of events.	 N4	4	no	Simulation	Knowledge test (client-specific), Work sample test
V	Learning from mistakes and incidents Analyses own errors and those of the team, discusses the cause openly in the work meeting and adjusts the agreements.	 N4	3	no	Situational Judgement Test	360 Feedback, Competency Check
V	Professional currency and specialist literature Tracks sources and guidelines structurally, weighs their quality and adapts the own working method to new insights.	 N4	3	no	Portfolio or evidence	Portfolio, Knowledge test (client-specific)
V	Writing technical documentation Writes complete documentation for a system or process, tests it with an unfamiliar reader and maintains versions.	 N4	3	no	Work sample test	Work sample test, Portfolio
V	Process automation Describes a process in steps, automates the repeatable steps and builds in checks on errors and exceptions.	 N4	3	no	Work sample test	Work sample test, Portfolio

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Functional and application management Independently manages an application, prioritises change requests with users and tests new versions before they go live.	 N4	3	no	Work sample test	Knowledge test (client-specific), Work sample test
V	Incident management and troubleshooting Sets an investigation line for an unfamiliar disruption, restores the service and records cause and solution for reuse.	 N3	3	no	Work sample test	Work sample test, Knowledge test (client-specific)
V	Data classification and retention Determines classification and retention period for an information flow and checks whether clean up happens as planned.	 N4	2	no	Knowledge test	Knowledge test (client-specific), Work sample test
K	Basic networking knowledge Deduces from symptoms in which network layer a problem sits and supports that with own measurements.	 N3	2	no	Knowledge test	Knowledge test (client-specific)
V	IT supplier and contract management Holds supplier meetings on performance and cost, records agreements and intervenes when agreements are not met.	 N3	1	no	Structured interview	Structured interview, Portfolio

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	System administration and monitoring Performs scheduled maintenance tasks and updates according to the runbook and reports deviations in monitoring signals.	 N2	1	no	Work sample test	Knowledge test (client-specific), Work sample test

3 Levels per seniority

The same profile with the job family seniority adjustment applied. Target levels are clamped to 1 to 5.

Skill	lead
Problem analysis	N5
Strategic thinking	N5
Governance and compliance	N5
Risk management	N5
Access and identity management	N5
Threat and risk analysis	N4
Accuracy and attention to detail	N5
integrity and dependability	N5
Accounting to supervisors and stakeholders	N5
Discipline and keeping commitments	N5
Stress tolerance	N5
Information security in the work process	N5
Using cloud platforms	N5
Information security awareness	N5
Policy development	N5
Security incident response	N4
Learning from mistakes and incidents	N4
Professional currency and specialist literature	N4
Writing technical documentation	N4
Process automation	N4
Functional and application management	N4
Incident management and troubleshooting	N3
Data classification and retention	N4

Skill	lead
Basic networking knowledge	N3
IT supplier and contract management	N3
System administration and monitoring	N2

4 The proficiency scale

Level	Label	Autonomy	Complexity	Scope	Depth of knowledge
N1	Guided	works under supervision and follows instruction	routine, one variable at a time	own task	basic understanding of terminology
N2	Applying	works independently within set frameworks	familiar situations with limited variation	own role	working knowledge, applies standard approach
N3	Proficient	sets own approach and seeks input proactively	several variables, some ambiguity	own team or process	thorough knowledge, weighs alternatives
N4	Advanced	directs others and decides on the approach	complex, with conflicting interests	several teams or a department	in-depth knowledge, advises others
N5	Leading	sets the standard and the policy	strategic, under high uncertainty	organisation, value chain or profession	authority, advances the profession

5 Behavioural anchors per skill

Anchors sit at N1, N3 and N5. N2 and N4 are deliberately not anchored: raters interpolate between them, following the O*NET convention.

