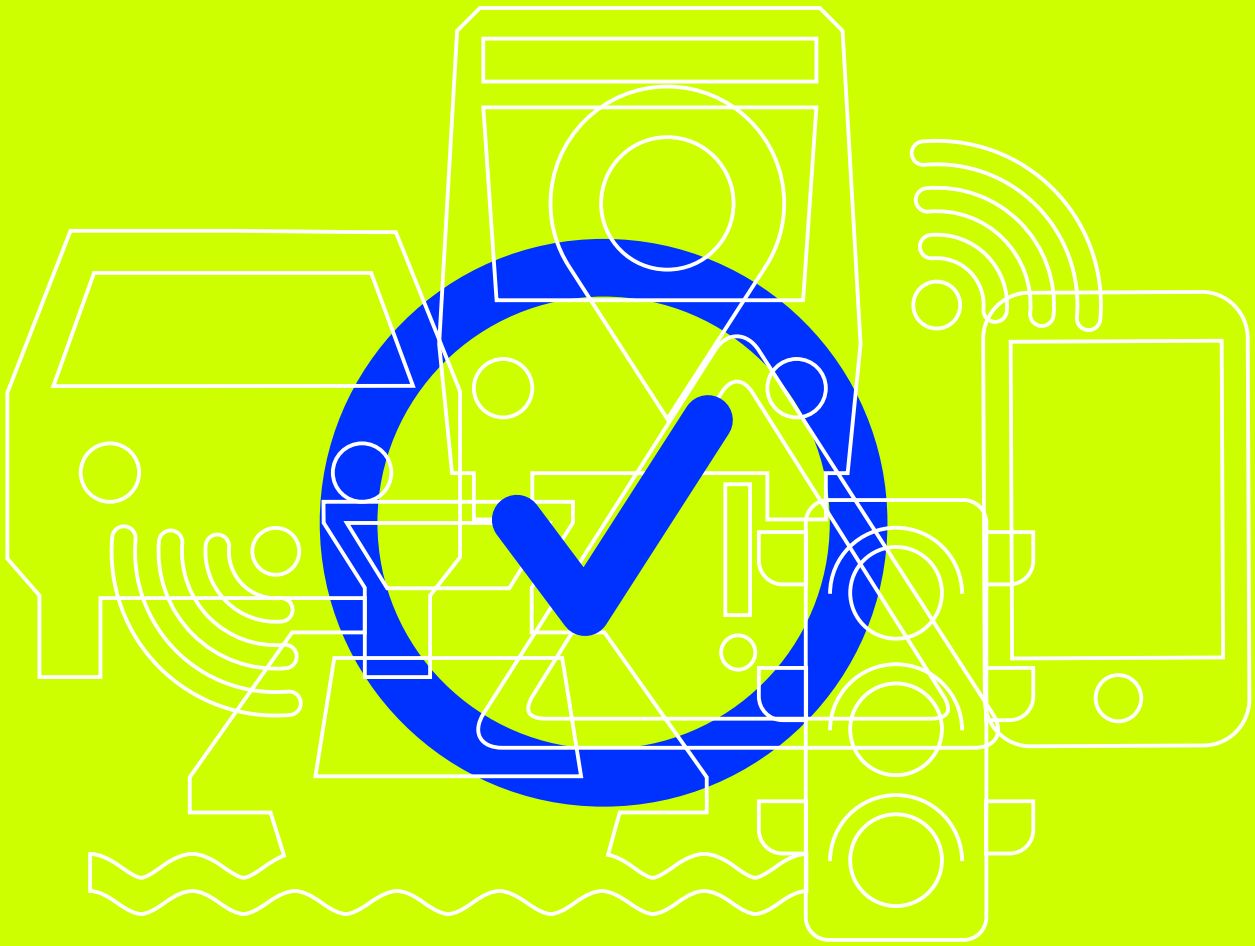
HANDLEIDING VEILIGE DATA-UITWISSELING DEELMOBILTEIT

City Data Specificatie-Mobiliteit (CDS-M)



CDS-M

City Data
Specificatie-Mobiliteit

REPORT QUICKSCAN CYBERSECURITY VAN VIANOVA

Lees meer over hoe CDS-M scoort op het gebied van cybersecurity.

Report QuickScan Cybersecurity

Cybersecurity & Privacy assessment Vianova

Date	:	23 juni 2022
Version	:	0.8-Concept
ID	:	GMA22004

kienia
industriële automatisering

Revision history

Table 1 Revisions

Version	Datum	Who	What
0.1	19-05-2022	Jurian Hage / Bert Drijver	First draft, base was interview on June the 22nd
0.2	30-06-2022	Jurian Hage / Bert Drijver	Complete text without tables
0.4	28-07-2022	Bert Drijver	Adaptions Questions Vianova
0.7	02-08-2022	Bert Drijver	Added the Excel tables
0.8	22-08-2022	Bert Drijver	Changed after review

Input documents

Ref.	Document	Version	From
(ISO)	NEN-EN-ISO / IEC 27001:2017	2017	ISO
(NIST)	NIST.SP.800-53r5	R5	NIST (National Institute of Standards and Technology)
(IBM)	20180821-grip-on-ssd-security-requirements-v20-2.pdf	2.0 2014	IBM
(GMA)	AVW Cyber 20042021.pptx	n.a.	Amsterdam

The table above provides an overview of the input documents that were used in setting up this advisory report. References to documents in this list will be made using the Ref. column.

Classification

Confidential: the content may not be shared with others without the permission of the copyright owner.

