

Thematic Data Analysis Sample Report on Information Security/Cybersecurity & Privacy Protection

Important Note

- This sample report includes selected datasets and questions for illustrative purposes in the analysis section.
- This sample report is based on CSA methodology for 2023.
- T-DAR comprises three distinct modules, with the depth of data analysis contingent upon the selected configuration. This report is structured into three sections, each providing an introduction to one of the three modules.

Contents

X	Topic Overview and S&P Global Corporate Sustainability Assessment (CSA) Relevance for the society, company and capital market
X	Data Universe and Guidance Scope of the analysis and how to read charts and symbols
XX	Data Analysis for..... Detailed data analysis at multiple levels to understand how the topic is addressed
XX	Company Performance.....
XX	Contact and Disclaimer

Information Security/Cybersecurity & Privacy Protection

Relevance for the society

Due to the current trend of digitalization worldwide, it is crucial that access to networks, IT systems and data is always assured. As consumers shift to online platforms and services, such as cloud systems and online marketplaces, identity theft is among the several privacy risks customers face when verifying personal information. Particularly, banking information and medical records are highly susceptible to exploitation following the influx of personal data received from online registrants needing financial or medical support during the pandemic. Safeguarding these records are even more challenging given the variety of applications and devices accessible to malicious agents for ransomware or insurance fraud acts. A transparent and comprehensive privacy policy is essential to build trust and ensure effective customer data protection.

Relevance for the business

Cybersecurity breaches and theft have become more frequent and costly, making information security and data protection top concerns for companies across different regions. A business may experience operational disruption and allocate additional funds for dealing with cybercrime incidents, potentially incurring fines and penalties on top of losing sensitive information. Thus, IT security plays a significant function in its governance and infrastructure. Research by S&P Global Sustainable1 reveals that 60% of companies in financials are prepared for cybersecurity breaches, while nearly 40% in healthcare test their incident responses less frequently. Actions taken by a company to identify gaps within its information security processes further strengthen cybersecurity measures amid the growing reliance of the global economy on digital technologies and solutions.

Relevance for the capital market

The exponential increase of issues related to information security poses a threat on corporate market value. Investors and stakeholders consider this as a financially material issue, with the World Economic Forum listing “widespread cybercrime and cyber insecurity” as one of the top ten global risks in the next decade. In this context, the frequency of internal audits for privacy policy compliance has picked up but far less for external audits, or less than 30% of companies assessed in S&P Global’s Corporate Sustainability Assessment (CSA). Now, more pressure is being applied by regulators for companies to set in place, for instance, technical standards and requirements under the EU’s adopted Digital Operational Resilience Act (DORA), or procedures to protect investor records and assets, which was identified as an area of risk by the SEC.

Source:

- CSA 2023
- [S&P Global Sustainable1](#)

Information Security/Cybersecurity & Privacy Protection

CSA 2023 Methodology

The basis of the analysis is the S&P Global 2023 Corporate Sustainability Assessment (CSA) which evaluated around 3'000 companies on various E, S, and G parameters, including specific questions about Cybersecurity & Privacy Protection, in line with many international reporting standards and frameworks. These questions cover topics such as engagement of board of directors and executive management in the information security/cybersecurity strategy and review process, IT security/ cybersecurity measures and infrastructure, privacy policy and its aspects. The analysis offers insights into the current performance of companies participating in the CSA across 11 industry groups and in 5 geographic locations.

List of the relevant questions from the Corporate Sustainability Assessment (CSA) 2023 covered in this report:

1. IT Security/ Cybersecurity Governance
2. IT Security/ Cybersecurity Measures
3. IT Security/ Cybersecurity Process & Infrastructure
4. Customer Privacy Information

Source: CSA 2023

Contents

X **Topic Overview and S&P Global Corporate Sustainability Assessment (CSA)**
Relevance for the society, company and capital market

X **Data Universe and Guidance**
Scope of the analysis and how to read charts and symbols

XX **Data Analysis at.....**
Detailed data analysis to understand how the topic is addressed

XX **Company Performance on.....**
Performance of the company on the specific topic, highlighting the major gaps in terms of score with respect to the CSA practice

XX **Contact and Disclaimer**

The Corporate Sustainability Assessment (CSA)

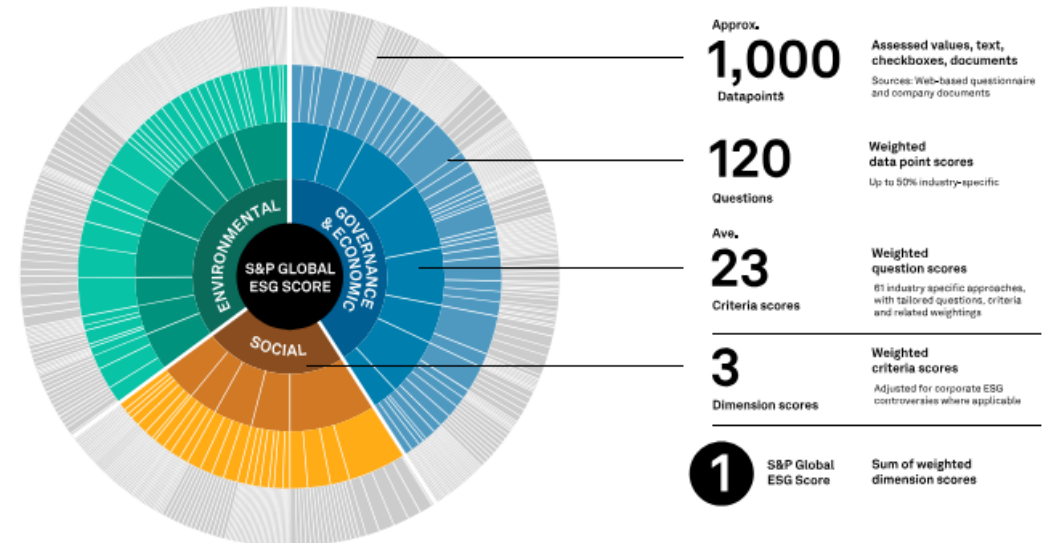
The Corporate Sustainability Assessment (CSA) is an annual evaluation of companies' sustainability practices. This year, S&P Global is inviting over 13,800 companies. The CSA focuses on criteria that are both industry-specific and financially material and has been doing so since 1999.

Key facts

- As of January 2020, the CSA is **issued by S&P Global**, where it forms the foundation of company ESG disclosure to S&P Global for financially material ESG factors and will underpin the ESG research across our different divisions (S&P Global Ratings, S&P Dow Jones Indices and S&P Global Market Intelligence).
- In Sustainability's Rate the Raters 2019 report, companies rated the CSA as the most useful ESG assessment thanks to its high level of transparency, its sector-specific view of material ESG issues, and its incorporation of emerging sustainability risks and opportunities. In the 2020 report, which looked at the investor perspective, the CSA came out top **among the highest-quality ratings** and was cited as a "strong signal of sustainability."
- For over 20 years, the results of the CSA are used for the annual rebalancing of the iconic **Dow Jones Sustainability Indices (DJSI)**. CSA scores are used in numerous other S&P Dow Jones indices including the Dow Jones Sustainability Indices (DJSI) and the S&P 500 ESG.
- S&P Global CSA Scores** calculated from the CSA are made available to the global Financial markets via the **S&P Capital IQ Pro platform**, robustly linked to financial and industry data, research and news, providing integral ESG intelligence to make business and financial decisions with conviction.
- Learn all about S&P Global's ESG Solutions at www.spglobal.com/ESG and the CSA at www.spglobal.com/esg/csa

From data to score

The Corporate Sustainability Assessment (CSA) uses a consistent, rule-based methodology to convert an average of 1000 data points per company into a **total sustainability score**. It applies 62 industry-specific approaches. The size of the segments in the sample graph below represents the **weight (materiality)** assigned at the different levels. This chart is not representative of your industry.



*On average a third of datapoints in each industry require public information









Data Universe Covered

Reference universe for this report

All companies that participated in CSA 2023 and that are eligible for inclusion in the Dow Jones Sustainability Indices.






How to Interpret the Icons of the CSA Methodology

CSA Expected Practice

Assessment Focus		Description of Information Sought
Disclosure / Transparency		Disclosure of qualitative/quantitative information
Documents		Document supporting company's response
Public Documents		Publicly available document supporting company's response
Exposure/Coverage		Coverage of measures implemented, or data reported
Trend		Trend of key indicators in the last three/four years
Performance		Performance of key indicators in comparison to the expected threshold
Awareness		Awareness about internal and external issues and measures taken
External Verification		Third party verification of data or of processes

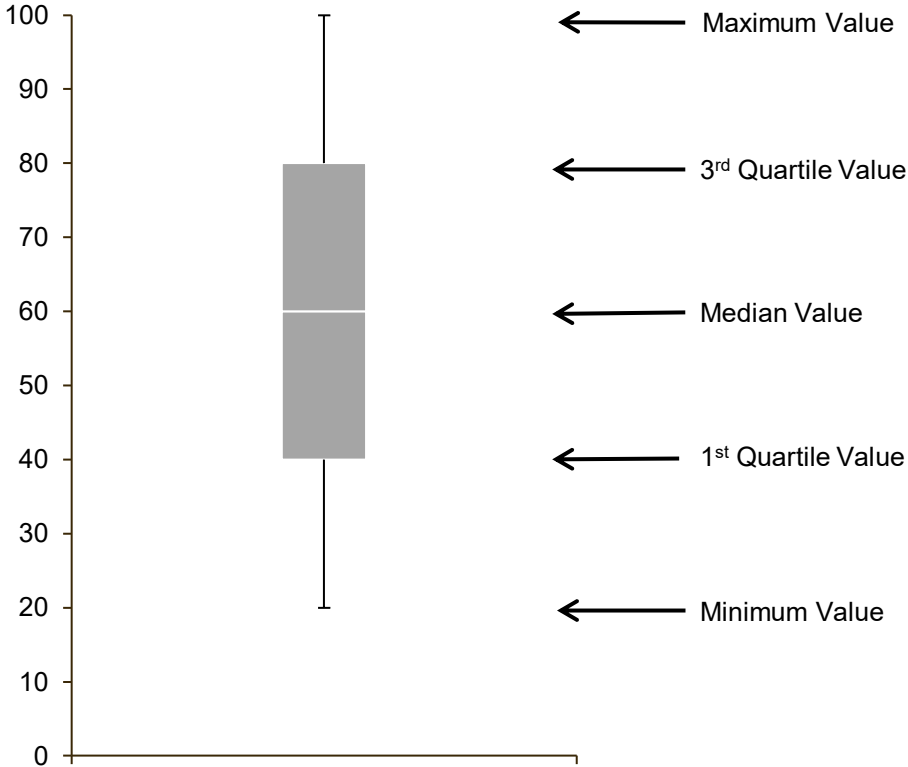
Source: CSA

Gap Analysis (only T-DAR Starter and Custom)