Skill	N1	N3	N5
Problem analysis Breaks a problem into parts, separates causes from effects and states which information is needed to move forward.	States precisely what deviates in a malfunction and which data are missing, and puts this to the supervisor.	Splits a recurring complaint into possible causes, tests these with own data and names the most likely cause.	Traces persistent organisational problems back to a few root causes and sets the analysis method that other teams will use.
Strategic thinking Analysing developments in the environment, market and technology and deriving strategic choices and alternatives from them for the longer term of an organisation or unit.	Collects data on market and competitors on request and summarises the main developments for the manager.	Places figures, customer signals and trends side by side and names two or three strategic options with their consequences.	Develops scenarios for the whole organisation, weighs uncertainties explicitly and sets the strategic agenda together with the executive board.

Skill	N1	N3	N5
Governance and compliance Knowing which laws, codes of conduct and internal rules apply to the own field and how supervision, mandate and accountability are arranged in the organisation.	Names the main rules for the own work and looks up the applicable procedure when in doubt.	Tests intended working methods against law and internal rules and submits deviations with substantiation to the responsible officer.	Draws up the governance framework of the organisation, defines mandates and oversight arrangements and accounts for compliance to external supervisors.
Risk management Identifying risks in work, projects or policy, weighing likelihood and impact, choosing control measures and periodically testing whether those measures work.	Reports unsafe or risky situations in the own work through the agreed reporting route.	Draws up a risk list with likelihood, impact and measure per risk and reviews it periodically with those involved.	Builds the risk framework of the organisation, sets risk appetite with the executive team and reports on it to the supervisory body.
Access and identity management Grants permissions based on role and necessity, periodically reviews who can access what and withdraws rights on change or departure.	Processes access requests according to the established role scheme and records every change.	Designs roles and permissions for an application, carries out the periodic review and corrects excessive access.	Sets the organisation's access policy and accounts for the control of permissions in audits.
Threat and risk analysis Maps threats, weaknesses and consequences for a system or process, weighs likelihood against impact and names appropriate measures.	Completes a risk inventory using a given list of threats and submits the outcome to the specialist.	Independently performs a threat analysis on an application, prioritises risks and advises on measures with costs and effect.	Determines the organisation's risk appetite and analysis method and accounts for the security risk picture to the board.
Accuracy and attention to detail Works carefully, checks own work for errors and keeps to agreements about completeness and correctness of data.	Goes through the own work with a checklist and repairs errors found before the work is passed on.	Builds check moments into the own process, keeps track of errors and prevents repetition by adjusting the method.	Sets the standards for completeness and correctness, has samples checked and addresses teams on structural sloppiness.

Skill	N1	N3	N5
integrity and dependability Acting in line with applicable standards and agreements, also without supervision, and being transparent about own interests, mistakes and doubtful cases.	Keeps to agreements and rules of conduct made and reports an own mistake to the manager.	Reports a possible conflict of interest on own initiative and asks for review before a decision is taken.	Sets the organisation's integrity standards, enforces them also with influential parties and explains the resulting choices publicly.
Accounting to supervisors and stakeholders Explaining results, choices and incidents to a supervisory board, works council, clients or inspectorate, with facts, context and visible consequences for policy.	Supplies factual data for an accountability report and checks it for accuracy and completeness.	Presents team results to sponsor and works council, also names what failed and which steps will follow.	Accounts for organisational results and incidents to the supervisory board, media or politics and links visible policy adjustments to them.
Discipline and keeping commitments Sticks to agreements, procedures and commitments even without supervision, and reports in good time when a commitment turns out to be unachievable.	Arrives at the agreed time with the agreed work and reports any delay to the supervisor.	Commits only to what is feasible, tracks own commitments and informs those involved as soon as a deadline comes under pressure.	Anchors the standard for reliable follow through in working agreements and addresses anyone at any level who lets that standard slip.
Stress tolerance Keeps delivering work of the same quality under time pressure, opposition or unexpected turns and maintains a businesslike tone with others.	Keeps working on the current task as pressure rises and asks the supervisor which task can wait.	Keeps working in a structured way at peak load, keeps agreements with clients clear and flags early which results are at risk.	Keeps the organisation workable in crises, takes decisions under high uncertainty and sets the standard for composed action under pressure.
Information security in the work process Applies security measures in daily work such as safe sharing, classifying and storing information and flags risky working practices.	Follows the security rules for sharing and storing information and reports a suspected incident immediately.	Weights security risks when setting new working agreements, adjusts measures and addresses colleagues on unsafe behaviour.	Sets information security policy and monitors organisation wide that processes meet the requirements set.