Contents

1 Introduction

The five largest cities in the Netherlands are working together on shared mobility. The aim of the collaboration between the five largest Dutch municipalities and Vianova is to support shared mobility policy in general with the use of data. They contracted Vianova to build the technical platform to realize this goal. Vianova's task is to provide the municipality with data on the use of shared mobility in a cyber secure way. Compliance with the EU General Data Protection Regulation (GDPR) is especially important for governments. Of course, this also applies to the five largest Dutch municipalities. With regard to the GDPR, it is essential that personal data is not shared unnecessarily. To collaborate with mobility providers, detailed data about, for example, a one-way journey is not necessary. The five largest municipalities want to know how Vianova has incorporated the requirements in the field of cybersecurity into the organization. The municipality of Amsterdam (representing the five largest municipalities) has asked KienIA to investigate Vianova's cybersecurity and GDPR maturity. This report is a so-called cyber security quick scan.

1.1 Introduction of Vianova

Vianova is building the digital layer between cities and operators to foster collaboration and facilitate modal shift toward more sustainable and accessible modes of transport. Vianova has 5 offices across Europe and is backed by RATP and Rebel Group. The RATP Group (French: Groupe RATP), also known as the RATP or Régie autonome des transports Parisiens, is a state-owned public transport operator and maintainer headquartered in Paris, France. The Rebel Group. Rebel works on the issues of the future in the fields of sustainability, transport, urban development, health care and the social sector. Besides that, the company is also as an investor. Further Vianova is audited annually by the investors.

The offices of Vianova are established in Paris, Zürich, London, Berlin and Barcelona.

Vianova has around 25 employees. The interview is with Frédéric Robinet, the Chief Technology Officer of Vianova.

1.2 Conform international standards

The cybersecurity requirements, about which questions have been asked for a secure infrastructure and organization, are described in the ISO 27001, ISO 27002, the NIST and NCSC standard. The document that Amsterdam has provided is "20180821-grip-on-ssd-security-requirements-v20-2.pdf".

2 The CS QuickScan

The CS QuickScan was set up get an impression of the maturity of the CS Vianova. The scan used the (ISO) as a guide.

In addition to the (ISO) questions, questions were also asked about requirements from the (NIST) and NCSC.

2.1 Products guided by ISO 27001

The CS QuickScan is not a formal audit. It is just a snapshot based on a survey, questions via e-mail and interview. The QuickScan consists of a couple of products that together cover the main topics from the entire (ISO). Each product is a composition of themes from (ISO). Each of the themes is subdivided into questions, after which a diagram is made of how the Plan, Do, Check and Act (PDCA) cycle is used within the themes.

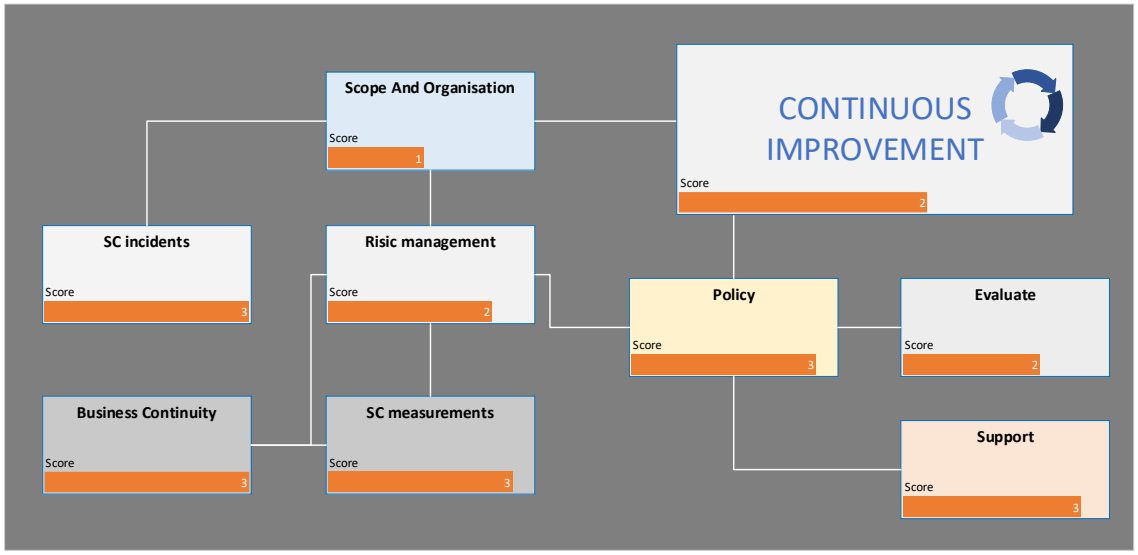


Figure 1: Questions are depicted above

The quality aspects that have been considered in the questions of this infrastructure CS quick scan are:

- Availability.
- Integrity.
- Confidentiality.

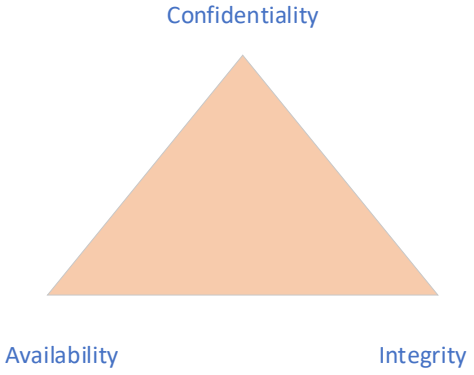


Figure 2: Availability vs. Confidentiality

The architecture Vianova uses, prioritizes confidentiality over integrity and availability. Of course, data integrity is also especially important. Personal data is too important and should be treated confidential.

2.2 The CS maturity score

The answers from the survey and the interview were converted into an CS maturity score that was applied to several products and associated themes. Figure *3* provides an overview of the 5 maturity levels that we distinguish with a brief explanation of what each level entails.