Assessment		Description
Full Score (100)		The company's answer received full points, or public information was found
Partial Score (1 to 99)		The company's answer did not fully meet the expected practice, or the company did not answer the question, but partial information was found publicly
Score of zero		The company did not answer the question, or the answer did not meet expectations
Additional information		Additional general or company specific information on the assessment approach and result
Not applicable		The question/aspect is not applicable for the company, resulting in a relative increase of question/aspect weights across the other questions/aspects in this criterion/dimension

How to Interpret the Box-and-Whisker Plot

Example of Box-and-Whisker Plot



Contents

X **Topic Overview and S&P Global Corporate Sustainability Assessment (CSA)**
Relevance for the society, company and capital market

X **Data Universe and Guidance**
Scope of the analysis and how to read charts and symbols

XX **Data Analysis**
Detailed data analysis to understand how the topic is addressed

XX **Company Performance on.....**
Performance of the company on the specific topic, highlighting the major gaps in terms of score with respect to the CSA practice

XX **Contact and Disclaimer**

Thematic Data Analysis Report - Basic Module

The module includes:

- General theme overview
- Relevance of the topic for the stakeholders and company
- Rationale and expected practices for the aspects analysed
- Data analysis of the topic at industry and region level



IT Security/ Cybersecurity Measures

Strengthening Employee Awareness for Cyber Resilience

CSA Expected Practice – IT Security/ Cybersecurity Measures



Topic rationale, focus and expected practice for the topic explain the context, materiality and data used for the analysis.

Rationale

Due to the current trend of digitization, including but not limited to cloud computing, online marketplaces, and payments, etc., it is crucial that access to networks, IT systems and data is assured at all times. As a result, lower than agreed upon system performance or service disruptions can result in higher costs and reputational risk for companies. The main risks stem from technical failure, human error, malicious attacks, weather events, natural disasters or terrorist attacks. Managing such risks, including contingency plans, is crucial to ensuring business continuity. Over the past decade, the number of information security breaches has grown exponentially with some attacks reaching unprecedented scales and the cyber threat landscape continues to grow and evolve, abusing existing and new technologies and exploiting vulnerable users. These incidents and the related costs have shown that information security/cybersecurity has become a financially material issue that must be diligently managed to protect corporate value. The costs of cyberattacks are manifold and can impact the company in different ways. Internal costs are operational costs and relate to dealing with cybercrime and incidence prevention. External costs include the consequences of the cyber-attack such as the loss or theft of sensitive information, operations' disruption, fines and penalties, infrastructure damage or revenue losses due to loss of customers. Thus, ensuring the security and resilience of networks and information systems is critical.

Source: CSA 2023

Focus and Expected Practice

Aspects	Focus and Expected practice description	
Security measures		Internal availability of information security/cyber security policy to employees
		Information security/cyber security awareness training
		Clear escalation process in place for employees
		Information security/cyber security is part of employee performance evaluation (e.g. disciplinary actions)

Measures to ensure awareness and importance of Information Security/Cybersecurity Measures

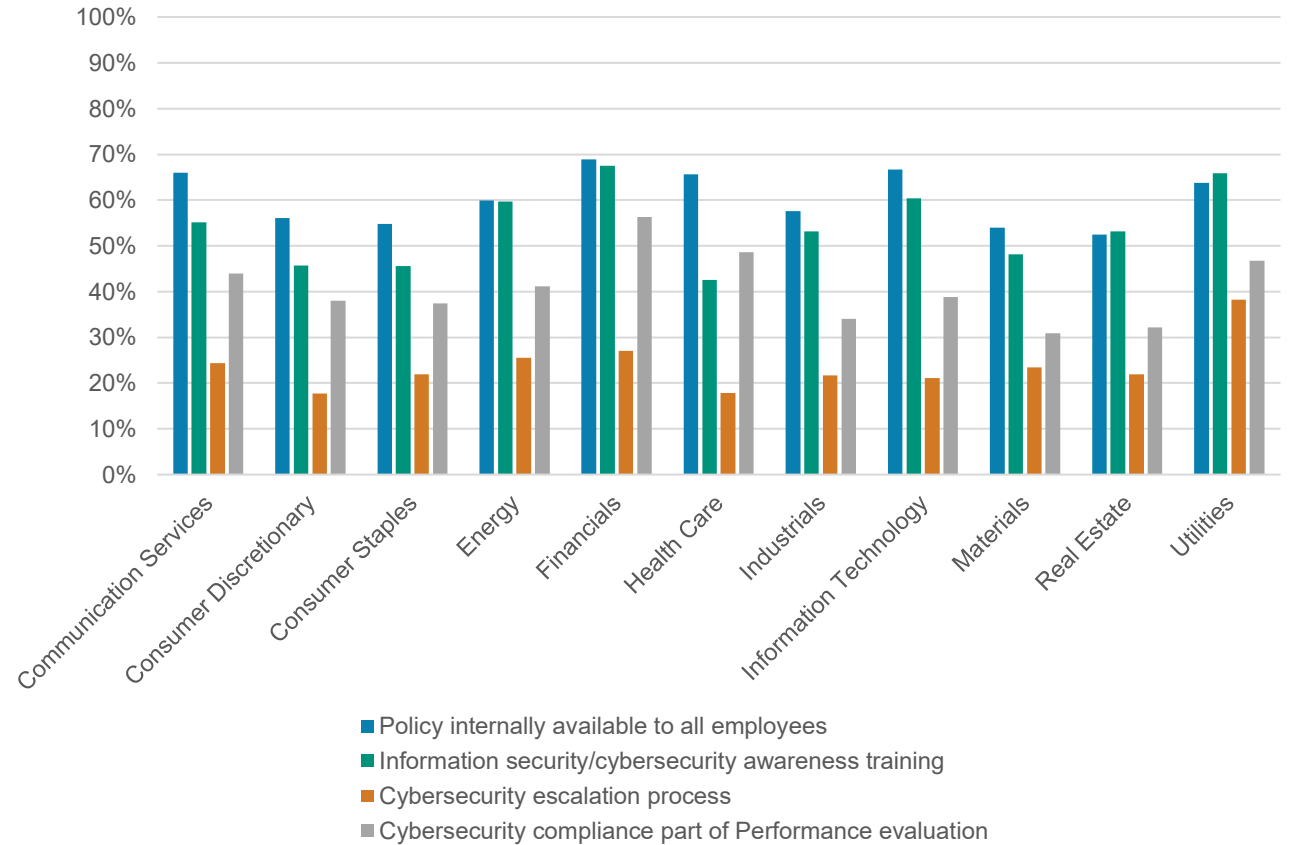
Note: The data analysis does not include companies for which this question has been considered as not applicable.

Data universe: Total number of participants

Description

- Majority of companies across industry groups illustrate a greater proportion that made internal cybersecurity policies available to all employees compared to two industry groups (Real Estate and Utilities) with more companies that implemented awareness training.
- Financials accounted for the greatest proportion of companies with various cybersecurity measures in place.
- On the contrary, employees are less likely to escalate suspicious cybersecurity activities especially those in Consumer Discretionary and Health Care industry groups (less than 20%).

Percentage of companies having various cybersecurity measures for the employees , by Industry Group



Source: CSA 2023

Measures to ensure awareness and importance of Information Security/ Cybersecurity Measures