Skill	N1	N3	N5
Using cloud platforms Sets up and manages services in a cloud environment, arranges permissions and costs and chooses between available service types based on requirements.	Uses existing cloud services as instructed and reports unusual behaviour or unexpected costs to the administrator.	Independently configures cloud services for an application, arranges permissions and backups and keeps costs and usage in view.	Determines the organisation's cloud strategy and decides which workloads are placed where.
Information security awareness Knows the most common threats such as phishing, ransomware and deception, recognises their signals and knows which action is then expected.	Recognises an obvious phishing message, does not click and reports the message through the designated channel.	Explains to colleagues how threats work, judges doubtful cases independently and adapts own behaviour to new threats.	Designs the organisation's awareness programme, measures its effect and adjusts the approach based on measured results.
Policy development Develops policy through problem analysis, exploration of options, consultation of stakeholders and elaboration into goals, instruments and evaluation.	Collects figures and documents for a policy exploration under guidance and summarises the findings briefly.	Independently elaborates a policy proposal with options and expected effects and organises consultation of the parties involved.	Sets the policy course for a domain, connects parties in the chain and has the effects evaluated systematically.
Security incident response Acts on a security incident following the runbook by containing it, preserving evidence, recovering and informing the right parties in time.	Reports a suspected incident immediately, touches nothing and follows the coordinator's instructions.	Independently limits damage during an incident, preserves evidence and delivers a traceable timeline of events.	Leads the organisation wide response team, decides on external communication and improves the runbook after every exercise.
Learning from mistakes and incidents Investigates after an error or incident what happened, names the cause without shifting blame and changes the working method on that point.	Reports an own error to the supervisor at once and repeats the task following the corrected instruction.	Analyses own errors and those of the team, discusses the cause openly in the work meeting and adjusts the agreements.	Ensures incidents are reported safely across the organisation, has causes analysed structurally and works the lessons into policy and standards.

Skill	N1	N3	N5
Professional currency and specialist literature Follows developments in the own profession through literature, guidelines and networks and works relevant new insights into own practice.	Reads the professional information received and names which part matters for the own work.	Tracks sources and guidelines structurally, weighs their quality and adapts the own working method to new insights.	Assesses the state of the field, weighs conflicting research and determines which guidelines the organisation will follow from now on.
Writing technical documentation Writes manuals, support documentation and decision records that a reader without prior knowledge can follow step by step and that stay current.	Completes a documentation template with the steps of a task and has the text checked by a colleague.	Writes complete documentation for a system or process, tests it with an unfamiliar reader and maintains versions.	Sets the organisation's documentation standard and ensures documentation is part of every delivery.
Process automation Analyses a recurring work process, builds or commissions automation of its steps and checks that the outcome stays reliable.	Runs an existing automation and reports when the outcome differs from what was expected.	Describes a process in steps, automates the repeatable steps and builds in checks on errors and exceptions.	Determines the organisation's automation agenda and decides which processes are and are not automated.
Functional and application management Keeps an application working and fitting for users by collecting needs, managing settings and coordinating changes with the supplier.	Handles user questions about an application as instructed and records requests in the designated register.	Independently manages an application, prioritises change requests with users and tests new versions before they go live.	Determines how functional management is organised and decides on the lifespan of applications.
Incident management and troubleshooting Takes in disruptions, establishes the cause through targeted steps, restores the service and keeps reporters and stakeholders informed.	Logs a disruption completely, works through the standard steps and escalates as soon as own steps do not work.	Sets an investigation line for an unfamiliar disruption, restores the service and records cause and solution for reuse.	Designs the organisation's incident process, leads the response to major disruptions and accounts for it to management and clients.