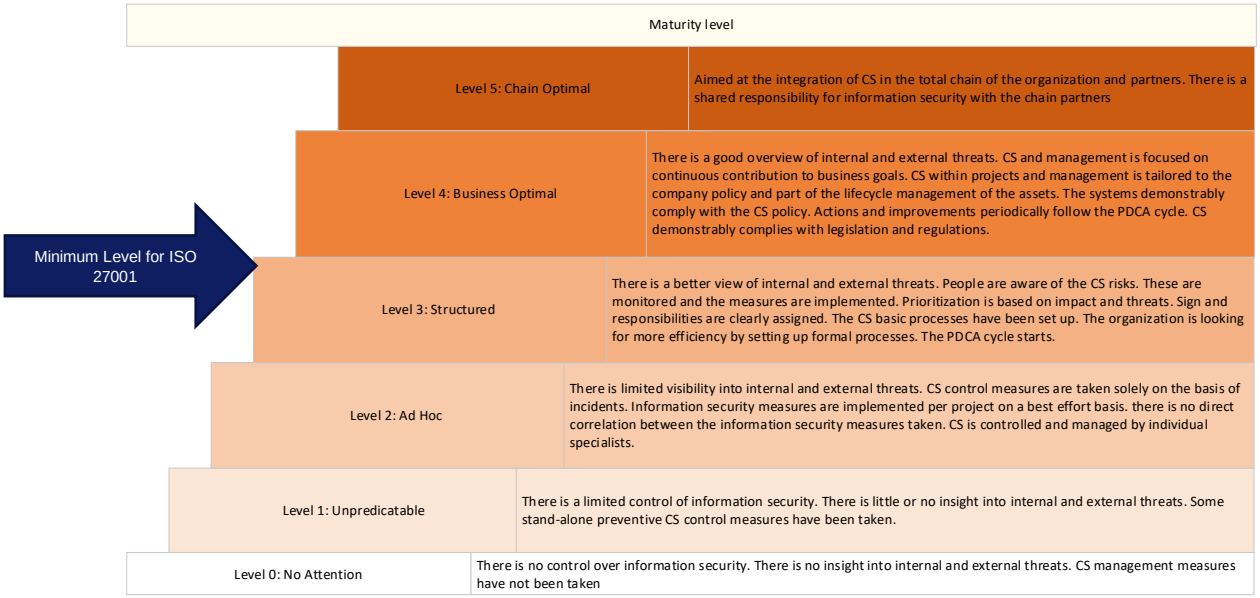


Figure *3*: Maturity levels according (ISO)

This maturity level 3 is the minimum required to demonstrably comply with the standard (ISO). The score can have a value of 0, 1, 2 or 3 or in between.

The questions in the survey are tailored to get an impression of Vianova's maturity and is not an audit for the maturity level.

3 The scope of the CS QuickScan

The municipality wants to get an impression of the cybersecurity, the protection of sensitive data and the organization of Vianova.

Vianova's mobility dashboards improve collaboration and communication between cities and transport services, so that public space is shared more efficiently, and the policy is carried out. The municipality has access via Vianova to mobility data from the various providers. It is possible for Vianova to search the database for real-time and historical data.

Vianova delivers high-quality data, reports, and dashboards. Municipalities can use the data for policy and important too: shared mobility makes the cities greener Cityscope is one of the products Vianova supplies and helps to improve mobility.

An example question many cities (and operators) ask about mobility is simple: where are the mobile assets?

With the help of Cityscope, various KPIs of vehicles can be requested:

- total number of vehicles on the street,
- percentage of total vehicles functional,
- average number of trips per vehicle.

Figure 4 KPI's example

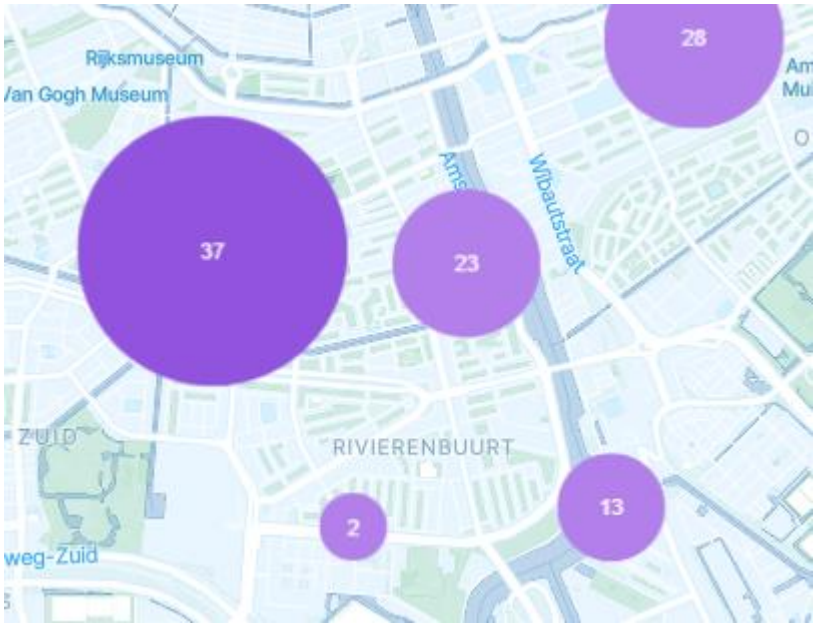


Figure 5 Number of transport assets

Vianova is a company with 5 branches throughout Europe where employees work together with the same products.

The functionality requires that the data must be accessible throughout Europe. Software development and testing must also be location independent. This requires secure infrastructure and software.

Vianova solutions enable cities to integrate and manage connected, shared and autonomous mobility in the public space.