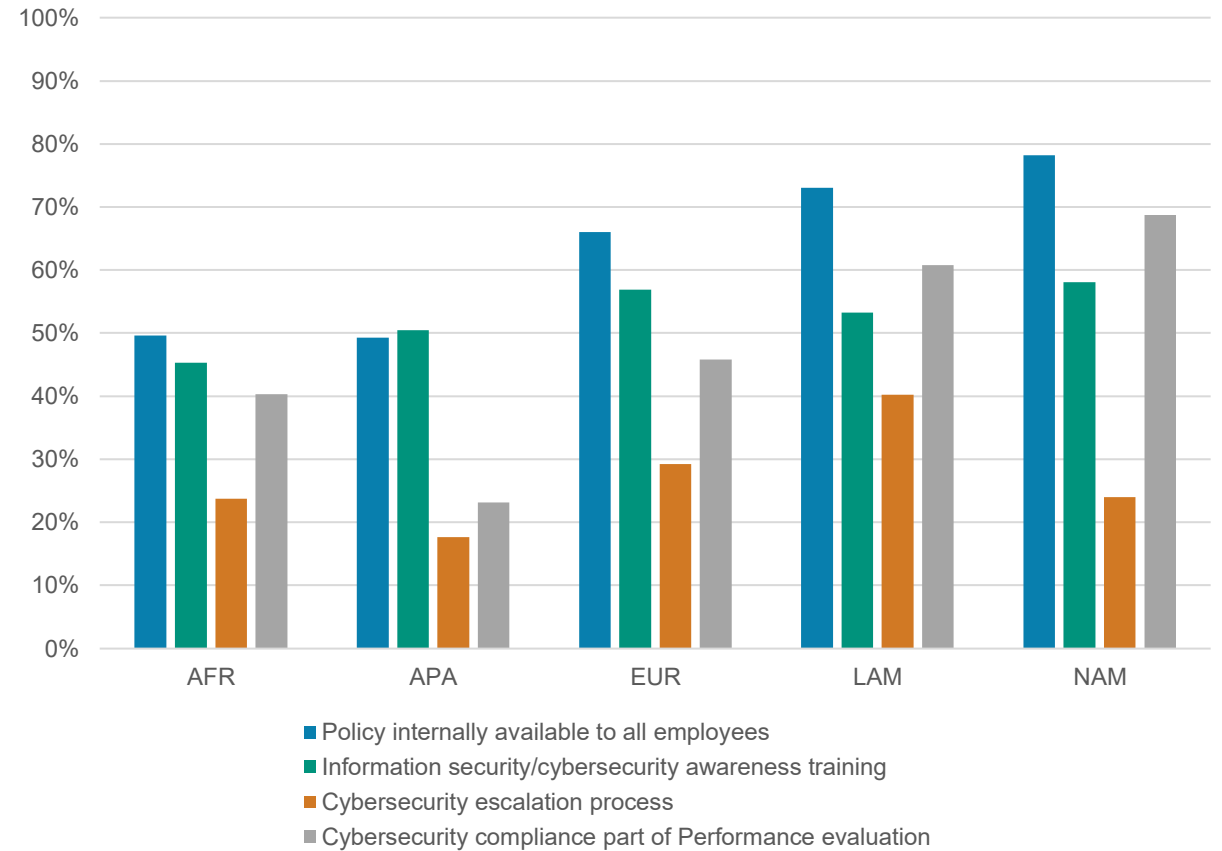
Note: The data analysis does not include companies for which this question has been considered as not applicable.

Data universe: Total number of participants

Description

- All regions but Asia-Pacific showed a higher percentage of companies that considered making cybersecurity policy internally available to all employees.
- North America illustrates the greatest proportion of companies with an internally available policy (78%), awareness training (58%) and performance evaluation (69%) measures in place.
- By comparison, at least 40% of companies in Latin America implemented every cybersecurity measure, with the highest percentage of companies having a clear escalation process for employees (40%) among regional peers.

Percentage of companies having various cybersecurity measures for the employees, by Region



Source: CSA 2023

Customer Privacy Information

Empower Your Privacy: Safeguarding Data in a Globalized World


CSA Expected Practice – Customer Privacy Information

Topic rationale, focus and expected practice for the topic explain the context, materiality and data used for the analysis.

Rationale

Networked data and globalized corporate activities require diligent information handling. In order to avoid the risks associated with these developments – such as legal costs, reputational damage, and exclusion from certain activities – companies must then endeavour to implement a comprehensive privacy policy spanning across their businesses, along with a sound implementation framework. For this question, we assess companies' transparency with customers on privacy protection issues.

Focus and Expected Practice

Aspects	Focus and Expected practice description
Privacy protection issues	<div data-bbox="1651 439 1709 491" style="display: inline-block; vertical-align: middle;">  </div> <p>Information is provided to the customers on the following privacy protection issues:</p> <ul style="list-style-type: none"> • Nature of information captured • Use of the collected information <p>Possibility for customers to decide how private data is collected, used, retained, and processed. Inclusion of the following aspects:</p> <ul style="list-style-type: none"> • Opt-out option is available • Opt-in consent is required • Request access to data held by the company

Source: CSA 2023


CSA Expected Practice – Customer Privacy Information

Topic rationale, focus and expected practice for the topic explain the context, materiality and data used for the analysis.

Rationale

Networked data and globalized corporate activities require diligent information handling. In order to avoid the risks associated with these developments – such as legal costs, reputational damage, and exclusion from certain activities – companies must then endeavour to implement a comprehensive privacy policy spanning across their businesses, along with a sound implementation framework. For this question, we assess companies' transparency with customers on privacy protection issues.

Focus and Expected Practice

Aspects	Focus and Expected practice description
Privacy protection issues <i>(continued)</i>	 <ul style="list-style-type: none"> Request their data be transferred to other service providers
	<ul style="list-style-type: none"> Request their data to be corrected
	<ul style="list-style-type: none"> Request their data to be deleted
	How long the information is kept on corporate files
	How the information is protected
	Third-parties disclosure policy (private and public entities)
	Disclosure of percentage of users whose customer data is used for secondary purposes

Source: CSA 2023

Transparency level of companies informing customers on privacy protection rights

Note: The data analysis does not include companies for which this question has been considered as not applicable.

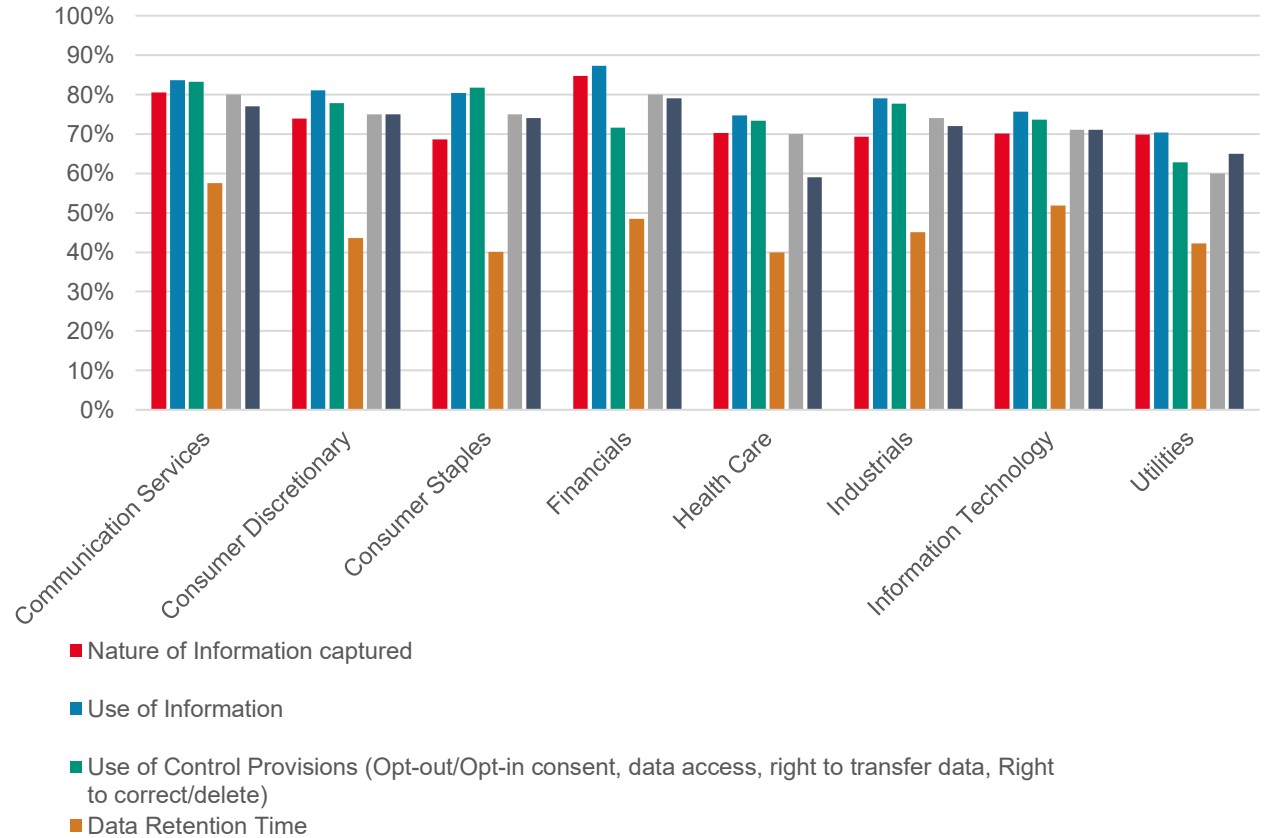
Data universe: Total number of participants

Source: CSA 2023

Description

- With the transparency in mind, no less than 40% of all companies kept customers informed about privacy issues — but companies were less inclined to share how long customer data is retained on file.
- A greater proportion of companies seven out of eight industry groups shared how customer information is used (70% to 87%), with Financials recording the highest percentage, as with the nature of information captured (85%) and third-party disclosure policy (79%)
- Meanwhile, most companies in Consumer Staples opted to inform customers on the range of control they have on personal data (82%).
- Utilities, by contrast, showed the lowest percentages of companies reporting on the use of information (70%), control provisions (63%) and data protection (60%).

