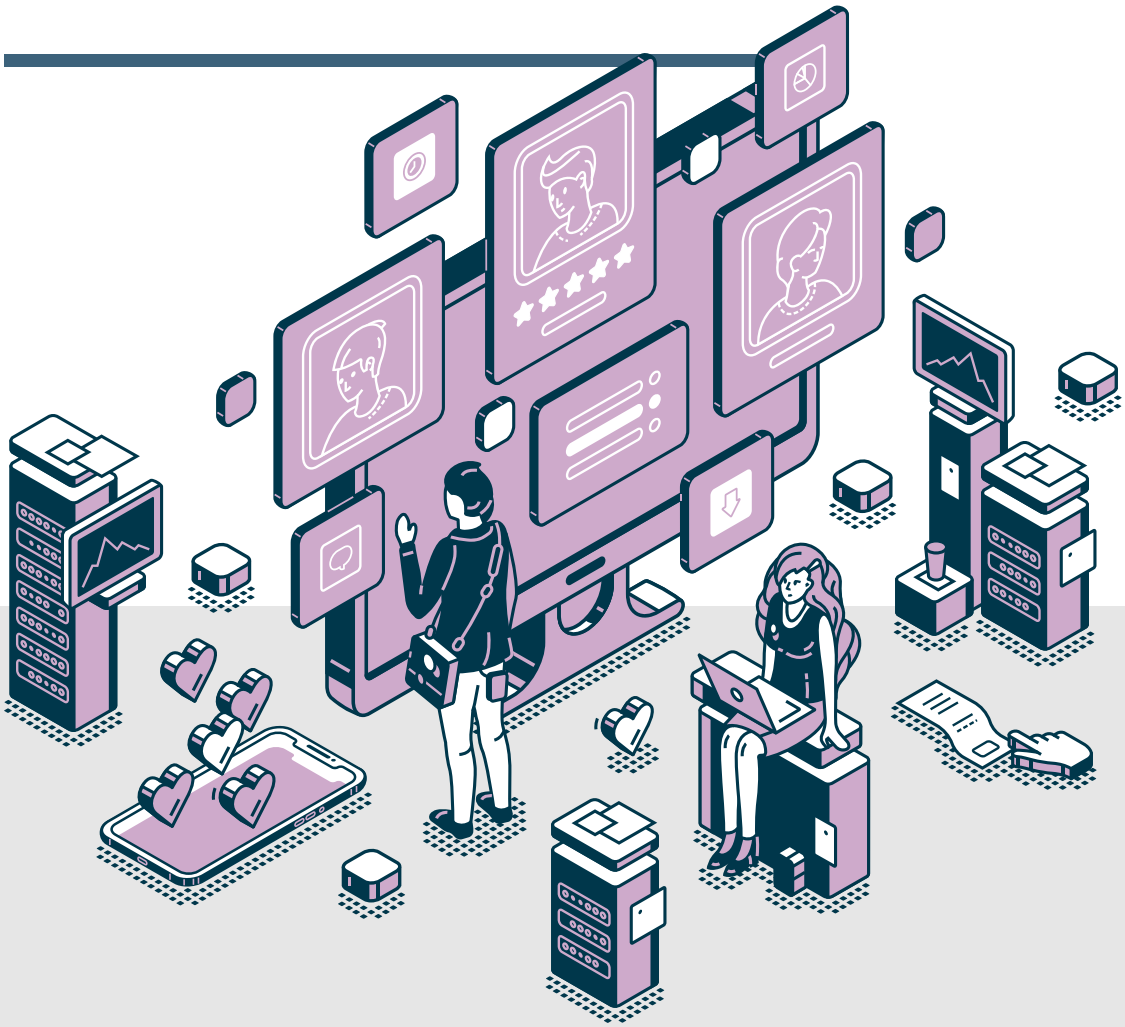
FROM THE APPLICATION TO THE VISION



What are the critical preparatory tasks (PreJobs tasks) for CISOs. This paper summarizes the view of different individuals and their experience during job changes and new starts. The tasks were divided into three phases: Before the interview, during the interview and after the interview.

Pre-interview:

This phase is critical for strategic preparations and information gathering. Here, the goal is to develop an in-depth understanding of the position and the business environment, identify potential challenges and opportunities, and formulate initial plans for the potential role.

During the interview:

This is where you gather more in-depth information directly from the field, clarify important questions regarding your role and responsibilities, and interact with key stakeholders to get a feel for the company culture and how information security is handled.

