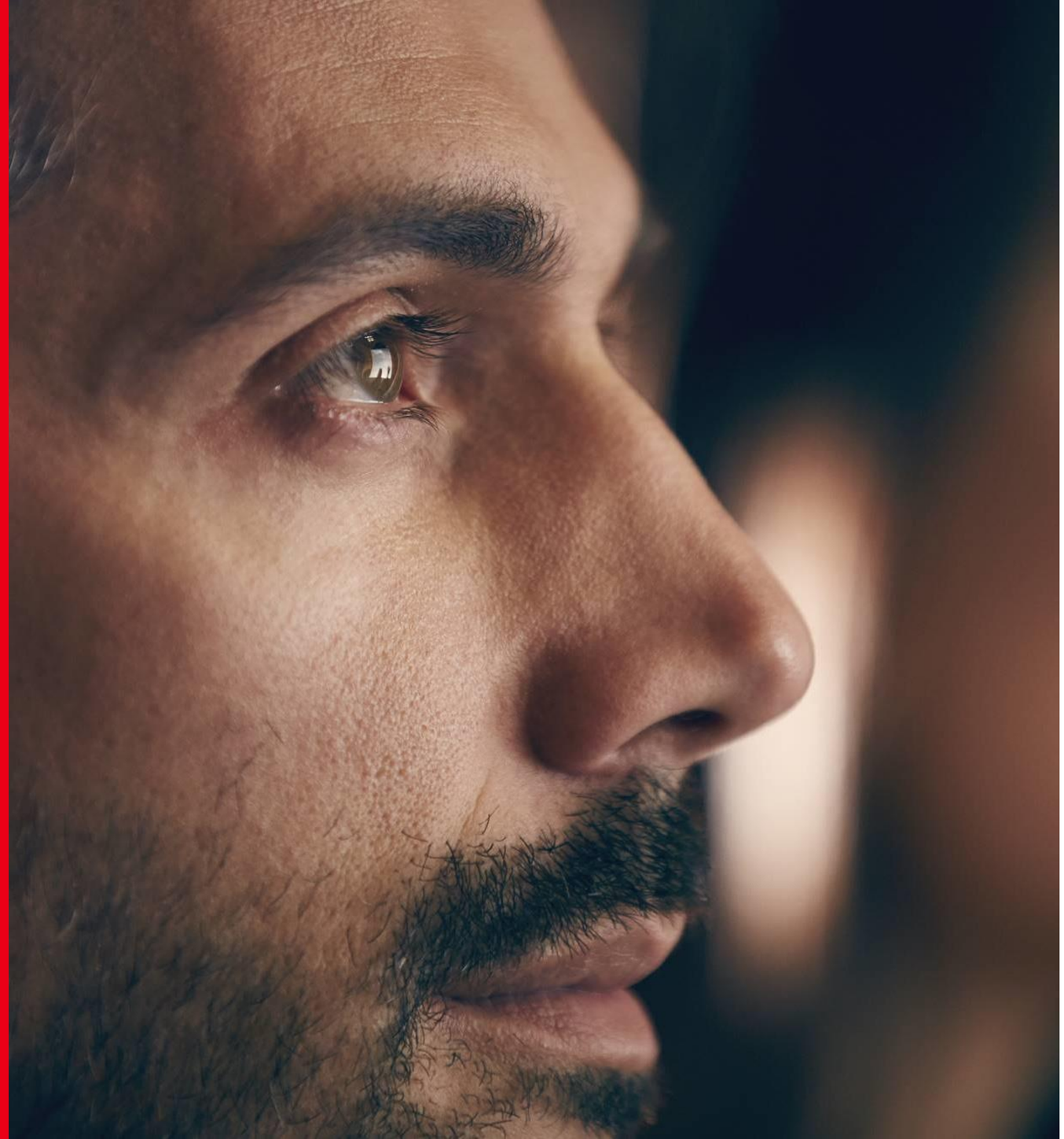
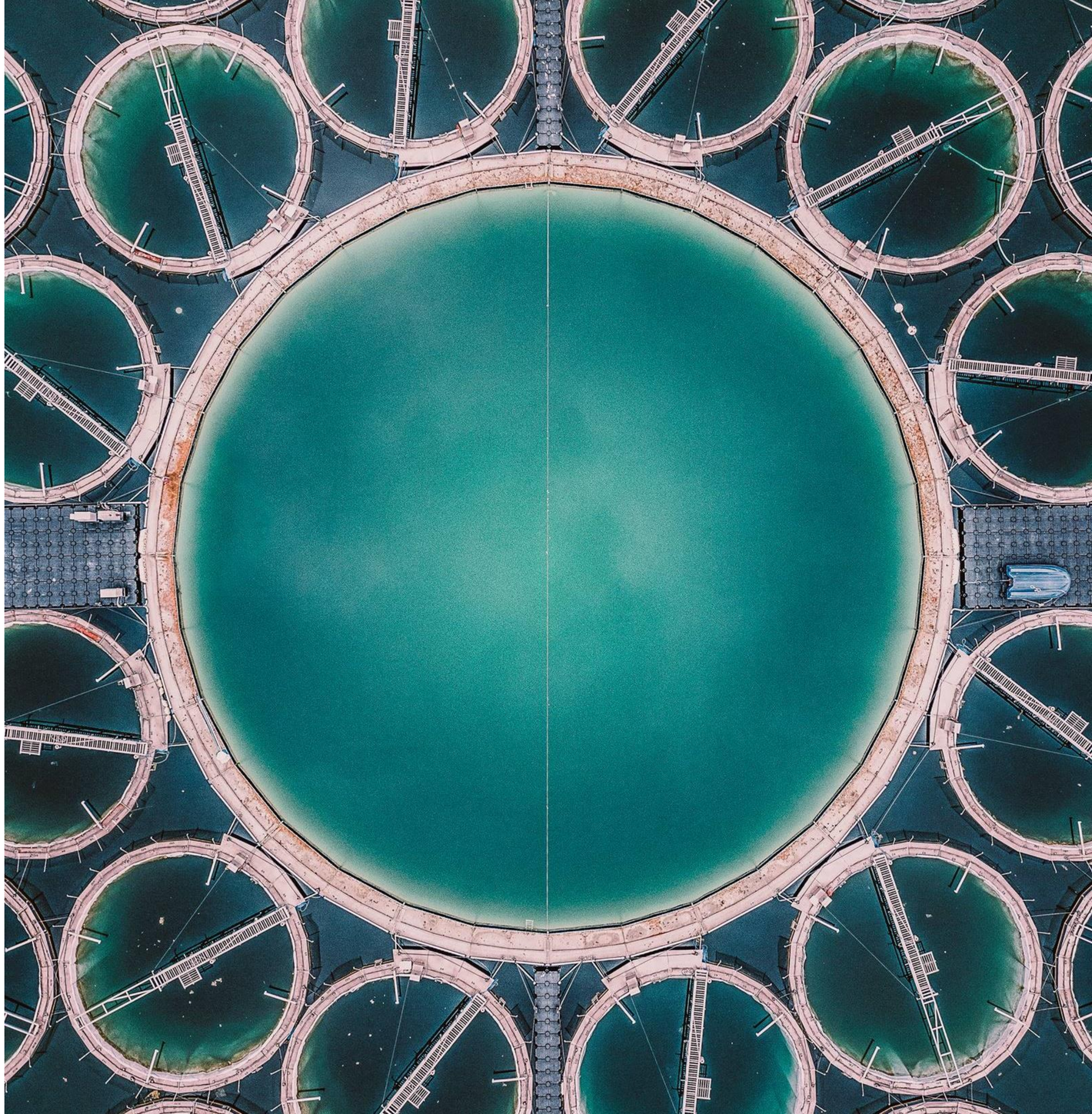


