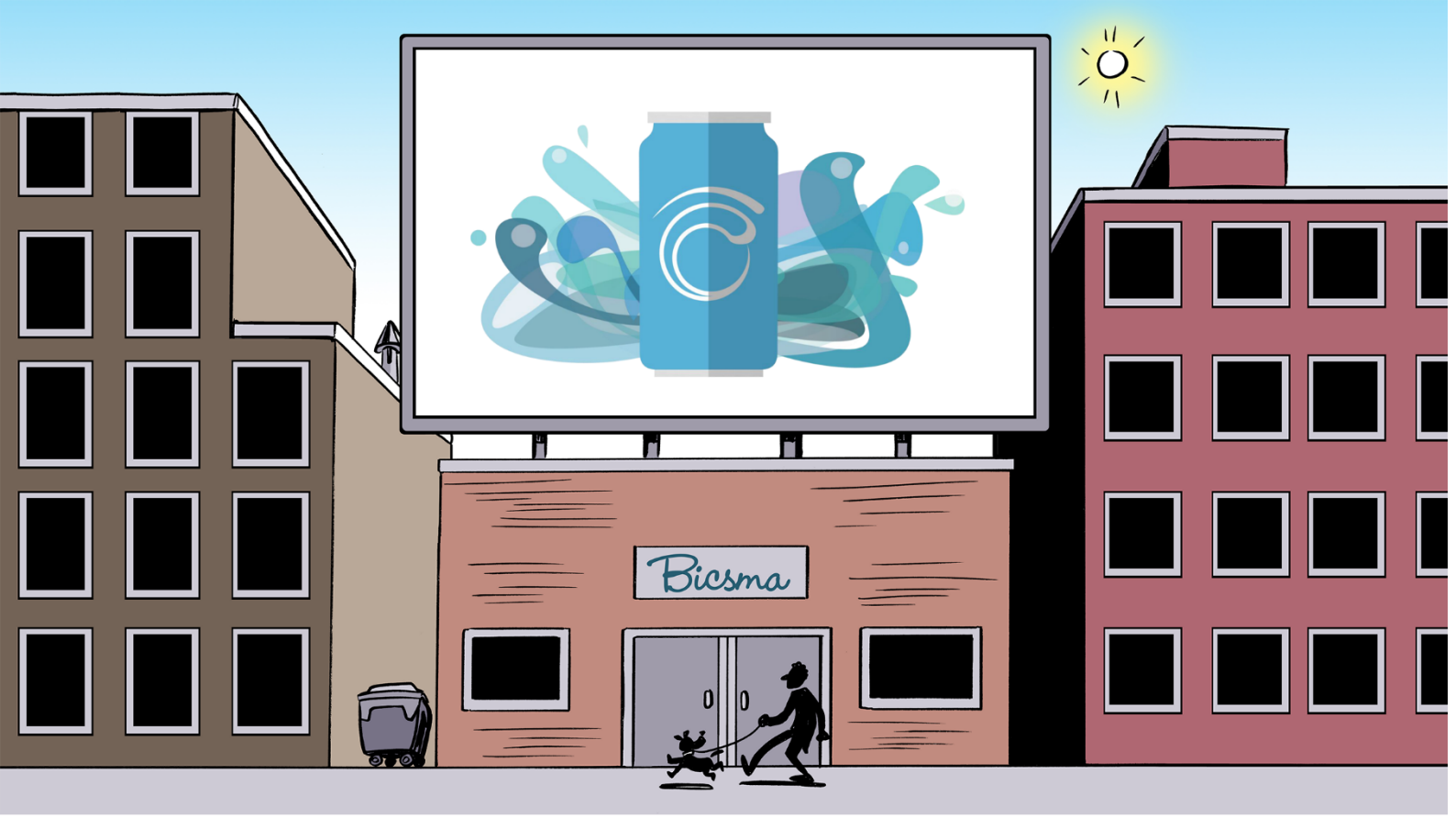

Bicsma

BICSMA'S VISION ON INFORMATION SECURITY

Table of Contents

1. Document features

1.1 Custodian contact details

Name:
Location:
Telephone:
E-mail:
URL:

1.2 Reviews

Date of most recent review:

Date of next review:

Date	Author	Version	Modifications

1.3 Paragraph list

Name	Function	Role	Date	Paragraph

1.4 Distribution list

Name	Function	Role	Version	Medium/ format

2 Introduction

Bicsma BV is taking efforts to protect its business operations against unwanted influences that might result in a negative impact on the business. As far as information management is concerned, this is performed by implementing an information security process. The objective of the information security process is to ensure and demonstrate that all aspects of the management and use of information and the related resources are in line with the applicable reliability requirements and the security measures these requirements are translated to. This Vision on information security is to ensure compliance throughout the organisation in a coherent and targeted manner. This Vision also governs the formulation of Bicsma's strategic information security policy and the selection of Bicsma's information security measures.