Percentage of companies reporting on various privacy issues they inform to customers publicly, by Industry Group



Transparency level of companies informing customers on privacy protection rights

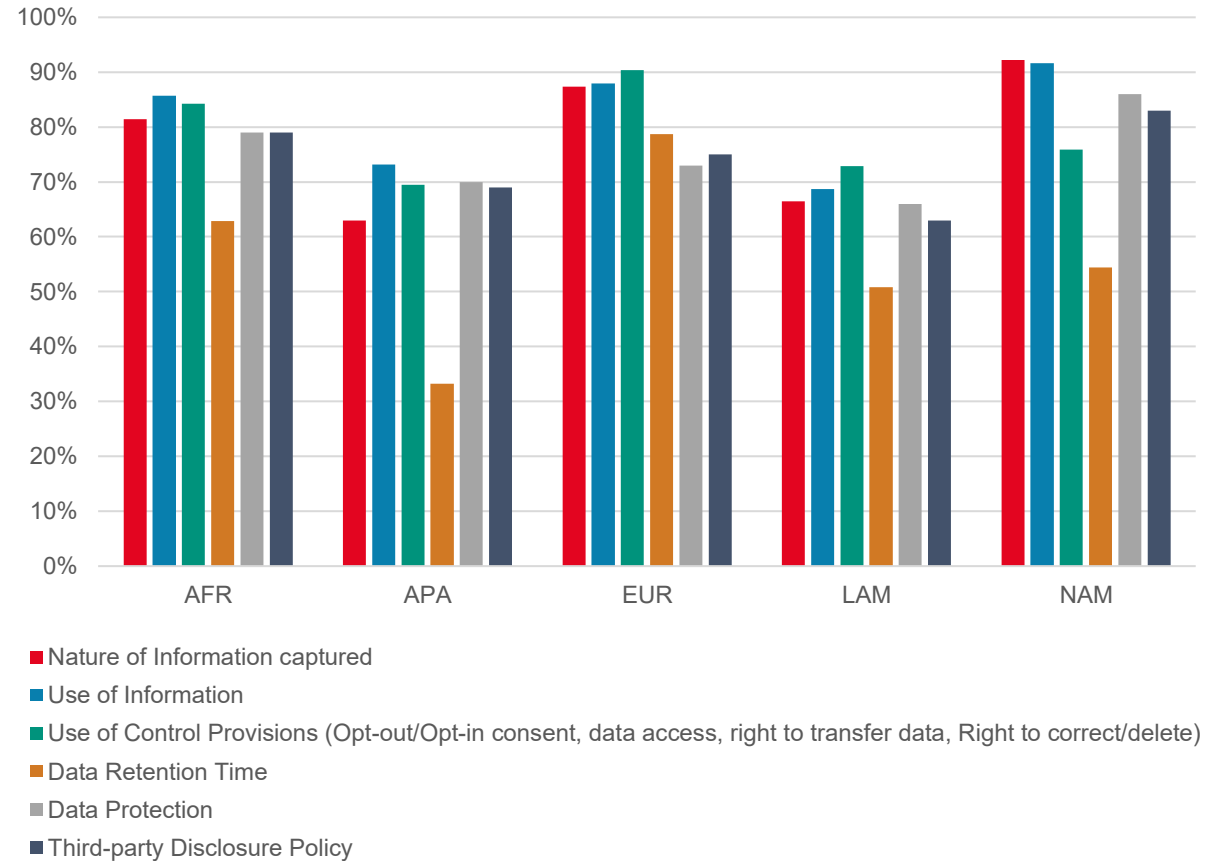
Note: The data analysis does not include companies for which this question has been considered as not applicable.

Data universe: Total number of participants

Description

- A small proportion of all companies reported on the time of data retained its customers are aware of (between 33% to 79%).
- Nevertheless, at least 60% of companies in all regions reported on other privacy issues they inform to customers.
- Europe and Latin America present a greater proportion of companies with customers knowing the extent of their private data endorsement compared to over 70% of companies in other regions sharing to customers how their information is used.
- Meanwhile, companies in North America accounted for the highest percentages reporting on privacy issues such as the nature of information captured (92%), data protection (86%), and third-party disclosure policy (83%).

Percentage of companies reporting on various privacy issues they inform to customers publicly, by Region



Source: CSA 2023

Thematic Data Analysis Report - Starter Module

The module includes:

- Benchmarking of the company performance on data-point level versus peers in the industry and countries of reference
- Gap-Analysis with respect to the CSA practice for the relevant aspects



IT Security/ Cybersecurity Governance

Cyber-Ready Leadership: Navigating Threats with Board and Executive
Collaboration





CSA Expected Practice – IT Security/ Cybersecurity Governance

Topic rationale, focus and expected practice for the topic explain the context, materiality and data used for the analysis.

Rationale

Over the past decade, the number of information security breaches has grown exponentially with some attacks reaching unprecedented scales and the cyber threat landscape continues to grow and evolve, abusing existing and new technologies and exploiting vulnerable users. These incidents and the related costs have shown that information security/cybersecurity has become a financially material issue that must be diligently managed to protect corporate value. The costs of cyberattacks are manifold and can impact the company in different ways. Internal costs are operational costs and relate to dealing with cybercrime and incidence prevention. External costs include the consequences of the cyber-attack such as the loss or theft of sensitive information, operations' disruption, fines and penalties, infrastructure damage or revenue losses due to loss of customers. Thus, ensuring the security and resilience of networks and information systems is critical. The question assesses what security measures are in place to ensure employees are aware of threat issues and the importance of information security/cybersecurity.

Focus and Expected Practice

Aspects	Focus and Expected practice description	
Involvement of board in the information security strategy		Engagement of the board of directors in the review of information security/cybersecurity strategy and relevant experience in previously held positions of the responsible board member(s)
		Board member's membership in the cyber security/information security committee
Executive Management Responsibility		Chief Information Security Officer (CISO) / Chief Security Officer (CSO) is appointed within the Executive Management team for overseeing cybersecurity in the company
		Public reporting on the executive level responsibility for IT Security / Cybersecurity

Source: CSA 2023

Cybersecurity Governance process with responsibility at board and executive level

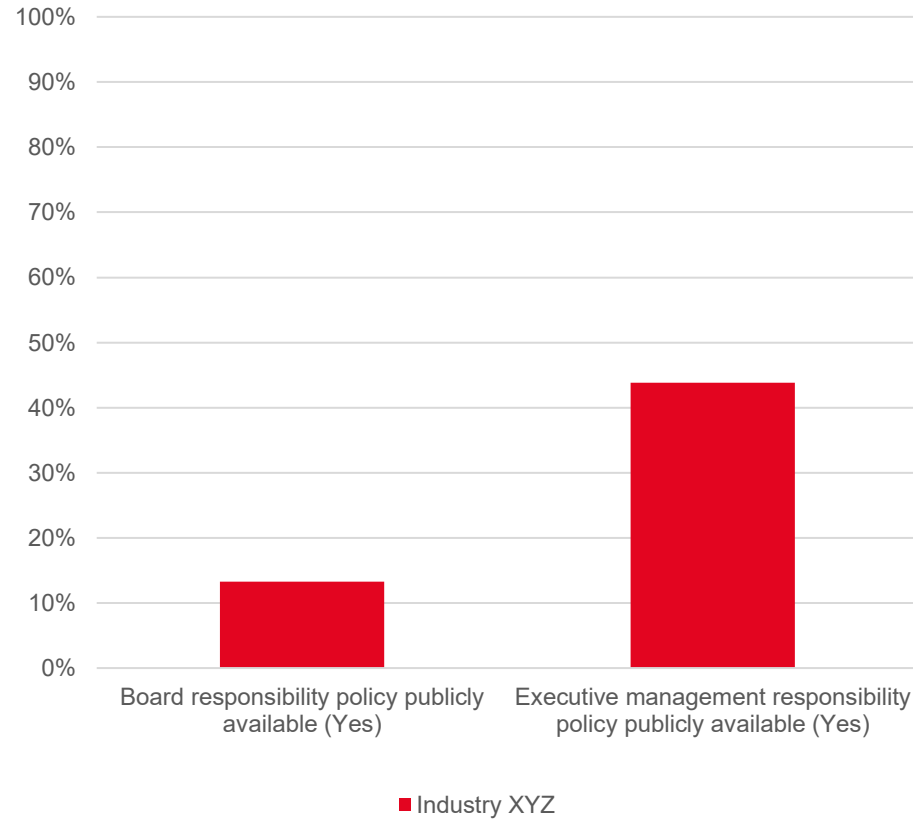
Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

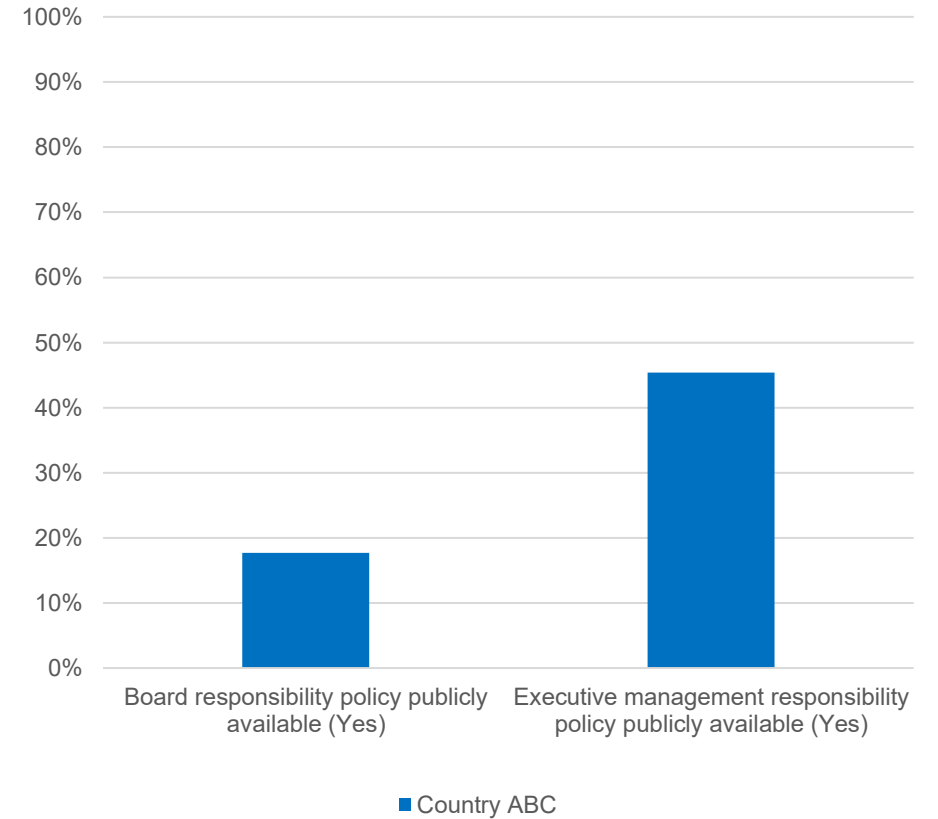
Company Performance
Board member and executive management is appointed for overseeing information security/cybersecurity

Data universe: Total number of participants

Percentage of companies having a cybersecurity governance process at board and executive level, for company's industry



Percentage of companies having a cybersecurity governance process at board and executive level, for company's country



Source: CSA 2023

Board membership in the committee which oversees cyber security strategy

Note: The data analysis does not include companies for which this question has been considered as not applicable.