Vendor Assessment by Aon Global Risk Consulting

Assessment: Sinqia (Scafplusnet)
For: Unileverprev

Table of Contents



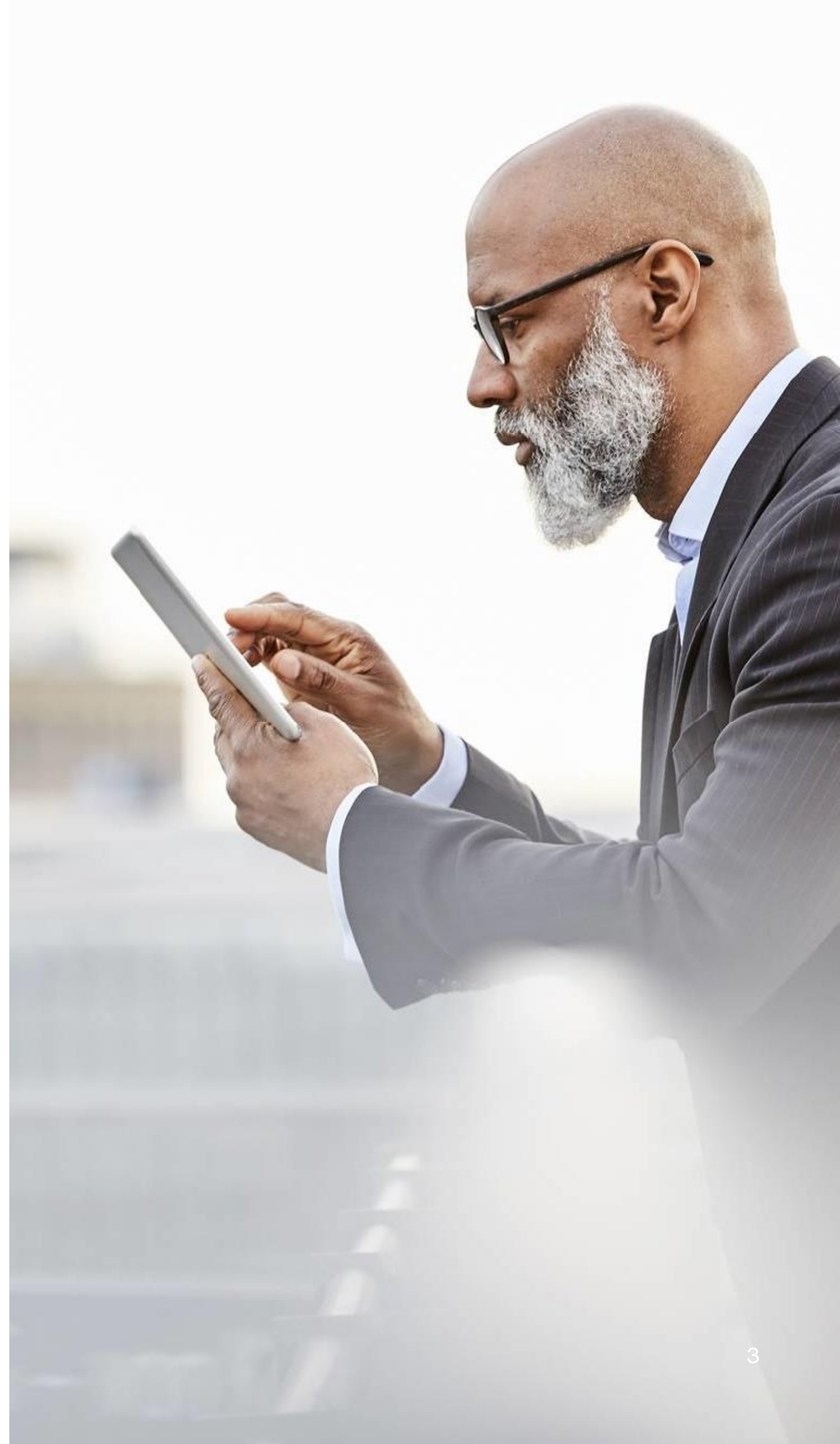
Introduction

According to Aon's most recent global risk survey, GRMS 2023, managers around the world point to cyber risk and supply chain failure as some of the main concerns for company management. These risks occupy the first and sixth position respectively, and for more than ten years they have been among the top ten risks that concern companies.

Cyber risk can be defined as exposure generated from a strong interaction with technology and data. While the risk of failure in the supply chain can be defined by the high dependence on external products and services to carry out the company's own deliveries.

When we analyze both threats more deeply, we understand that they are intrinsically linked, that is, it is possible for there to be a failure in the supply chain due to cyber risks to which our suppliers are exposed, in the same way that it is possible to suffer a cyber attack due to from a gateway found by criminals via suppliers.

Therefore, it is essential that companies are prepared to evaluate their suppliers, establishing security and privacy SLAs so that a baseline is created for risk management in these two areas. Once the company understands its own level of maturity, understands the depth to which it is exposed to its suppliers, understands the impact caused by security and privacy issues, it will be better prepared to deal with the adversities of events occurring that involve these two spheres. of risk.



Introduction