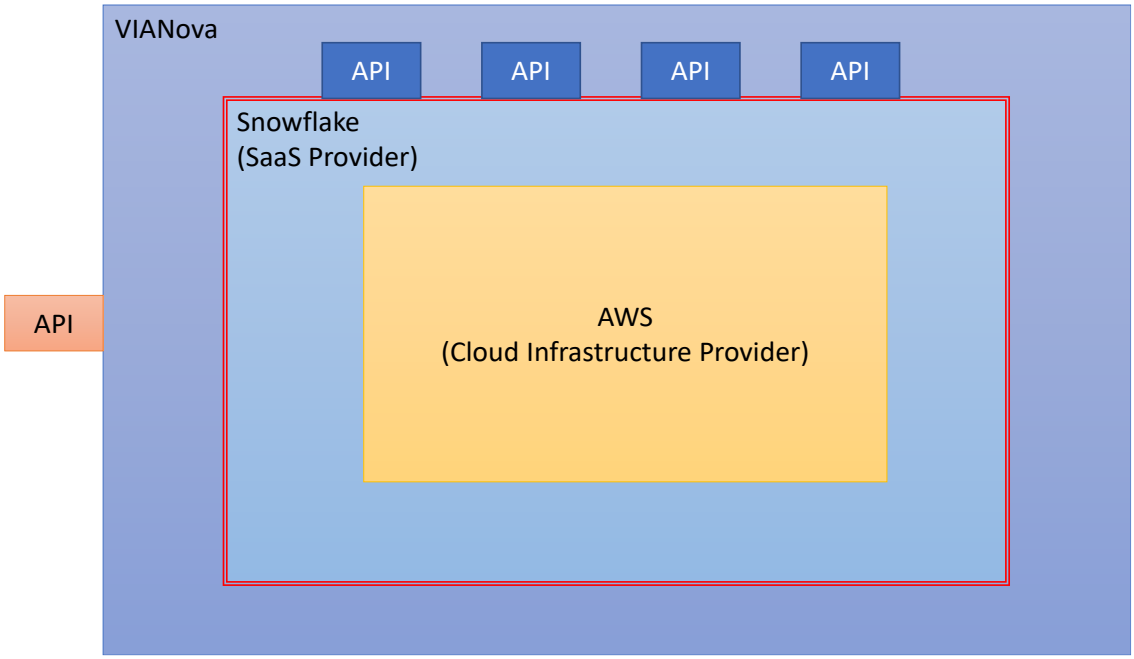


Figure 6 The rectangle is the cs quick scan scope

With this report we give an impression of CS security.

3.1 Software development and security

We realize that there are many more tools used to develop the API's and dashboards than those discussed during the interview. Importantly, the results of the cybersecurity tests performed are followed up by a change, this process is in place. SC tests are part of the development cycle. The test results should be documented as well. The next section refers to the infrastructure and tools used.

Table 1: Vianova infrastructure and tools

Product	Application
AWS	Amazon Web Services, Cloud platform, Infrastructure as a Service, IAAS, solution
Google drive	Google Storage documents
Google products	Google is an American multinational technology company for a huge variety of services and products
Okta	Is an American identity and access management company
Prowler	Prowler is an Open-Source security tool to perform AWS security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness.
Snowflake	Software as a Service, SaaS, solution

3.1.1 Amazon Web Services

Amazon Web Services (AWS) is the cloud platform of the American e-commerce giant Amazon. AWS is a comprehensive cloud computing platform that includes Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offering. AWS services offer scalable solutions for compute, storage, databases, analytics, and more. AWS has datacentres all over the world.

Scalability is important for Vianova. If a new city wants to use Vianova's services, it is important to increase its resources in a very flexible way.

3.1.2 Snowflake

Snowflake is a Software as a Service, SaaS, solution. With Snowflake a developer can create applications that auto-scale and can be deployed globally and across clouds. There is no software to install of configure. Maintenance and upgrades are managed by Snowflake. Snowflake runs completely on public cloud infrastructure like AWS.

Snowflake is HIPAA, PCI DSS, SOC 1 and SOC 2 Type 2 compliant. We focus on SOC 2. SOC 2 type 2 is important for the municipalities. A SOC 2 compliance report is tailored to the unique needs of the organization. Depending on its specific business practices, each organization can design controls that follow one or more principles of trust. These internal reports provide organizations and their regulators, business partners, and suppliers, with essential information about how the organization manages its data. There are two types of SOC 2 reports:

- Type 1 describes the organization's systems and whether the system design complies with the relevant trust principles.
- Type 2 details the operational efficiency of these systems.

Compliance with SOC 2 requirements indicates that an organization maintains a high level of information security. Strict compliance requirements (tested through on-site audits) help to ensure that sensitive information is handled responsibly by Snowflake.

3.1.3 Access management with Okta

Okta is a secure identity cloud that links all your accounts, logins and devices into a unified digital fabric. This service is named IdaaS, Identity as a Service.

Identity and access management is technology used to classify users and groups in a software system, as well as what resources they can access and what functions they can perform. Okta or IdaaS, addresses authentication, authorization, account management and access control.

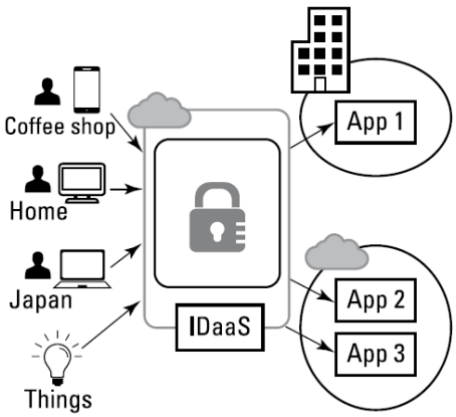


Figure 7 Location independent Access

3.1.4 Assessment tool Prowler

Prowler is an Open-Source security tool to perform AWS security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness. It contains more than 240 controls covering CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS and custom security frameworks[1].

[1] https://github.com/prowler-cloud/prowler

4 The results CS QuickScan

The first part is the used infrastructure and used cloud environment. This chapter continues with the results of the quick scan.