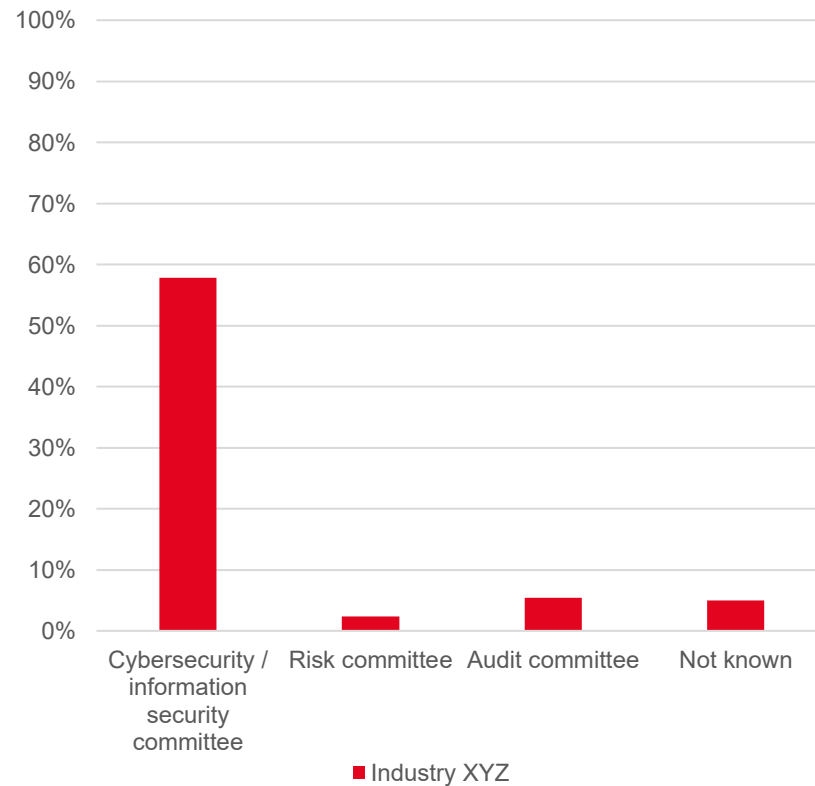
The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

Company Performance

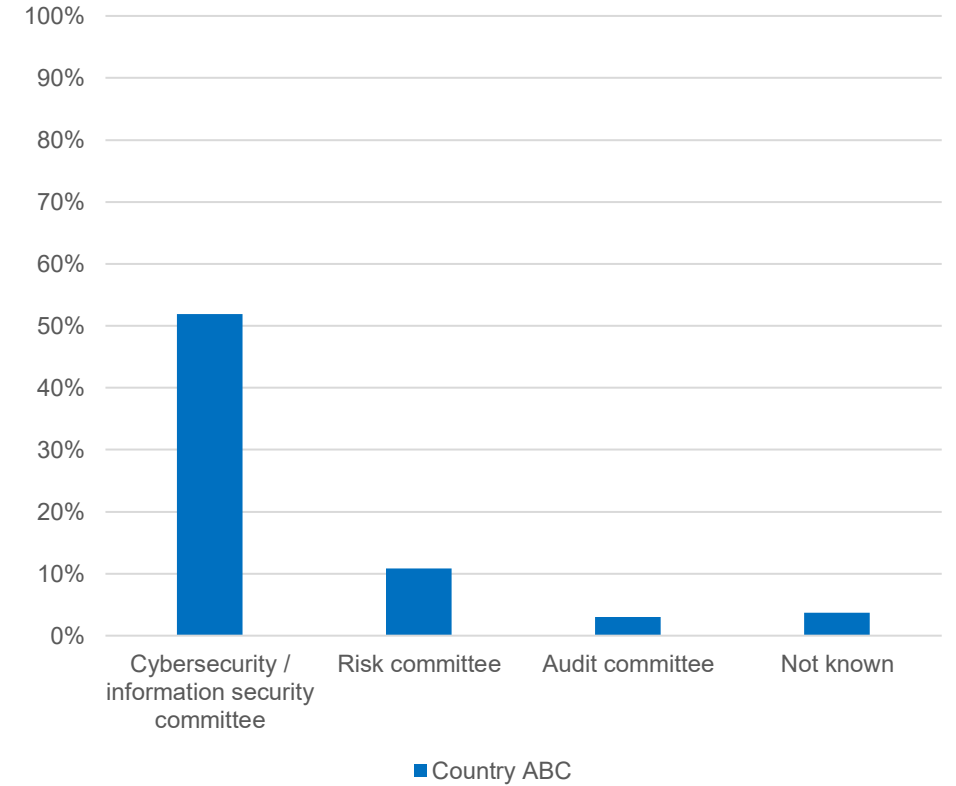
Board member's membership is in the Risk committee which oversees cyber security strategy

Data universe: Total number of participants

Percentage of companies reporting on board member's membership in the committee which oversees cyber security strategy, for the company's industry



Percentage of companies reporting on board member's membership in the committee which oversees cyber security strategy, for the company's country



Source: CSA 2023

Executive Management Responsibility

Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

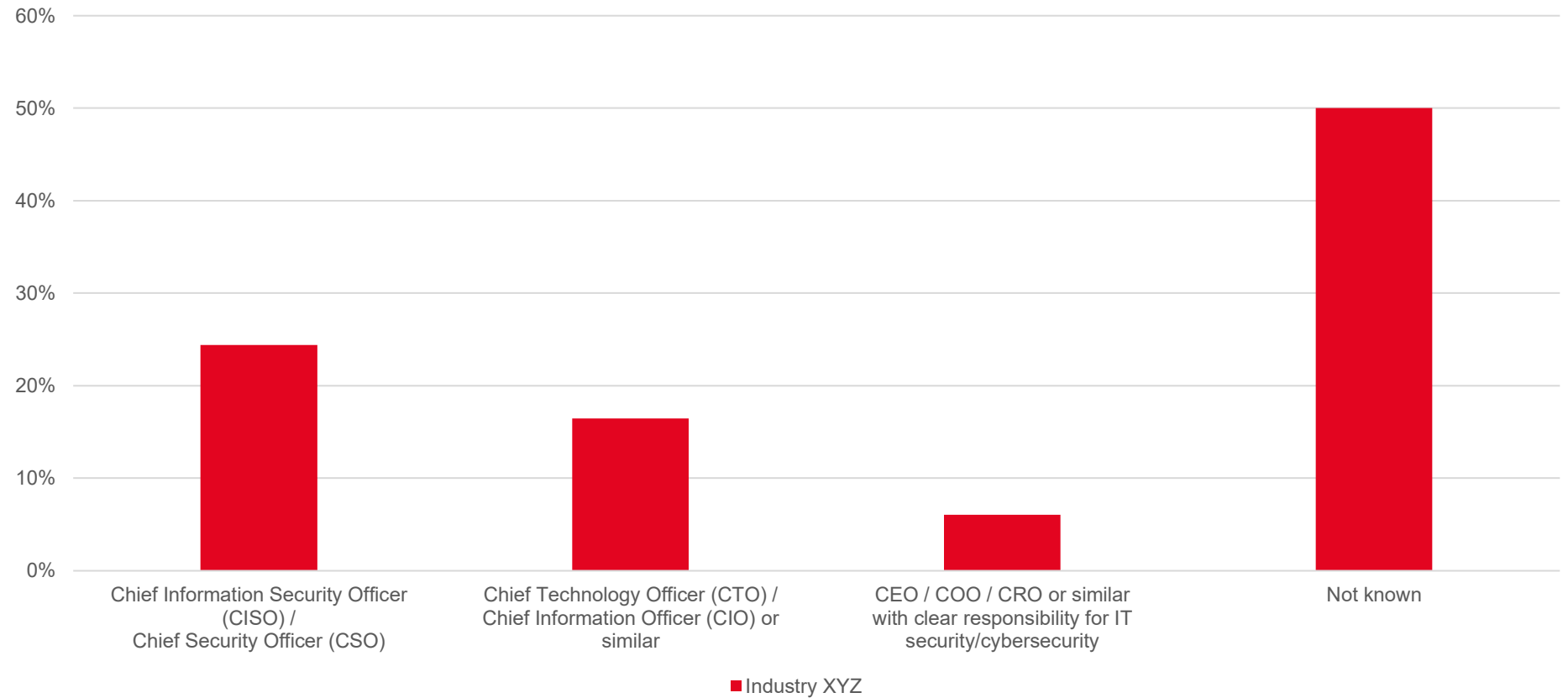
Company Performance

Chief Technology Officer (CTO) / Chief Information Officer (CIO) or similar is appointed within executive management team for overseeing cybersecurity in the company

Data universe: Total number of participants

Source: CSA 2023

Percentage of companies having a function within executive management team for overseeing cybersecurity in the company, for company's industry