Post-interview:

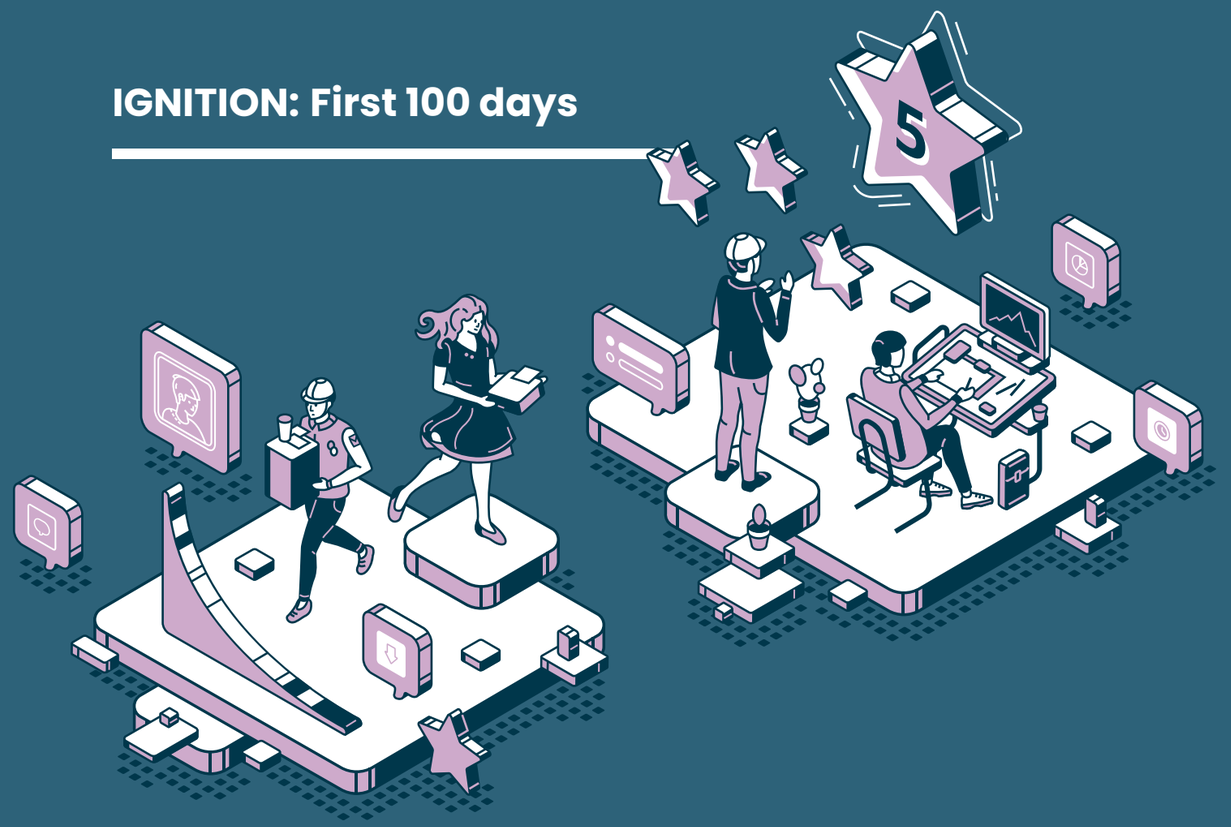
This stage is crucial to reflect on your experience and assess whether the position and the company align with your personal goals and values.

The following table summarises the specific tasks in each phase:

Phase	Task	Description
Before the Interview	Create Own Requirement Profile	Create a profile that matches the job profile. Keyword: Template
Before the Interview	Screen OpenSource-Infos (internal/external) about potential employer - Desk Research	New Management, M&A activities, Incidents
Before the Interview	Check Network	Who works or has worked at the target employer I know and can ask? Compare with own impressions from 1st and 2nd interview
Before the Interview	Prepare the 4-5 most important questions for the 1st interview	Think about scenario questions to learn more about culture and attitude - e.g., how would the team function if the CISO would be absent for a longer period?
Before the Interview	Start own plan for the first 100 days and be ready	Could also be a question in the interview: describe roughly how you will design the first 100 days
During the Interview	Onsite-Check before the Interview	Come early and make an impression - how are you received, how easy is access to the premises (without access controls). How does the whole environment appear - well organized, attentive, chaotic?
During the Interview	Clarify: Why is the position open	New or replacement - speak to current CISO/try to reach/speak to exCISO
During the Interview	Check VR and Management's attitude to Security	-
During the Interview	Clarify CISO's reporting paths	Who does he report to and who reports to him (indicator: who leads the interviews?)
During the Interview	Request talks with the most important stakeholders for the 2nd or 3rd interview	This is where you learn directly about openness and culture
During the Interview	Clarify the CISO's scope of responsibility	-
During the Interview	Observe: in the interview	Transparency and unity on information security
During the Interview	Check the maturity of the 1st Line of Defence	In the context of stakeholder interviews
During the Interview	Clarify: Vision for information security	And what exact expectations are directed at the CISO. What specific goals are to be achieved after 12 months?
During the Interview	Have described: short overview of the most important security processes	Have described and delve into certain points. Check what is all shown publicly, although a confidentiality level is behind it
During the Interview	Have described: which projects are currently running	In the field of information security and which projects are planned with which priority