In this report, Aon will present the results of its supplier maturity analysis based on CyQu. CyQu, or Cyber Quotient Evaluation, is a proprietary tool, developed by Aon for evaluating Cyber Risks based on NIST (security framework).

By analyzing 97 questions, 35 control areas, and 9 security domains, Aon determines a NIST-based cyber hygiene profile. Grades are established from 1 to 4, with 1 being the lowest level of cyber maturity and hygiene, considered basic; and 4 the highest level, defining the profile as advanced.

Companies with lower levels of governance and cyber hygiene, whether generally or individually in the areas of control, are considered reactive companies, with a basic profile, more susceptible to more catastrophic developments in cyber attacks and data leaks. Companies at higher levels are considered proactive, subject to better damage and loss containment, and a higher success rate in executing their recovery and response plans.

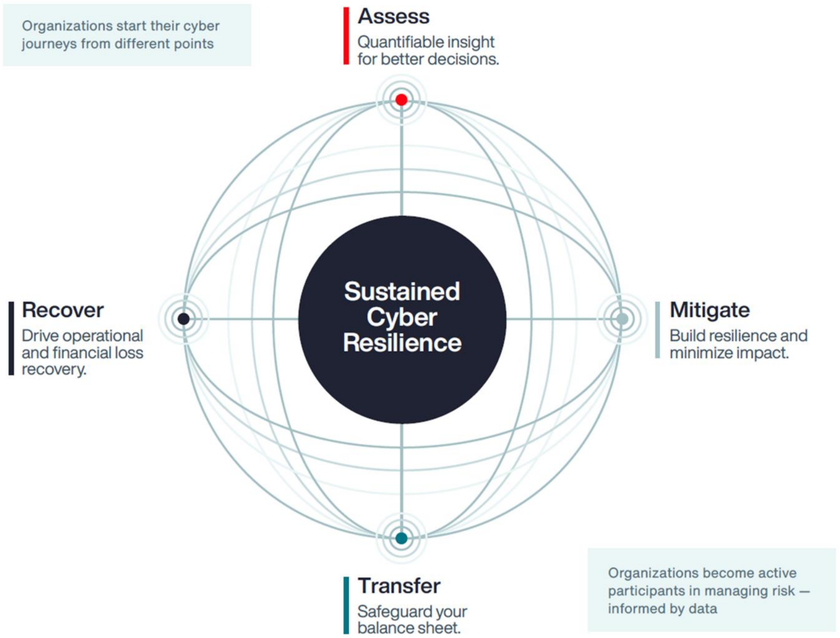
Thus, through this assessment, it is possible to determine work and correction focuses, as well as investment focuses for the company based on what has the greatest impact on operations.

Cyber Loop

Methodology

- The **Aon Cyber Loop** is **Aon**'s strategy for addressing cyber risks. It is a cyclical and holistic strategy, possible to adhere to at any time. We believe that cyber risk management is a constant and continuous action, and that only close monitoring and regularity can put us ahead of the threats that arise every day.

- The first step is to carry out a diagnosis of cyber risk management, by applying the **Cyber Quotient Evaluation (CyQu)** analytical tool, through which the organization across 9 domains has a clear understanding of its preventive and protective practices.