Skill	N1	N3	N5
Data classification and retention Classifies information by sensitivity and importance, links retention periods to it and ensures deletion and archiving actually happen.	Assigns a classification label according to the scheme and refers unclear cases to the administrator.	Determines classification and retention period for an information flow and checks whether clean up happens as planned.	Designs the organisation's classification and retention policy and accounts for it in audits and supervision.
Basic networking knowledge Knows how networks work at a high level such as addressing, routing, ports and name resolution and states where a connection problem may arise.	Explains which parts make up a connection and performs a provided check such as a connectivity test.	Deduces from symptoms in which network layer a problem sits and supports that with own measurements.	Disseminates networking knowledge in the organisation, sets design principles and reviews network designs from suppliers.
IT supplier and contract management Manages agreements with IT suppliers on delivery, performance and cost, monitors compliance and addresses suppliers on deviations.	Checks invoices and delivered services against the contract and reports deviations to the contract manager.	Holds supplier meetings on performance and cost, records agreements and intervenes when agreements are not met.	Sets the organisation's supplier policy, concludes the main contracts and decides on termination or switching.
System administration and monitoring Keeps systems running by managing settings, updates and permissions, sets up monitoring and acts on signals before users are affected.	Performs scheduled maintenance tasks and updates according to the runbook and reports deviations in monitoring signals.	Independently manages a system environment, sets monitoring thresholds and removes recurring causes of disruptions.	Sets the organisation's administration and monitoring standards and decides on the design of the system environment.

6 Assessment methods and validity

The validities are the corrected meta-analytic estimates from Sackett, Zhang, Berry and Lievens (2022) in the Journal of Applied Psychology, which replace the older Schmidt and Hunter (1998) figures. The spread matters as much as the mean: with a high SD, validity varies strongly by context.

Assessment method	rho	SD	What it is
Assessment centre	0.29	0.09	Multiple exercises, multiple assessors, dimension-wise scoring.
Knowledge test	0.40	0.13	Test of declarative job knowledge, usually assembled per client.
Work sample test	0.33	0.09	The candidate performs a representative work sample under standardised conditions.
Personality questionnaire	0.40	0.15	Self-report of behavioural preferences. At hrmforce the Big Fifty and the 15PF.
Portfolio or evidence	-	-	A collection of prior work or results, assessed against fixed criteria.
Simulation	-	-	Simulated work situation, usually digital, with standardised scoring.
Situational Judgement Test	0.12	0.11	Scenario with response options, scored on knowledge or behavioural tendency.
Structured interview	0.42	0.19	Behaviour-based interview with fixed questions and a rating scale per question.

7 Assessment instruments for this job

hrmforce instrument	Skills	What it measures
Knowledge test (client-specific)	14	Professional knowledge test, customized for each client
Work sample test	9	Representative work sample under standardized conditions
Competency Check	6	Behavioral-Level Competency Assessment
360 Feedback	5	Multiple assessments based on behavioral anchors
Portfolio	5	Evaluation of prior work against fixed criteria
Big Fifty	3	Personality questionnaire, 150 items, 25 factors
Ability Scan	2	Aptitude Test: Verbal, Numerical, and Abstract Reasoning Skills
Structured interview	2	Behavioral interview with a fixed structure

hrmforce instrument	Skills	What it measures
15PF	2	Personality Profile, a shorter alternative to the Big Fifty
Big Fifty (Integrity Scale)	1	
Mental Resilience (4C)	1	Mental Resilience According to the 4C Model

8 How to use this profile

1. Agree the profile with the hiring manager before the first candidate is measured. Weights shifted afterwards make the outcome indefensible.
2. Choose the assessment method per skill from the Assessment method column. Combine at most three methods per candidate.
3. Calibrate the assessors in a two-hour session using the anchors in chapter 5. Anchors without rater training deliver little.
4. Fill in the match calculator and discuss the gaps in the development conversation. Type A and type G are selection criteria, not one-quarter development goals.

Source: hrmforce Skills Framework 2.0, version 2.0.0, built 2026-09-08. Crosswalks to ESCO v1.2.1, O*NET 31.0, Lightcast Open Skills, SFIA 9, DigComp 3.0, EntreComp, LifeComp, GreenComp, AILit, WEF Future of Jobs 2025, ISCO-08 and the Dutch CBS occupational classification BRC 2014 edition 2025. This profile is a starting point, not a standard: align it with your own organisation before selecting on it.