Executive Management Responsibility

Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

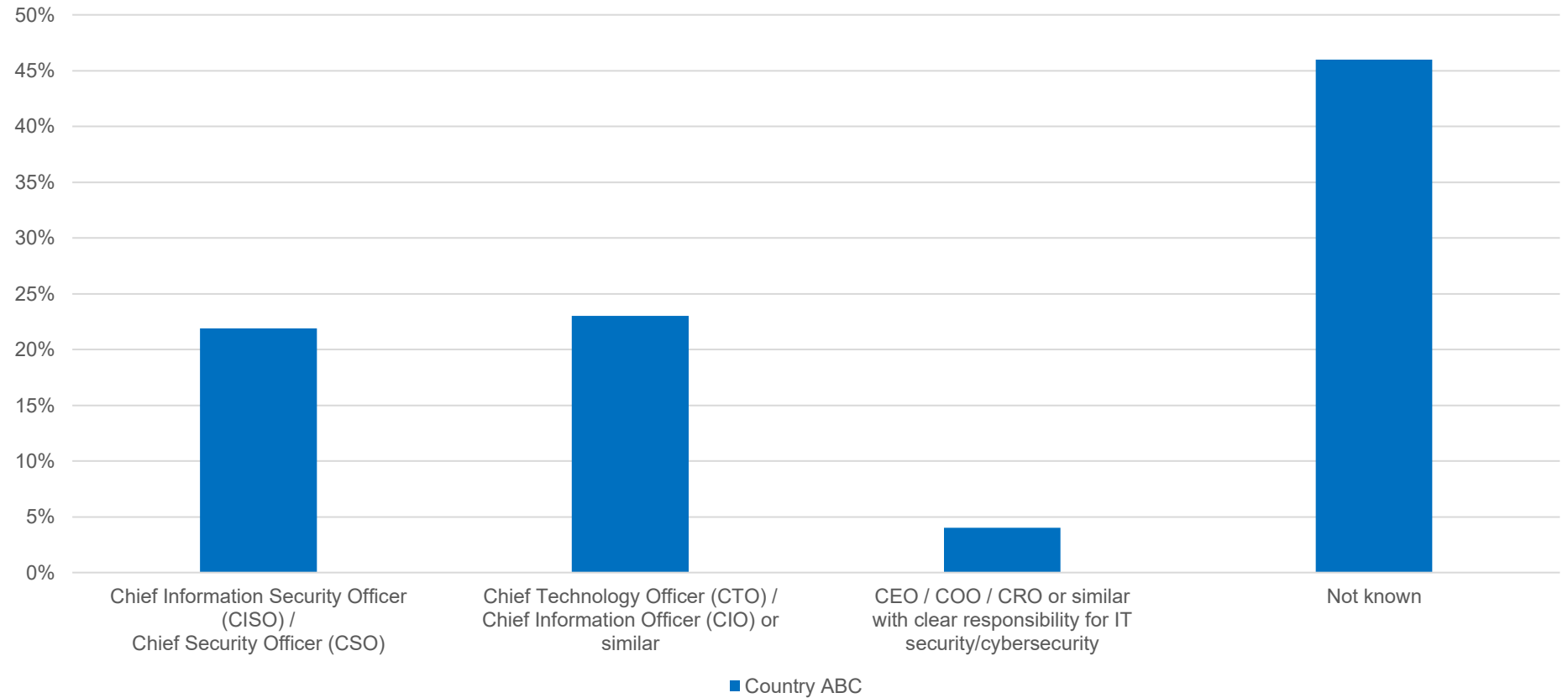
Company Performance

Chief Technology Officer (CTO) / Chief Information Officer (CIO) or similar is appointed within executive management team for overseeing cybersecurity in the company

Data universe: Total number of participants

Source: CSA 2023

Percentage of companies having a function within executive management team for overseeing cybersecurity in the company, for company's country



Types of mechanisms for effective implementation of privacy policy

Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

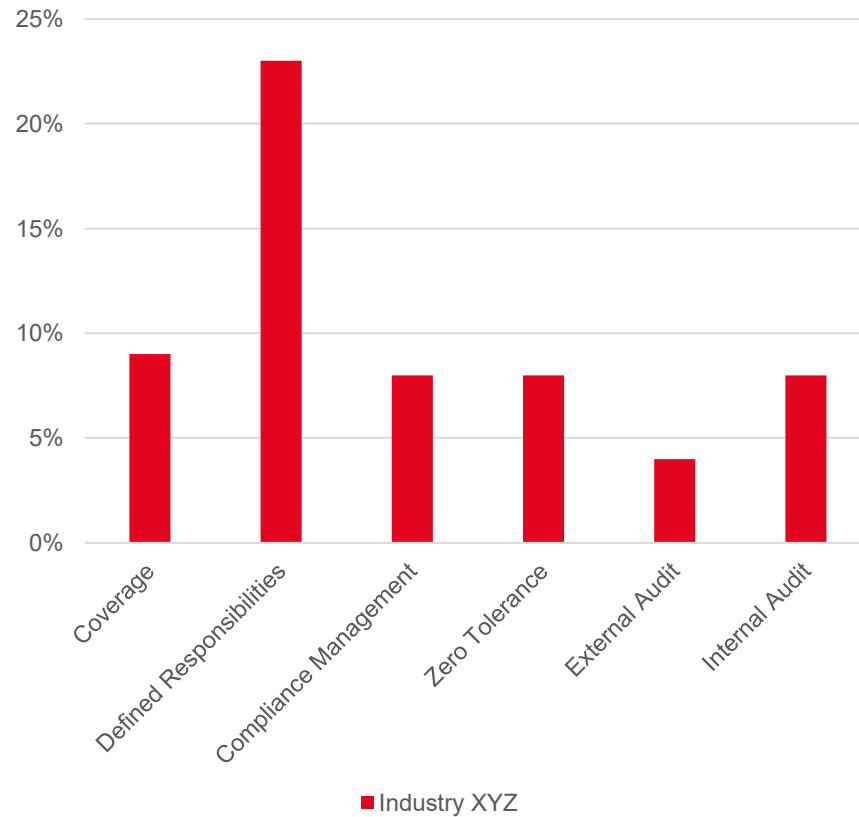
Company Performance

The company has disclosed Coverage, Responsibility and Compliance. However, no disclosure on Zero tolerance, External audit and Internal audit

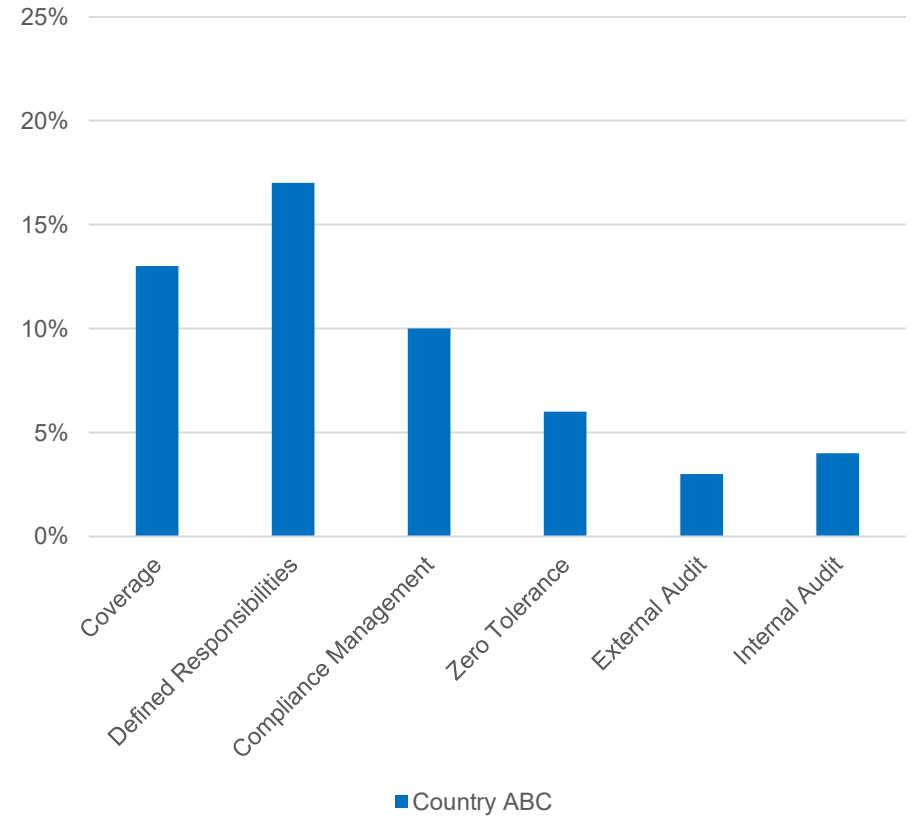
Data universe: Total number of participants

Source: CSA 2023

Percentage of companies reporting on various aspects of effective implementation of their privacy policy, in company's industry



Percentage of companies reporting on various aspects of effective implementation of their privacy policy, in company's country



Contents

X	Topic Overview and S&P Global Corporate Sustainability Assessment (CSA) Relevance for the society, company and capital market
X	Data Universe and Guidance Scope of the analysis and how to read charts and symbols
XX	Data Analysis Detailed data analysis to understand how the topic is addressed
XX	Company Performance on..... Performance of the company on the specific topic, highlighting the major gaps in terms of score with respect to the CSA practice
XX	Contact and Disclaimer

CSA Gap Analysis – IT Security/ Cybersecurity Governance

1.8.1 IT Security/ Cybersecurity Governance

Aspects	Focus and Expected practice description	Assessment
Involvement of board in the information security strategy	Engagement of the board of directors in the review of information security/cybersecurity strategy and relevant experience in previously held positions of the responsible board member(s)	Board member is engaged in the information security/cybersecurity strategy and review process and has relevant prior experience
	Board member’s membership in the cyber security/information security committee	Board member is a part of Risk Committee, and the information is available publicly. However, the company is expected to have an information security or cybersecurity committee for a maximum score
Executive Management Responsibility	Chief Information Security Officer (CISO) / Chief Security Officer (CSO) is appointed within the Executive Management team for overseeing cybersecurity in the company	Chief Digital and Information Officer is appointed within the Executive Management team for overseeing cybersecurity in the company. However, the company is expected to have a Chief Information Security Officer (CISO) / Chief Security Officer (CSO) for overseeing cybersecurity for a maximum score
	Public reporting on the executive level responsibility for IT Security / Cybersecurity	