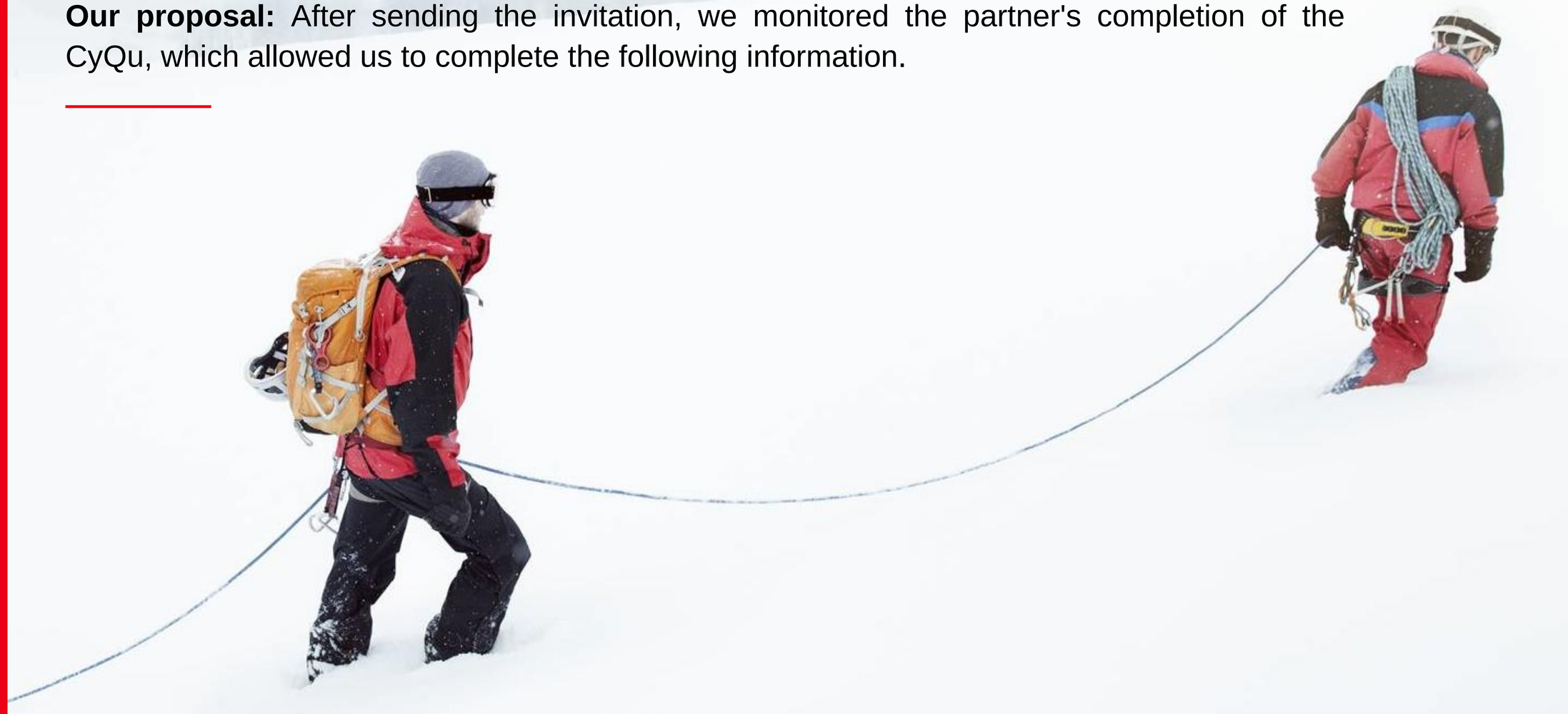
What is next?

- Benchmark: CyQu offers a complete benchmark, including general comparative notes, by security domain, by control area.
- Assessment: have instant visibility of maturity levels by control area, establish focuses and responsibilities.
- Roadmap: based on CyQu's assessment, determine the course of the company's next actions.

Executive Summary

Objective: The scope consists of carrying out a risk profile assessment of critical partners listed by UnileverPrev. Together, we established the work model, as well as the invitation that was sent to the selected partner.

Our proposal: After sending the invitation, we monitored the partner's completion of the CyQu, which allowed us to complete the following information.



Sinqia

At a glance

Summary

Find below the CyQu result for Sinqia, project Scafplusnet. Sinqia Scafplusnet´s General Score was 3.4. After review of version one, there was significant improvement considering that this report only refers to a fraction of the operation dedicated to support Unilever and with specific controls to its personalized environment.

CyQu Domains

- Data Security
- Access Controls
- Endpoints and System Security
- Network Security
- Physical Security
- Application Security
- Third Party Managment
- Resilience
- Remote Work

ATENÇÃO!

Assessments of cyber risk, by its complex nature, can be very subjective. Gaps and uncertainties will exist due to the variability in completeness, accuracy and currency of data and analysis referenced in this review. The above Cyber Quotient Evaluation Score is a score that is produced exclusively from the answers submitted to questions. It represents an assumption and opinion based upon facts and circumstances as reported at the time of the submission. Answers on the cyber security posture and arrangements have not been externally validated and/or tested. Subsequently, all information is to be reviewed and validated by the company. The accuracy of the results will remain dependent on the accuracy of information provided by the company, and assumptions made can vary significantly.
No representations or warranties are made in providing the Cyber Quotient Evaluation Score and it is supplied for informational purposes only and may not be relied upon or in any way used in making decisions about cyber security or to determine the vulnerability of your organization to a cyberattack or other similar threat.
Should the organization wish to use the CyQu results to facilitate a conversation with an insurance broker, a separate report is available on request where all scores are removed and responses to the CyQu questions remain. Any responses should be validated and adjusted via meeting with your insurance broker.