Phase	Task	Description
After the Interview	Review	After each of the first and second interviews: does the personal SWOT match the SWOT of the potential employer - is it a MATCH?
After the Interview	Course of the recruitment process	Were all participants on time? How was communication between interviews? How reliably were information delivered? How well organized was the entire recruitment process?
After the Interview	Soft-Factor-Check	What is the chemistry to the direct superior - how to the most important stakes? What signals were sent between the lines? What is the final gut feeling?

IGNITION: First 100 days

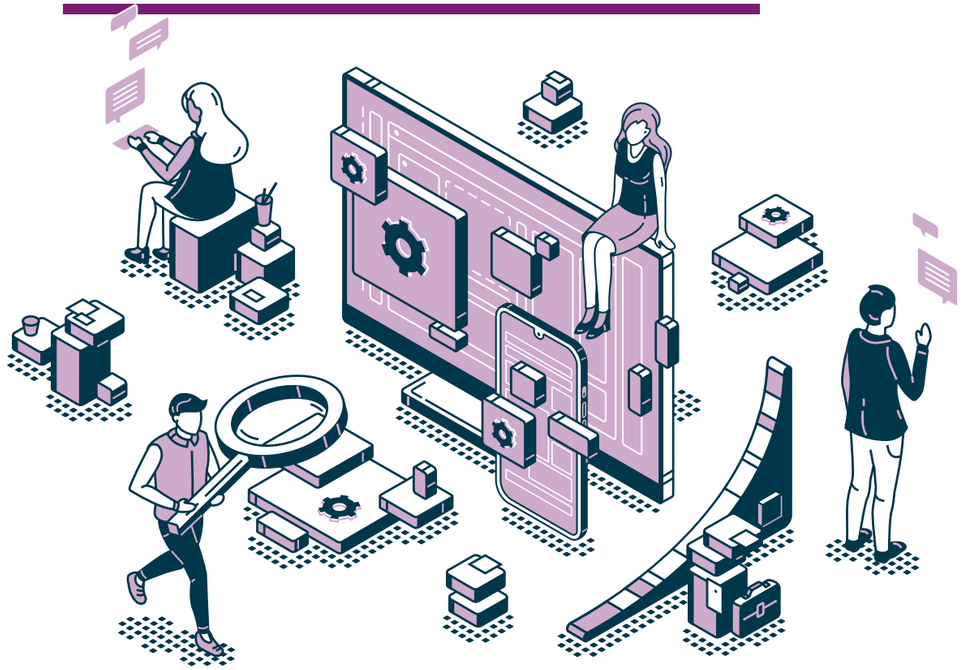


The first 100 days of a new leadership position are crucial to grasp the status quo and gain an understanding of the company. This enables a sound GAP analysis, strategic planning and the definition of one's role. This phase lays the foundation for future success and the achievement of the company's goals.