4.1 Average CS maturity level

Figure 8 shows the mean CS maturity level for Vianova across the subjects. The maximum score that can be achieved in this CS quick scan is 3. The orange line indicates the current CS maturity level for each subject.

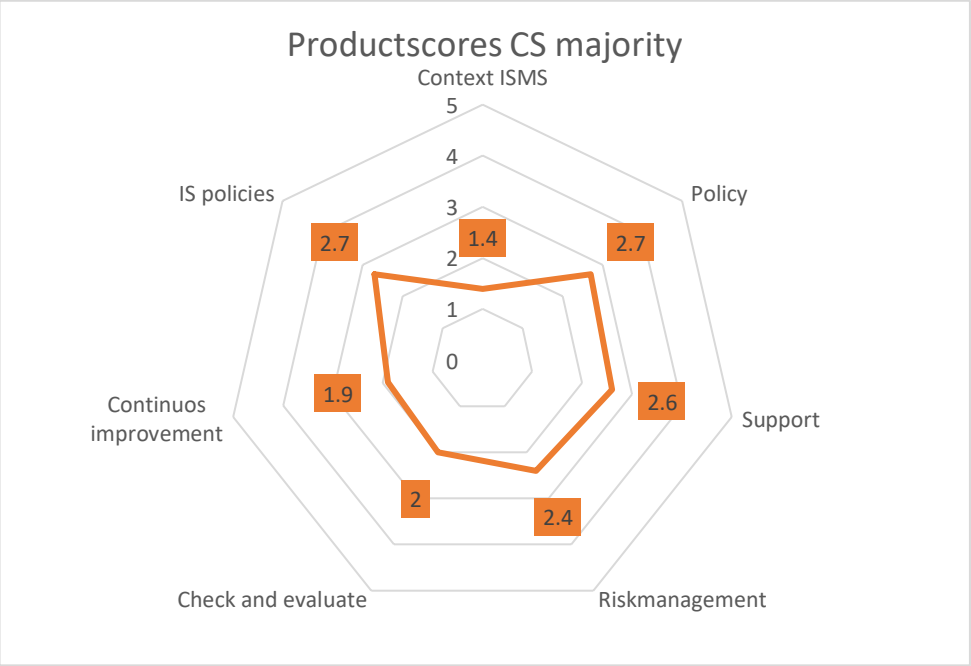


Figure 8: Score per subject

The average score on the subjects is above 2. This means that Vianova has in maturity level between 2 and 3 in CS. The absolute score is not very important, but the range of the score per subject is.

4.2 CS maturity level per subject

An average score, however, provides little insight into how you as an organization can improve. This section shows the scores achieved. The scores were determined based on the interview and email exchange we had with Vianova.

Table 2: table maturity per subject

Subject	Score	Maturity level	Characteristic
Context ISMS	1,4	1 – 2	ad hoc
Policy	2,7	2 – 3	structured
Support	2,6	2 – 3	structured
Risk management	2,4	2 – 3	structured
Check and evaluate	2	2 – 3	structured
Continuous improvement	1,9	1 – 2	ad hoc
IS policies	2,7	2 – 3	structured

4.3 Dashboard – CS maturity level per subject

Figure 6 shows the overview of the results achieved per theme from (ISO). The current maturity is shown in a bar-chart, scaled from 0-3.