Full Report

1. About UnileverPrev

About the company

UnileverPrev is an innovative company in the private pension sector, committed to providing solid and personalized financial solutions to its customers. It has stood out in the market for its client-centric approach, transparency and excellence in investment management.

Its purpose is to take care of its participants and their beneficiaries, managing their social security benefits to guarantee in the future, during retirement, the same quality of life they have today.

With a team of highly specialized and experienced specialists, UnileverPrev stands out for the quality of its services and its commitment to providing security and peace of mind for its customers' financial future.

At UnileverPrev, pension planning is essential to ensure a smooth and stable transfer. Therefore, we work tirelessly to offer the best investment options, combined with personalized and efficient service.

Full Report

1. Company´s accolades

1981

A UnileverPrev ou antiga Previgel, foi constituída para administrar o Plano de Benefício Definido oferecido aos empregados da Unilever.

2003

Criação do Plano de Previdência Complementar UnileverPrev - PPCU (na modalidade de Contribuição Definida) com opção de migração voluntária pelos participantes do Plano de Benefício Definido e fechamento deste para futuras adesões.

2017

Alteração regulamentar que eliminou os benefícios de risco do plano PPCU, fazendo dele um plano 100% Contribuição Definida.

2022

Estamos entre as 25 maiores entidades fechadas de previdência complementar não públicas do Brasil, e nosso plano PPCU está entre os 15 maiores planos de Contribuição Definida do país segundo o relatório Consolidado Estatístico ABRAPP de 09/2021.

Detailed report

3 – Vendor appointed by UnileverPrev

sinqia

A specialist in the financial system, Sinqia is one of the fastest growing companies in Brazil. Elected several times as one of the 100 largest Fintechs in the world, its software is present in 8 out of 10 financial institutions in the country. It started its small operation in the 1990s in a coffee shop on the streets of São Paulo and, after a dizzying increase in its production capacity, it consolidated itself as a leader in software and innovation for the Brazilian financial system and one of the largest suppliers. of technology and services for this industry.

The objective was to migrate from a business model based exclusively on services to a more complete model that also encompassed product development, whose first business software was launched in 2000. Two years later, the company was considered as a BNDES Prosoft resource, accelerating the change and modernizing your business.

The year 2004 marks the launch of SBS (Senior Banking Solution), which became the company's main product as it was one of the first Brazilian applications for the treasury of financial institutions. In 2005, more investments were received with the sale of shares in BNDESPAR and FMIEE Stratus GC.

AON

Detailed report

3 – Vendor appointed by UnileverPrev

sinqia

The scope of SBS was then expanded, developing modules for exchange, derivatives and fixed income, and the growth strategy via acquisitions began with the incorporation of NetAge (SIAN software for treasury and investments) in 2005. Since then A very successful consolidation strategy began, which resulted in sector leadership.

Sinqia has been present in the select group of publicly traded companies on B3 since 2013, known as SQIA3 by investors.

Today, with more than 26 years of experience, the company offers software platforms aimed at banks, funds, pensions and consortiums, in addition to outsourcing and consulting services.

In 2021, with the recent acquisitions, a business unit was created focused on digital solutions that complement all software and services segments. This structure focuses on each segment, enhancing solutions that boost the financial system.

AON

Detailed Report

4. Diagnostic – 4.1. Cyber Quotient Evaluation (CyQu)

CyQu is a tool developed by **Aon** to help organizations understand their level of maturity regarding cyber risks. The tool was built based on the NIST framework and ISO 27001. By analyzing 9 security domains and their respective 35 critical control areas, the organization will be able to better understand its strengths and those for improvement in its security management.

The report is also capable of offering the organization comparisons of its scores with other companies in the market that are similar in terms of revenue and industry. This helps to establish short and long-term objectives, and prioritize investments according to the specific needs of the company. industry and, obviously, the company.

Detailed Report

4.2. CyQu Results Key Findings

Key Findings

- Sinqia presents a robust and secure environment to manage cyber risk in terms of the contract it has with UnileverPrev
- We highlight the scores in the domains of system and endpoint security, as well as network security, which are extremely important for this relationship and have high scores, establishing a high degree of maturity on the part of Sinqia.
- We recommend monitoring the implementation of the SSO project.

1	Initial

CONTROL AREAS

- Remote Business Continuity

2	Basic

CONTROL AREAS

- Multi-Factor Authentication
- Software Management
- Remote Security Awareness

3	Managed

CONTROL AREAS

- Data Classification
- Governance
- Risk Management
- Access Management
- Password Configuration
- Wireless
- Network Penetration Testing
- Due Diligence
- Third-Party Inventory
- Incident Response
- Backup
- Device Vulnerability & Monitoring

4	Advanced

CONTROL AREAS

- User Awareness and Training
- Data Protection
- Endpoint Protection
- Vulnerability Management
- Asset Inventory
- Secure Configuration
- Logging & Monitoring
- Network Environment
- Network Capacity
- Physical Access
- Physical Penetration Testing
- Tampering & Alteration
- Environmental
- Training
- Secure Development
- Third-Party Contracts
- Business Continuity/DR
- Remote Connectivity
- Authentication & Identity