Area	Task	Description
1. Status Quo Assessment	Business Strategy Analysis	Understand the current business strategy to gain insight into the company's goals and direction.
	IT Strategy and Alignment	Analyze the IT strategy and its alignment with the business strategy to understand the interplay.
	Framework Evaluation	Get to know the used IT framework to understand how technology is used within the company.
	Organizational Structure Analysis	Evaluate the organization to understand how the company is structured and how departments interact.
	Stakeholder Identification	Identify the decision-makers in the company to understand who influences the IT strategy.
	Process and Compliance Understanding	Investigate the relevant company processes and the influence of compliance and corporate risk on cybersecurity.
	Revenue Generation and Relevance Analysis	Analyze how revenue is generated and identify the most important business areas.
	Documentation Review	Review official documents such as business reports, audits, and press releases to gain a comprehensive understanding of the company.
	Technology Setup Review	Review the current technological setup to understand the current state of IT within the company.
	Industry-Specific Analysis	Learn about the specific industry and understand relevant laws and regulations.
2. Interactive Assessment	Stakeholder Engagement	Establish contact and conduct meetings with identified stakeholders to understand their needs and concerns.
	Area Visits	Visit the most relevant company areas to gain a deeper understanding through direct experience.
	"Shadow Government" Identification	Identify and meet with informal influence groups within the organization.
	Staff Survey	Conduct a staff survey to get a comprehensive picture of the organization and the state of awareness on the topic.
3. Results Interpretation	Current-to-Desired State Analysis	Sketch the current state and perform a GAP analysis to the desired state to identify where changes are needed.
	Risk Analysis	Identify and derive potential risks based on the findings so far.
	Culture and Stakeholder Analysis	Describe the corporate culture and its subgroups and categorize all stakeholders as enablers, supporters, and blockers.
4. Strategy Development	Time Planning	Identify relevant dates from the past that may be important in the future.

Area	Task	Description
	Consideration of Upcoming Regulations	Include upcoming regulatory changes in strategic planning.
	Strategy Derivation	Develop an IT strategy based on the findings so far.
	Roadmap Definition	Develop a roadmap based on the GAP analysis that outlines the path to achieving the goals.
	Role Definition	Define your own role and expectations within the company.
5. Transition to Management	Management Integration	Implement the developed strategy and integrate into the management team.

Future CISO role - integration, focus on business and stakeholder management



The future role of the Chief Information Security Officer (CISO) in cyber security is characterised by increased integration with the business and a focus on security direction. As a business enabler, it is critical that the CISO has outstanding stakeholder management skills.

The role of Chief Information Security Officers (CISOs) is rapidly shifting from a technical-centric position to one that demands strong communication skills, empathy, business acumen, and an understanding of ethics and privacy regulations. This abstract explores the changing landscape of the CISO role, emphasizing the essential competencies required for future success.

As organizations increasingly recognize the significance of cybersecurity and maintaining customer trust, CISOs now bear responsibilities beyond technical security implementation. Effective collaboration, relationship building, and the ability to translate complex security concepts into business insights are now essential communication skills for CISOs.

Furthermore, the future CISO must demonstrate empathy, understanding the needs and concerns of various stakeholders. This empathetic approach allows for effective communication of security importance, considering its impact on productivity, user experience, and overall organizational objectives.

In addition to communication and empathy, future CISOs must possess business and economic acumen to align security initiatives with strategic goals and ensure a measurable return on investment. Risk management principles should guide their prioritization and resource allocation.

Ethical considerations and privacy regulations are also becoming key responsibilities for CISOs. Familiarity with regulations like the General Data Protection Regulation (GDPR) is crucial, as CISOs play a pivotal role in developing policies that balance security requirements with privacy rights.

Ways to achieve the future CISO role

To achieve the future CISO role, it is important that the CISO influences the company culture and contributes to business success. Cyber security plays a critical role in protecting a company's core revenue-driving processes. A security incident can have significant financial and legal consequences. By implementing effective security measures, the CISO can build customer and partner confidence, protect the company's reputation and prevent potential business disruption. Persuasive communication and effective resource management are key skills in communicating the importance of cyber security in protecting core business processes and providing the necessary resources for security initiatives.

Conclusion

Essential skills for the future CISO role Certain skills are particularly important for the future CISO role. Excellent communication skills enable the CISO to convey the importance of security throughout the organisation. A high tolerance for frustration helps to deal with the challenges of the role. Leadership and coaching skills are critical to influence the company culture and encourage employees to be proactive in security. Strategic thinking is essential to strengthen the CISO's role as a business enabler and set the direction of security. Effective resource management is required to efficiently lead and implement security initiatives.

Cyber Circle, located in Switzerland, is a project that connects CISOs (Chief Information Security Officers) with researchers. This collaborative community meets every two months for an evening of valuable discussions and activities centered around their roles. The focus is on providing insights, facilitating cross-industry learning, enabling external peer networking, and conducting practical workshops. The ultimate goal is to establish improved cybersecurity principles, including human-centered security, within companies.

Join Cyber Circle and become part of a friendly community shaping the future of cybersecurity!

Based on Cyber Circle Season 2 / Session 3, Zürich, May 2023