Question Score:

- Full score
- Partial score
- Zero points
- Additional information
- Not applicable

CSA Gap Analysis – Privacy Policy: Systems/ Procedures (1/2)

3.8.1 Privacy Policy: Systems/ Procedures





Aspects	Focus and Expected practice description	Assessment	
Mechanism for effective implementation of privacy policy	Public reporting on the following measures to ensure effective implementation of privacy policy:		
	• Applicability of privacy policy to all operations including the suppliers		
	• Defined point of contact in place for escalation of privacy issues		
	• Privacy policy system embedded in group-wide risk/compliance management		
	• Disciplinary actions in case of breach (i.e. zero tolerance policy)		The company does not have disciplinary actions in place in case of breach.
			<i>The company's reported information on page 100 of the 'Sustainability Report 2023' covers processing of personal data and responds to data subject rights exercised by individuals in line with data privacy laws and regulations, however, no disclosure on disciplinary action taken in case of breach is provided. Hence, the response was not accepted.</i>

Question Score:






- Full score
- Partial score
- Zero points
- Additional information
- Not applicable

CSA Gap Analysis – Privacy Policy: Systems/ Procedures (2/2)

3.8.1 Privacy Policy: Systems/ Procedures

Aspects	Focus and Expected practice description	Assessment
Mechanism for effective implementation of privacy policy <i>(continued)</i>	 <ul style="list-style-type: none"> Third-party audits of privacy policy compliance 	 The company does not conduct third-party audits of the privacy policy compliance
	<ul style="list-style-type: none"> Internal audit of privacy policy compliance 	 The company does not conduct internal audits of the privacy policy compliance.  <i>The company's reported information on page 100 of the 'Sustainability Report 2023' covers processing of personal data and responds to data subject rights exercised by individuals in line with data privacy laws and regulations, however, no disclosure on any audit conducted is provided. Thus, the response was not accepted.</i>

Question Score:

-  Full score
-  Partial score
-  Zero points
-  Additional information
-  Not applicable

Thematic Data Analysis Report - Expert Module

The module includes:

- Descriptive statistics on scores of peer companies
- Benchmarking of the company performance on data-point level versus a strategic peer group



IT Security/ Cybersecurity Process & Infrastructure

Safeguarding Digital Frontiers: Ensuring Continuity in an Evolving Cyber Landscape

CSA Expected Practice – IT Security/ Cybersecurity Process & Infrastructure

Topic rationale, focus and expected practice for the topic explain the context, materiality and data used for the analysis.






Rationale

Due to the current trend of digitization, including but not limited to cloud computing, online marketplaces and payments, etc., it is crucial that access to networks, IT systems and data is assured at all times. As a result, lower than agreed upon system performance or service disruptions can result in higher costs and reputational risk for companies. The main risks stem from technical failure, human error, malicious attacks, weather events, natural disasters or terrorist attacks. Managing such risks, including contingency plans, is crucial to ensuring business continuity.

Thus, ensuring the security and resilience of networks and information systems is critical.

The question focuses on how well companies are prepared to prevent major IT infrastructure and information security/cybersecurity incidents and if they can react appropriately in the event of such events.

Focus and Expected Practice

Aspects	Focus and Expected practice description	
Incident response		Business continuity/contingency plans and incident response procedures in place and tested at least semi-annually
Certification	 	Information security management system certified to ISO 27001, NIST or similar
External verification and vulnerability analysis		External verification of the IT infrastructure/ information security management systems, with letter of opinion of the external auditors issued during the latest fiscal year
		Third-party vulnerability analysis conducted to assure the security of the IT infrastructure/information security management systems
		The company has conducted simulated hacker attacks as part of third-party vulnerability analysis
Breaches		Total number of information security breaches reported for the last fiscal year
		Total number of clients, customers and employees affected by the breaches reported for the last fiscal year

Source: CSA 2023

Selected Peer Groups

Industry Top 10 & Selected Peer Group

Industry top 10 2023

- Apples Ltd
- Bananas Inc
- Cucumber AG
- Dates Ltd
- Coffe Holdings Co
- Grapefruit NV
- Honey AG
- Sample compay
- Hummus Corporation
- Lasagna Automotives

Selected Peer Group 2023

- Apples Ltd
- Bananas Inc
- Dates Ltd
- Cucumber AG
- Coffe Holdings Co
- Grapefruit NV
- Honey AG
- Sample compay
- Hummus Corporation
- Lasagna Automotives

Company XYZ's Performance vs. Selected Peer Group

The name of the companies included in this peer group is available on page 31 of the report.

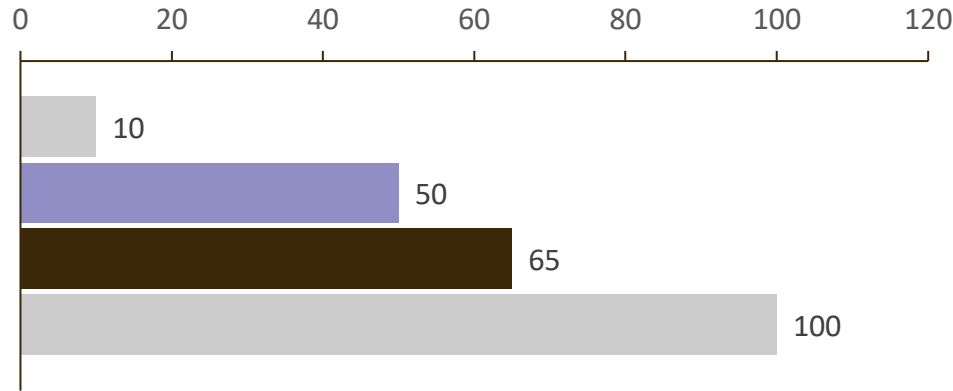
- Lowest Score
- Peer Average
- Company XYZ
- Best Company Score

The histogram shows for each score decile, the frequency in %, i.e. the % of companies in the peer group that score in a certain range, as well as the score of your company.

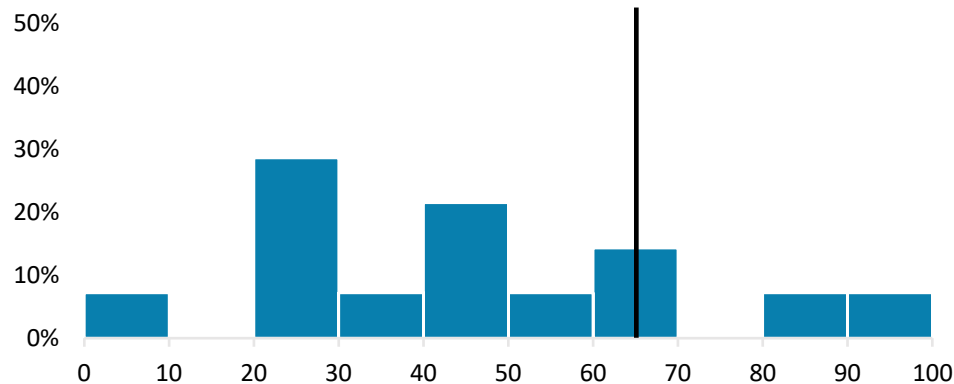
N/A: The question is introduced in 2021. Therefore, delta YOY is not available.

Source: CSA 2023

Company Performance vs. Peer Group, 2023



Score Distribution for Companies Analyzed in the Peer Group 2023



Key Metrics: Company Compared to Selected Peer Group

Company Rank (Percentile)	79
Relative to best company (%)	65

YoY Changes in Selected Peer Group

Descriptive Value	Δ YoY
Lowest Score	5
Peer Average	10
Company XYZ	20
Best Company Score	25

Key Statistics: Selected Peer Group

Descriptive Value	Companies Analyzed
Average	50
Standard deviation	24
Percentage <i>Not Applicable</i> *	7%
Number of companies analyzed	14

* Percentage of companies in the industry for which Not Applicable was accepted for this criterion.