Detailed Report

4.3. Consolidated results from CyQu

CyQu Components

Security Domains -> Control Areas -> Questions

1 Initial	2 Basic	3 Managed	4 Advanced
Organizational cyber security risk management practices are not performed If the organization identifies and addresses risks it is done within silos only; components and activities of the risk management process are limited in scope and implemented in an ad-hoc manner	Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner Risk management practices and technologies are not established organization-wide	Risk management practices and technologies are performed and established throughout the majority of the organization Adapts its cyber security practices based on best practices and predictive indicators throughout the majority of the business Policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk	Adopts an organization-wide approach to manage cyber security risk Organizational cyber security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape Process of continuous improvement incorporating advanced cyber security technologies and practices
1 – 1,8	1,9 – 2,6	2,7 – 3,2	3,3 – 4

Overview

According to the data contained in our systems, and according to the results obtained by Sinqia in CyQu, the company is classified, on 12/02/2024, as an Advanced risk company. A company that has an advanced risk profile can be understood as a forward-looking company in security and privacy, proactive, which has adequately documented, tested processes and procedures. It is also a company that considers participation (and possible failure of critical suppliers) in its tests.

Considerations

Safe environments can be costly and require continuous monitoring and investment. We strongly recommend creating a periodic risk assessment routine, including comparative assessments over time. We recommend periodic review of Liability clauses and that the contractor requires Cyber, E&O and Crime insurance, as additional guarantees to the contract.

Detailed Report

Classification by control area

Control Areas	Your CyQu	Peer
Data Security *Manages safeguards to protect the confidentiality, integrity, and availability of information.*	3.4	2.9
Data Classification *Manages classification of data to determine appropriate technical safeguards.*	3.0	2.6
User Awareness and Training *Delivers education for employees on security best practices and common threats that could compromise the confidentiality, availability, integrity of information.*	4.0	3.3
Data Protection *Manages the protection of sensitive data using data encryption and loss-monitoring tools.*	3.5	2.9
Governance *Board / Executive Management ownership and commitment to cyber security as a critical factor for achieving business objectives and protecting value*	3.1	2.9
Risk Management *Integration of cyber security into the risk management framework to achieve alignment on risk metrics and improve decision making processes*	3.3	2.7
Access Control *Grants authorized users the right to use a service while preventing access to non-authorized users.*	3.1	2.9
Access Management *Prevents compromise of confidential data by ensuring least privileged access rights.*	3.2	2.8
Password Configuration *Prevents compromise of confidential data by ensuring password configuration settings.*	3.4	3.3
Multi-Factor Authentication *Prevents compromise of confidential data by providing an extra layer of security where the first layer mechanism may be at risk or compromised.*	2.5	2.9
Endpoint and Systems Security *Delivery and administration of infrastructure services, systems monitoring, endpoint protection, configuration management, storage management, infrastructure operations.*	3.9	2.9
Endpoint Protection *Manages endpoint security software to limit viruses, trojans and other malware that could result in unauthorized access to sensitive information, data exfiltration and/or noncompliance.*	4.0	3.0
Vulnerability Management *Manages process to identify, rate, prioritize, report on information system vulnerabilities and recommend an appropriate treatment response.*	3.8	2.8
Asset Inventory *Maintains information and relationships for a collection of assets in order to provide visibility into an organization's environment and drive key decisions based on risk.*	4.0	2.6
Secure Configuration *Manages a process to identify, rate and track gaps in critical information system compliance against a pre-defined standard.*	4.0	2.8
Logging & Monitoring *Delivers centralized security logging, monitoring, and analytics capabilities to support incident response efforts and regulatory/compliance mandates.*	3.9	3.0
Network Security *Delivers infrastructure services including enterprise defense for network, compute, physical presence, cloud, storage management and operations.*	3.7	3.0

Detailed Report

Classification by control area

Network Environment *Provides network based detective and preventive control capabilities to stop unwanted traffic and offer visibility for investigation and remediation.*	4.0	3.0
Wireless *Manages a process to identify, rate and track gaps in critical wireless devices against a pre-defined standard.*	2.8	2.7
Network Penetration Testing *Manages process to identify, rate, prioritize, report on network vulnerabilities and recommend an appropriate treatment response.*	3.0	3.2
Network Capacity *Manages system capacity and resourcing to limit denial of service and other availability issues.*	4.0	2.9
Physical Security *Protects facilities, equipment, resources, and personnel from unauthorized access, damage or harm.*	4.0	2.9
Physical Access *Manages appropriate access to key physical locations.*	4.0	3.3
Physical Penetration Testing *Manages process to identify, rate, prioritize, report on physical vulnerabilities and recommend an appropriate treatment response.*	4.0	1.9
Tampering & Alteration *Manages appropriate access to key physical infrastructure equipment or systems.*	4.0	2.1
Environmental *Plans for securing key physical infrastructure against environmental threats.*	4.0	3.3
Application Security *Protects applications from threats by requiring measures or checks during each stage of the application development life cycle.*	3.1	2.5
Training *Provides software security training to development community including a structured approach to identify, quantify, and address the security risks associated with an application.*	4.0	2.7
Secure Development *Delivers dynamic analysis and penetration testing for applications including correlation of application vulnerabilities, assessment of the level of risk, and recommendations on appropriate remediation and mitigation.*	3.5	2.8
Software Management *Manages process for authorizing and allow listing applications.*	2.0	2.0
Third Party *Monitors relationships with third parties to ensure provided services adhere to defined security policies.*	3.3	2.4
Third-Party Contracts *Manages third-party risk through formal legal agreements.*	3.5	2.5
Due Diligence *Prevents and detects third-party risk through standard security assessments.*	3.2	2.3
Third-Party Inventory *Manages list of key vendors with access to system or data.*	3.0	3.0
Business Resilience *Plans for prompt and effective continuation of business critical services in the event of a disruption.*	3.2	2.6
Business Continuity/DR *Plans for prompt and effective continuation of business critical services in the event of a disruption.*	3.5	2.6
Incident Response *Allows for recovery of critical applications and business process in the event of a failure.*	3.0	2.7
Backup *Allows for recovery from an unplanned security or operational event.*	3.0	2.7