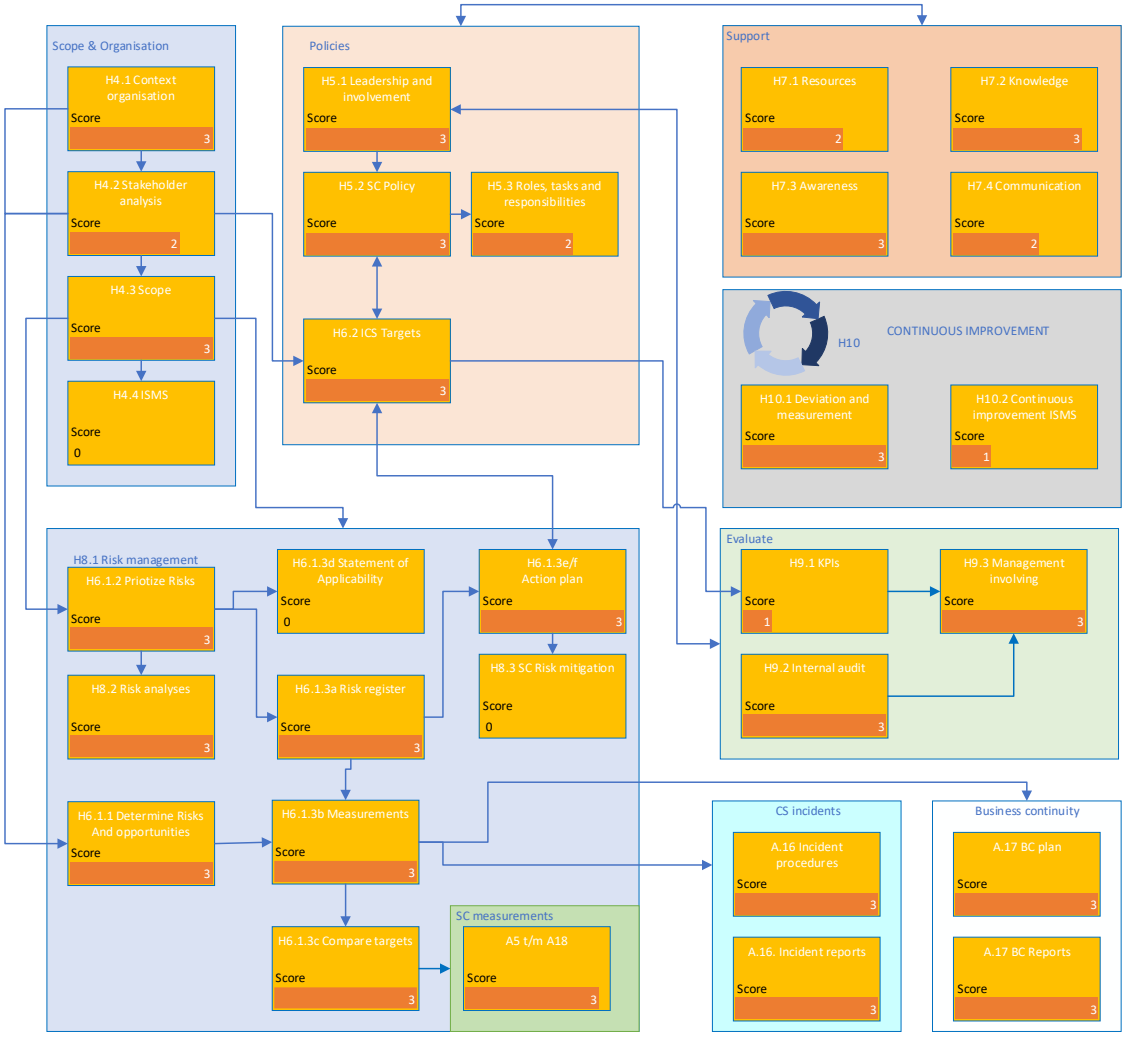


Figure 9: Dashboard with a few details

The objects are described in more detail in the conclusion. The score indicates the range.

5 Conclusion

OT Cybersecurity is part of daily business operations.

The Vianova organization has clearly chosen to make time, capacity and money available to keep CS at a high level of maturity. Roles, tasks and responsibilities are clearly assigned and secured by the board, management and software developers.

CS is not seen as a separate topic that you have to deal with but is part of the daily work.

CS is core business for Vianova because it is an important selling point. Major suppliers and tools ensure that the systems meet industry standards and requirements. At Vianova, every employee is also responsible for the CS.

If a data breach has taken place, it is bad for the image of Vianova and the municipalities and can even have financial consequences.

5.1 Agile development

Agile development, used by Vianova, is an iterative method of software development that teams can use in projects. Self-organized, cross-functional teams often analyse conditions and user needs to adapt projects.

Vianova uses the information and knowledge of The Open Web Application Security Project, OWASP, to improve software security. The OWASP Foundation is the resource for developers to secure the web and their applications. The CS tests have been documented and an example has been shared with Kienia. The product development cycle is well organized and supported by procedures. Security testing is part of the development, new functionality or bug fixes are not accepted in production until the software has gone through a quality process.

Vianova has an incident management procedure. Any software improvements are also included in the development process after an incident has been resolved. The service desk is manned alternately, which we see as a good way to share knowledge about incidents. Code reviews are common at Vianova. The PDCA Deming cycle is followed, and software development is at a professional level.

5.2 New employee process

When hiring new people, a procedure is followed and consists of several interviews. The procedure also includes bit of coding. The Chief Technical Officer is responsible for hiring new employees.

5.3 Backup.

For the users of the products Vianova delivers it is important to think about continuity with a certain reliability and availability. That means a backup a strategy and backup plan:

- There are backups in a different environment,
- Tests are performed,
- Loss of data can be prevented,
- The complete environment can be rebuilt in the Snowflake environment.

The complete environment required for Vianova’s products can be restored in the cloud. That is particularly important for the continuity of the services delivered.

5.4 Business Continuity Plan

Vianova has a backup recovery plan in the event of a service failure. At this point, moving from AWS to Google Cloud has not been evaluated and the answer to the time involved has not yet

been clarified. The time needed to move from AWS to AWS is not yet clear, but it is possible to execute.

5.5 Transport Layer Security

Interfaces used by Vianova are secured with TLS. TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established. Vianova uses valid and trusted SSL certificates for their websites.

5.6 PCI-compliant

It is not necessary for Vianova to be Payment Card Industry Data Security Standard, PCI, compliant as no payments are processed. Snowflake however is PCI-compliant.

5.7 Authorisation and Authentication

Authentication and authorisation physical access and logical access are structured via an employment checklist procedure. Logical access is important for a company like Vianova and 2FA has been set up for this. A badge is used for physical access to the office.

Okta is a security wise choice for IDaaS and give a specialized company the complex task in the cloud in a flexible way. Okta has support for API's as well.

5.8 Company audit

A complete company audit is performed regularly for the investors. An (ISO) audit is scheduled for 2023. A risk analysis has been performed and a risk matrix is available.

5.9 Penetration test

A penetration test, pen test, is an authorized simulated attack performed on a computer system to evaluate the security of the used system. A pen-test has been performed, one critical was found and is solved.

5.10 GDPR

Special attention is paid to the GDPR. The example of the Bradley taxi is used to indicate that GDPR is included in the development process. A distinction is made between direct and indirect personal data. Data is aggregated so that Vianova prevents data from being traceable to a person. The aggregation of trips consists of at least three different trips. [2]

The data retention period is configurable and after that period the data is deleted in an automatic cleaning process.

The organization has set itself the goal and thus the ambition to start with a (ISO) certification at the end of 2022 or early 2023.

There is no clean desk and clear screen policy, so working in a public place, such as a coffee shop or at home, can pose a risk of unintentionally sharing information.

5.11 OMF and GDPR

At Vianova, someone has the legal role to ensure, together with OMF, that European regulations are followed.

[2] https://www.salingerprivacy.com.au/2015/04/19/bradley-coopers-taxi-ride-a-lesson-in-privacy-risk/

5.12 Development systems

The development systems used are the responsibility of the end user. These systems are not managed. Updates or patches on the system of the developer are executed when it suits him or her. The development machine can be a Mac or Windows system.