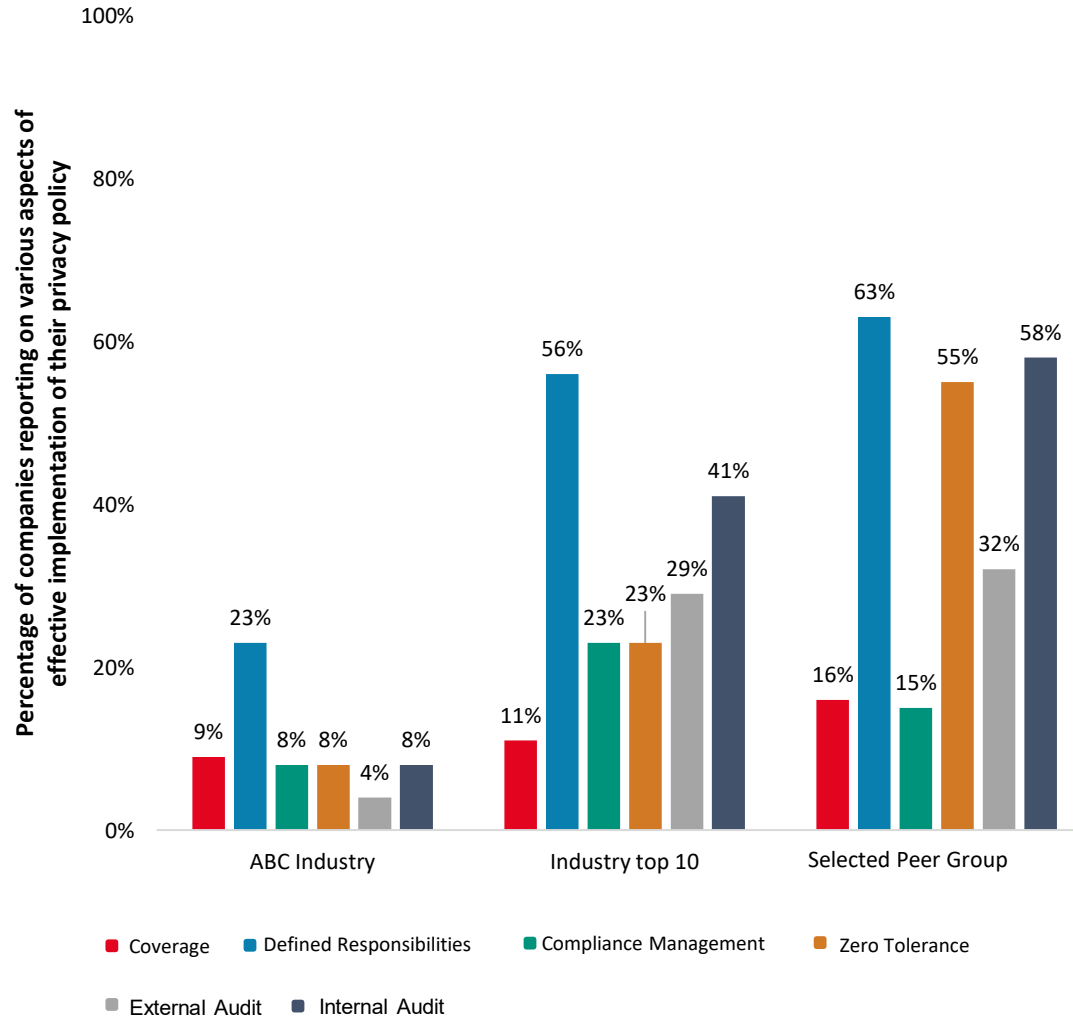
Company score

Data Breakdown on the company’s adoption of metrics to measure impact on privacy policy

Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company’s industry and country of reference, as classified by GICS and S&P Global, are in scope.

Total assessed companies in CSA 2023: XXXX



Size of the Peer Groups

Peer Group	Number of Companies 2023
Industry	136
Industry Top 10	10
Selected Peer Group	14

Source: CSA 2023

External verification and third-party vulnerability analysis of IT infrastructure / Information Security Management Systems

Note: The data analysis does not include companies for which this question has been considered as not applicable.

The company's industry and country of reference, as classified by GICS and S&P Global, are in scope.

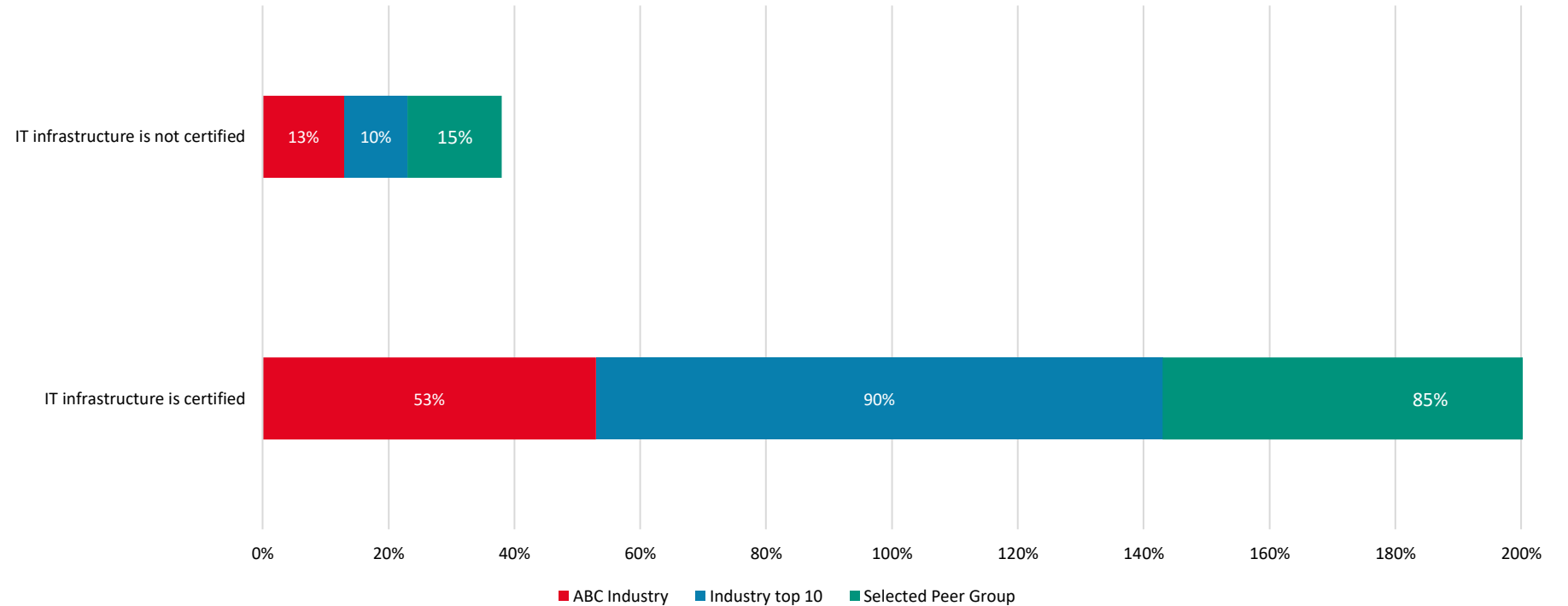
Company Performance

The company has conducted third-party vulnerability analysis. However, no external verification and simulated hacker attacks

Data universe: Total number of participants

Source: CSA 2023

Percentage of companies having their IT infrastructure and information security management system certified to ISO 27001, NIST or similar



Contents

X	Topic Overview and S&P Global Corporate Sustainability Assessment (CSA) Relevance for the society, company and capital market
X	Data Universe and Guidance Scope of the analysis and how to read charts and symbols
XX	Data Analysis Detailed data analysis to understand how the topic is addressed
XX	Company Performance on..... Performance of the company on the specific topic, highlighting the major gaps in terms of score with respect to the CSA practice

XX	Contact and Disclaimer
----	-------------------------------

Your Contact at S&P Global

Sustainability Benchmarking Services
S1BenchmarkingServices@spglobal.com
www.spglobal.com/esg/csa/esg-benchmarking

S&P Global Switzerland SA

Zurich Branch
Neumuehlequai 6
8001 Zurich
Switzerland

Disclaimer

This content (including any information, data, analyses, opinions, ratings, scores, and other statements) (“Content”) has been prepared solely for information purposes and is owned by or licensed to S&P Global and/or its affiliates (collectively, “S&P Global”). This Content may not be modified, reverse engineered, reproduced or distributed in any form by any means without the prior written permission of S&P Global. You acquire absolutely no rights or licenses in or to this Content and any related text, graphics, photographs, trademarks, logos, sounds, music, audio, video, artwork, computer code, information, data and material therein, other than the limited right to utilize this Content for your own personal, internal, non-commercial purposes or as further provided herein. Any unauthorized use, facilitation or encouragement of a third party’s unauthorized use (including without limitation copy, distribution, transmission or modification) of this Content or any related information is not permitted without S&P Global’s prior consent and shall be deemed an infringement, violation, breach or contravention of the rights of S&P Global or any applicable third-party (including any copyright, trademark, patent, rights of privacy or publicity or any other proprietary rights). A reference to a particular investment or security, a score, rating or any observation concerning an investment or security that is part of this Content is not a recommendation to buy, sell or hold such investment or security, does not address the suitability of an investment or security and should not be relied on as investment advice. S&P Global shall have no liability, duty or obligation for or in connection with this Content, any other related information (including for any errors, inaccuracies, omissions or delays in the data) and/or any actions taken in reliance thereon. In no event shall S&P Global be liable for any special, incidental, or consequential damages, arising out of the use of this Content and/or any related information. The S&P and S&P Global logos are trademarks of S&P Global registered in many jurisdictions worldwide. You shall not use any of S&P Global’s trademarks, trade names or service marks in any manner, and in no event in a manner accessible by or available to any third party. You acknowledge that you have no ownership or license rights in or to any of these names or marks.

Adherence to S&P’s Internal Polices

S&P Global adopts policies and procedures to maintain the confidentiality of non-public information received in connection with its analytical processes. As a result, S&P Global employees are required to process non-public information in accordance with the technical and organizational measures referenced in the internal S&P Global Information Security and Acceptable Use policies and related guidelines.

Conflicts of Interest

S&P Global is committed to providing transparency to the market through high-quality independent opinions. Safeguarding the quality, independence and integrity of Content is embedded in its culture and at the core of everything S&P Global does. Accordingly, S&P Global has developed measures to identify, eliminate and/or minimize potential conflicts of interest for Sustainable1 as an organization and for individual employees. Such measures include, without limitation, establishing a clear separation between the activities and interactions of its analytical teams and non-analytical teams; email surveillance by compliance teams; and policy role designations. In addition, S&P Global employees are subject to mandatory annual training and attestations and must adhere to the Sustainable1 Independence and Objectivity Policy, the Sustainable1 Code of Conduct, the S&P Global Code of Business Ethics and any other related policies.

For information provided as part of the CSA questionnaire refer to our “Use of Information and Confidentiality Policy” https://portal.csa.spglobal.com/survey/documents/Use_of_Information_Policy.pdf and for personal information provided to S&P refer to S&P Global’s Privacy Policy: <https://www.spglobal.com/en/privacy/privacy-policy-English>. See additional Disclaimers at <https://www.spglobal.com/en/terms-of-use>.

Copyright© 2024 S&P Global Inc. All rights reserved.