Detailed Report

Classification by control area

Remote Work *Enabling users to remotely access corporate systems and data securely to deliver on their roles and responsibilities when outside of corporate working environments.*	3.0	2.9
Remote Connectivity *Providing the ability to connect from non-corporate locations to business information systems, applications and data.*	3.5	3.4
Authentication & Identity *Enabling the business to identify and control access where appropriate and allowing users to connect to the required and relevant systems, data and domains to perform their specific duties.*	3.5	3.0
Device Vulnerability & Monitoring *Securing remote devices from the latest known vulnerabilities with regular updates and security monitoring.*	3.0	2.6
Remote Business Continuity *Providing organizations the ability to backup information from remote clients and maintain business continuity in the event of large scale remote working.*	1.9	2.3
Remote Security Awareness *Educating business and technology users on relevant cyber security attacks, threats and risks based on their remote working environments, and how to safeguard themselves appropriately.*	2.0	2.3

Detailed Report

4.4. Recomendations

In general, Sinqia's Scafplusnet project meets the best corporate governance, information security and privacy practices based on the NIST model. With a score of 3.4, the company is at an advanced level of cyber hygiene.

From our perspective, this is a transferable and insurable risk. Not presenting notes that could restrict the insurer's appetite. Therefore, we recommend that UnileverPrev consider requesting professional civil liability, fraud and cyber civil liability insurance, in order to ensure better collateralization.

The CyQu tool does not point out redflags or any specific concerns. The company is currently part of the Scafplusnet project, in compliance. Aon recommends that this report be redone twice a year to monitor results and controls.

We remind you that all evaluations and analyzes were carried out based on the answers given by Sinqia, there was no presentation of evidence, collection of answers via interview/meeting, nor any type of remote verification of vulnerabilities.

We still recommend risk analysis using tools such as Security Score Card and Bitsight, however we believe that these tools are unable to perform a granular analysis, in order to segregate the Scafplusnet project from other environments.

Attention!

Despite no mention of the tool used to assess risk, our consultants believe there are points to be discussed

1 **Supply Chain Management**

We recommend that UnileverPrev asks Sinqia for a complete and detailed presentation on its supplier management policies. Sinqia's dependence on suppliers could result in a considerable impact on UnileverPrev.

2 **Privacy and Cybersecurity**

Access management is a critical point for this relationship considering the nature of the operations. Monitoring projects such as the implementation of SSO and other automation measures for granting and revoking access are essential.

3 **API and Software management**

We suggest that the controls and protective measures applied to the execution and use of unauthorized software be clarified.

Detailed Report

4.5 – Análise de Risco e Potenciais Impactos

Given the scope of service provision, risk analysis is crucial to identify vulnerabilities that could impact the operation. Below, we highlight criteria that are directly linked to the operation and its potential impacts.

Potential Risks and their impacts:

- **Interruption of Services – Sinqia (Scafplusnet)**

The security failure of existing controls can result in significant interruptions in the services provided, directly impacting UnileverPrev's end customer. In addition to having its own insurance and risk management program, we recommend that UnileverPrev consider:

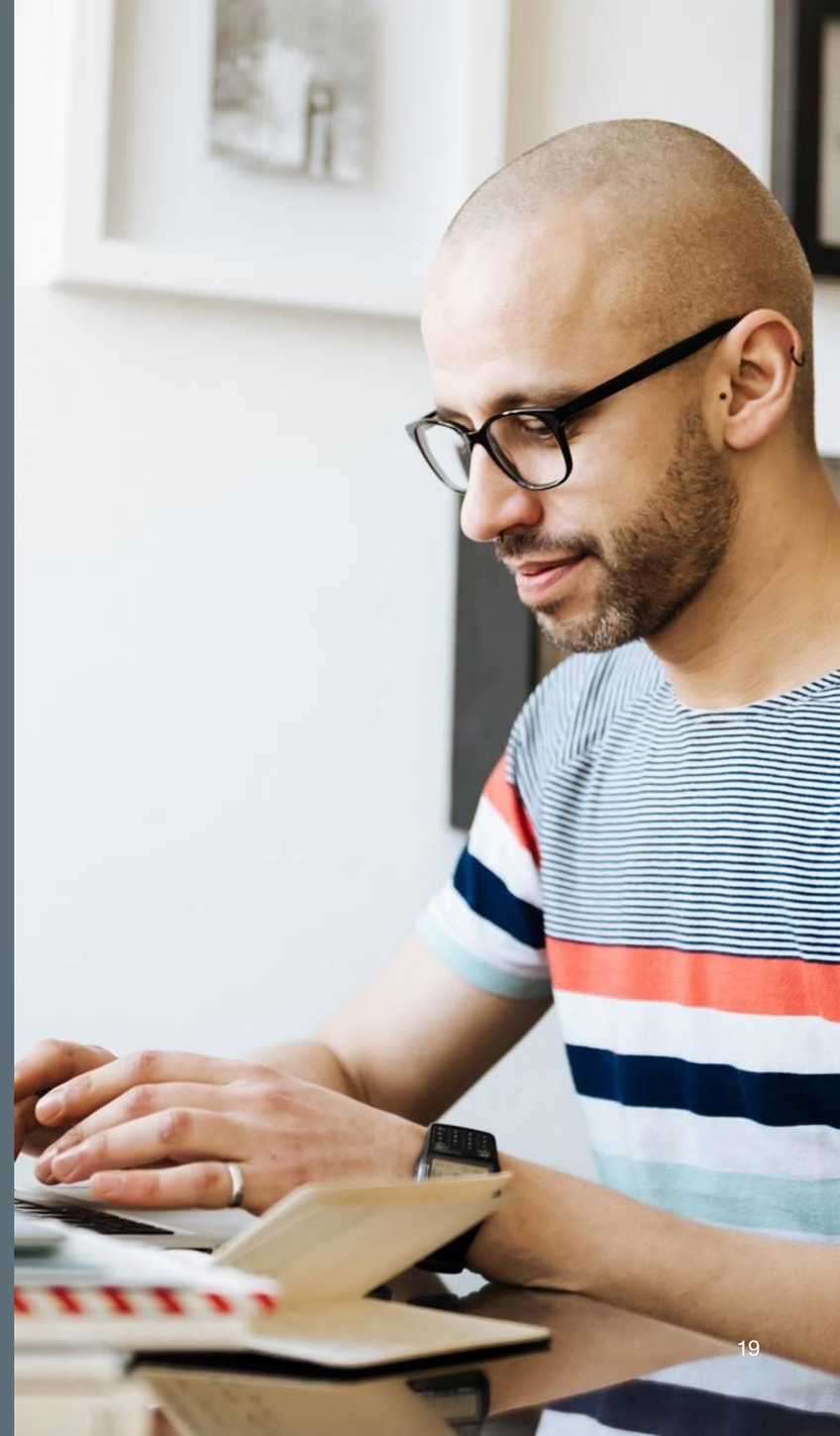
a) Consider learning about Sinqia's incident response and disaster recovery plan, define your role and assess impacts. In this sense, also consider participating in exercises to execute these plans and simulations. Also, understand the redundancies involved and recovery times for consideration in your own incident response plan.

- **Data Loss**

UnileverPrev customer data may be exposed, even though storage, collection and processing do not necessarily occur in the hands of UnileverPrev, before regulators responsibility may be determined differently. Therefore, be prepared for possible discussions at an administrative level regarding Unilever's responsibilities regarding hiring and dependence on its third parties.

- **Reputation and Trust**

Customers may feel inclined to seek alternatives if they do not feel that their information and assets are adequately treated and cared for.



Detailed Report

4.5 – Risk Analysis and Potential Impacts

Supply Chain Managment

A good relationship with suppliers is essential, and understanding how this chain develops further is essential. We recommend:.

- Request additional explanations about controls and protection for physical access to Sinqia's critical infrastructure suppliers, related to the Scafplusnet project.
- We recommend requiring Errors and Omissions, Cyber and Fraud Insurance from suppliers.
- We recommend encouraging and participating in crisis testing and exercises.

Privacy and Security Projects

Security and privacy management is a constant task and requires a continuous investment of time and financial resources. We recommend:

- Monitor the development of security project implementation projects and additional tools.
- Monitor the implementation of alternative security strategies for domains and control areas that move towards a higher level of maturity.

Software and APIs Management

Software development is a task of great responsibility and exposure. We recommend:

- Request presentation about the development process. Inquiring about issues related to the development and controlled use of tools, such as artificial intelligence, code pools, previously unauthorized software, etc.

Access Management

Access management can be a major vulnerability for the company in terms of the ability of criminals and malicious agents to subvert values and access for their own benefit, creating unknown exposures that are difficult to trace. We recommend:

- Demand clarity in the process of evaluating, granting and revoking access. Question the implementation of automaticity in these processes, or on the other hand demand a detailed explanation of the process with exemplification and presentation of evidence.

Conclusion

We identified that the company Sinqia, for the Scafplusnet project, is classified as an ‘‘Advanced’’ company.

We believe that all controls presented comply with the standards necessary to establish a sustainable and safe relationship with UnileverPrev.

We recommend that follow-up routines be created for points left open, as well as more efficient integration routines between the two companies.

Assumptions

During the preparation of our report, we assume and rely on the answers provided by the recipient and responsible for the CyQu questionnaire. We do not validate the accuracy, completeness and reliability of these responses received and/or the actual and current profile of the organization's cybersecurity structure. The information included in the valuation report is based on data and conditions communicated to us, which may be subject to rapid and material changes. Although this change may have an impact on our assumptions and results, we have no obligation to update, revise or restate our review, assumptions or opinions. No one should act on such information without appropriate professional advice after a full examination of the particular situation. The Assessment Report may not be distributed, reproduced or used without the express prior written consent of Aon.

Aon will have no liability to the recipient or any other party arising from the recipient's or such other party's use of this information.