6 Advise

The first impression of Vianova is that the software development is at a mature level. The organization and processes are in order. Using companies like Snowflake is a good choice. Being compliant is Snowflake's core business. Companies that are suppliers of Vianova have arranged security well and therefore already meet many of the CS requirements.

The only thing we noticed is the risk of unintentionally sharing information. A clean desk and clear screen policy can help. The employees work in many different countries and environments, protecting that information is important.

The use of VPN is not required by Vianova, but in some cases public networks are used. And this can be a vulnerability if a public network is used.

It is possible to bring your own device, laptop or mobile phone. With Mobile Device Management (MDM), the management and security of all mobile devices can all be controlled from one central point. Vianova could consider Mobile Device Management to make those endpoints even more secure.

6.1 Review the threads on yearly base

If not already in place at Vianova the seven steps proposed in the picture makes it possible to manage the top risks in a pragmatic way by means of updates of measures.

Figure 10: Process steps CS

7 Appendix A Definitions

Some relevant abbreviations are explained in this table:

Table 2: abbreviation

abbreviation	Explanation
API	Application programming interface
CS	Cybersecurity
FFIEC	Federal Financial Institutions Examination Council
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISMS	Information Security Management System
OWASP	Open Web Application Security Project
PCI-DSS	Payment Card Industry Data security standard
Penetration test	A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security.
SOC 1	Systems and Organization Controls 1 is an evaluation of the effectiveness of a service organization's internal controls.
SOC 2	Systems and Organization Controls 2, in addition to soc 1 the report addresses potential risks that internal controls intend to mitigate.

Table 3: Definitions

Definition	Explanation
Risk analysis	Risk analysis is the process of assessing the likelihood of an adverse event occurring.

8 Appendix B The CS QuickScan Dashboards

In this appendix the dashboards are explained in more detail. The most important findings are explained per product and theme in the appendix. For each question, a "Yes" or "No" indicates whether a requirement has been met or an "NA" if the question does not apply. Each question is followed by a short explanation.

Each theme and each question have been given a certain importance or weight. This weight is a relative percentage and is related to the potential effort required to meet the theme or requirement. A question with a higher percentage is therefore more important or heavier, because the effort required to meet this demand is also higher compared to the other questions within a theme. This also applies to themes that coincide within one product. A theme with a higher weight has more influence on the total because it is more difficult to match this theme.

Next to the dashboard, the improvement opportunities are described to grow to maturity level 3. These improvement opportunities are described in relation to the CS maturity level 3 (see The CS maturity score).

To provide a clear picture, in the following paragraphs per product and the underlying themes, a dashboard is shown of the achieved CS maturity level compared to the structured maturity level 3. The green bars indicate the current level of a product and theme. In this report, it is important to what extent Vianova is cs mature.

8.1 Context

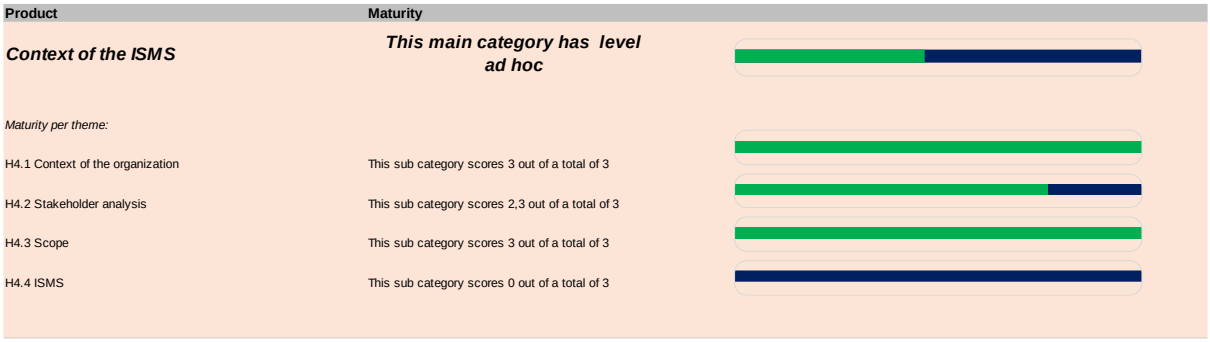


Figure 11 Context ISMS

H4.4 Because an ISMS has not yet been implemented; this question has been answered with no. The score is between 1 en 2. However, Vianova planned to get the (ISO) certificate end of this year or start next year.

8.2 Policy

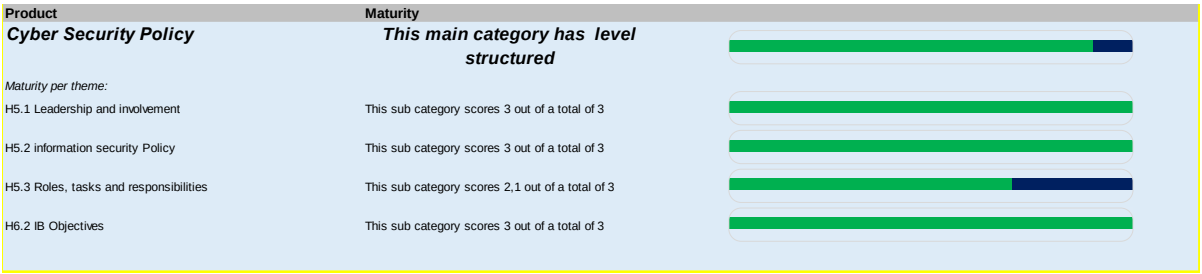


Figure 12 Dashboard Policy

Policies scored between 2 en 3, thus are in place and mature.

8.3 Support

Product	Maturity
Support	***This main category has level structured***
Maturity per theme:	
H7.1 Resources	This sub category scores 2,1 out of a total of 3
H7.2 Competences	This sub category scores 2,7 out of a total of 3
H7.3 Awareness	This sub category scores 3 out of a total of 3
H7.4 Communication	This sub category scores 1,8 out of a total of 3

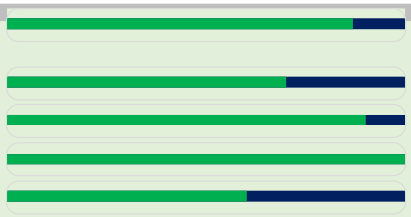


Figure 13 Dashboard Support

Overall support is in place, so it is mature.

8.4 Risk management

Product	Maturity
Risk management	***This main category has level structured***
Maturity per theme:	
H6.1.2 Risk assessment procedure information security	This sub category scores 3 out of a total of 3
H6.1.1 Determine risks and opportunities	This sub category scores 3 out of a total of 3
H6.1.3a Risk Registry	This sub category scores 3 out of a total of 3
H8.2 Regular and planned risk analyzes	This sub category scores 3 out of a total of 3
H6.1.3b control measures	This sub category scores 3 out of a total of 3
H6.1.3e / f Action plan / treatment plan	This sub category scores 3 out of a total of 3
H8.3 Mitigate information security risks	This sub category scores 0 out of a total of 3
H6.1.3C Compare	This sub category scores 3 out of a total of 3
H6.1.3D Statement or Applicability	This sub category scores 0 out of a total of 3

Figure 14 Dashboard Risk Management

Two subjects about risk management H8.3 and H6.1.3D are answered with no.

Subject "H8.3" with te following question: Are actions plotted according to the risk treatment plan for information security risks? Those questions are answered no.

Subject "H6.1.3D" with the following question: "The Declaration of Applicability" The Declaration of Applicability is a document in which an organization describes which cs control measures have been implemented. Does the mentioned document exist? Those questions are answered no.

8.5 Check and Evaluate

Product	Maturity
Check and evaluate	***This main category has level ad hoc***
Maturity per theme:	
H9.1 Performance measurements	This sub category scores 0,6 out of a total of 3
H9.2 Internal audit	This sub category scores 3 out of a total of 3
H9.3 Executive assessment	This sub category scores 3 out of a total of 3

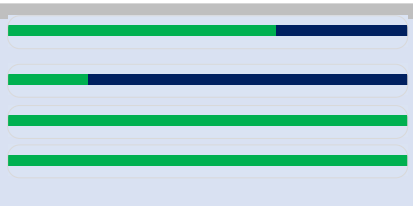


Figure 15 Dashboard Check and Evaluate

Four questions out of 5 are documenting measuring performance test. Those questions were answered with no.

8.6 Continuous Improvement

Product	Maturity
Improve continuously	***This main category has level ad hoc***
Maturity per theme:	
H10.1 Deviations and corrective measures	This sub category scores 3 out of a total of 3
H10.2 Continuous improvement in ISMS	This sub category scores 0,8 out of a total of 3

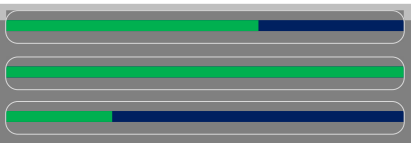


Figure 16 Dashboard Continuous Improvement

Vianova is preparing an ISMS. So, this score is between 1 and 2 at the moment. In the software development is a PDCA circle implemented.

8.7 CS Measurements CS

The [(ISO) standard has an Annex A in which management objectives and management measures for information security are described. This Appendix provides guidelines for the organization to identify cyber risks. The control measures in this Annex A have been individually assessed for maturity. This means that it is only clear which controls the organization has implemented, with the maturity score indicating to what extent the controls have been implemented. The short explanation for each control measure on the maturity score can be found in the “QuickScan questionnaire”.

Product	Maturity
Information security measures	***This main category has level structured***
Maturity per theme:	
A5 – Information- security policy	This sub category scores 3 out of a total of 3
A6 – Organisation of the information security	This sub category scores 2,1 out of a total of 3
A7 – Reliable personnel	This sub category scores 3 out of a total of 3
A8 – Asset management	This sub category scores 2,1 out of a total of 3
A9 – Access - security	This sub category scores 3 out of a total of 3
A10 – Cryptography	This sub category scores 3 out of a total of 3
A11 – Physical Security	This sub category scores 2,1 out of a total of 3
A12 – Business security policies	This sub category scores 3 out of a total of 3
A13 – Communication security	This sub category scores 3 out of a total of 3
A14 – Information systems acquisition, development and maintenance	This sub category scores 3 out of a total of 3
A15 – Suppliers	This sub category scores 3 out of a total of 3
A16 – Security Incident Management Information	This sub category scores 3 out of a total of 3
A17 – information security-aspects business continuity	This sub category scores 3 out of a total of 3
A18 – Compliance with legal and contractual requirements	This sub category scores 3 out of a total of 3

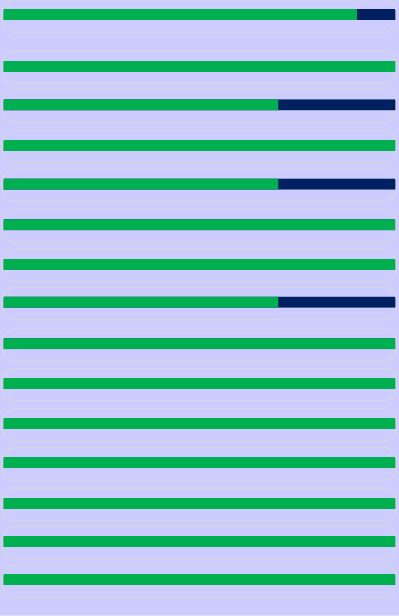


Figure 17 Dashboard CS Measurements

The asset management and physical security are not a big issue for Vianova. Maturity is between 2 and 3.