Chapter 2 of this Vision sets out the purpose of this document. Chapter 3 outlines the framework in which the document should be used. Chapter 4 describes Bicsma BV's vision on information security. Chapter 5 describes the information security principles that govern Bicsma's information security policy and Bicsma's security measures. Finally, Chapter 6 outlines the most important principles for strategic implementation.

3 Framework

The word 'information security' is a container concept and, as such, has a different meaning to everyone. To prevent differences in interpretation, the definition and scope of information security, as used in this document, are outlined below.

3.1 Definition of information security

In this Vision, information security is defined as *the establishment and maintenance of a coherent package of measures to ensure the reliability (confidentiality, integrity and availability) of the information assets. Information assets include equipment, software, stored data, procedures and people*.

3.2 Scope

In order to achieve concrete results, the scope of information security within this document is (provisionally) limited to the following:

Information security within Bicsma BV refers to preserving the security of the computer network and the related IT processes. Computer network includes interfaces with other networks, e.g. third party networks and the internet.

As regards information stored in paper format, this Vision solely applies to information that should be secured to ensure the security and maintenance of the computer network and the related IT processes.

Interfaces with other networks are included in the scope of this Vision to prevent third-party risks from affecting the computer network. This does not alter the fact that the aforementioned risks should be addressed in their own environments. However, the way of addressing these risks is beyond the scope of this document.

3.3 Target group

Formulating a vision is a one-time action taking place on the strategic level. Following the approval of this Vision, the document will be revised at regular intervals. It should be pointed out that this Vision provides guidance to the line organisation in making tactical-operational-level decisions.

4. Bicsma's vision on information security

From Bicsma BV's corporate mission and vision, the following goals have been derived for information security.

4.1 Information security is primarily aimed at facilitating business operations and ensuring an optimal level of personal safety

Bicsma BV believes that its primary obligation is to ensure the optimal running of the business operations and guarantee an optimal level of personal safety. Therefore, Bicsma conceives information security as a tool primarily aimed at facilitating business operations and ensuring an optimal level of personal safety. Consequently, Bicsma strives to arrange its information security in line with these interests and incorporates information security in the decision-making process.

4.2 Information security forms an integral part of the business processes

Integrating information security into the business processes guarantees that information security is incorporated in the decision-making process. This implies an unambiguous integration of information security-related tasks, mandates and responsibilities in the business processes. The aim thereof is to avoid the isolation and/or marginalisation of information security and to prevent local security measures from hindering business operations and/or negatively impacting personal safety in the organisation as a whole.

4.3 Bicsma BV adopts a risk-averse approach to information security

In view of its social responsibility, together with its responsibility towards all shareholders, Bicsma BV adopts a risk-averse approach towards information security. That is to say that Bicsma BV adopts a risk-based approach to information security and, consequently, takes information security risks into account in the decision-making process. This implies that Bicsma opts for lower risk and gives preference to "proven technology" and "best practices" when selecting security measures.

4.4 Bicsma BV strives to comply with the Code of Practice for Information Security

The reliability and availability of Bicsma BV is secured by demonstrating that Bicsma BV has brought its information security under control. The Code of Practice for Information Security, as described in ISO-IEC-27001 and ISO-IEC-27002, is a set of best practices covering all aspects of information security. Bicsma BV strives to create transparent and demonstrably controlled information security by complying with the aforementioned Code of Practice, and aims to make use of independent compliance assessments. Compliance with the Code of Practice is in line with Bicsma BV's ambition to develop a corporate image built on social responsibility.

5. Bicsma's information security principles

The statements set out in the previous chapter are translated to information security principles to facilitate Bicsma BV's decision-making in information security.

5.1 BICSMA BV exerts control over its information security

When using third-party services and products for the implementation and maintenance of information security, Bicsma BV fulfills and will always fulfill a steering role. Consequently, Bicsma BV will, wherever possible, make use of open standards for file formats, communication protocols and algorithms.

5.2 Operations govern, technology supports

The implementation of security measures is aimed at reducing identified information security risks to an acceptable level. Once risks are identified, Bicsma determines whether a technical solution should be implemented. Should the need arise, technical solutions must be implemented in such a way that their disruptive influence on business operations is kept to a minimum.

5.3 In the event of a potential conflict of interests, availability prevails

Should Bicsma face a risk that might be hedged in several ways, or should the envisaged security measures have a conflicting impact on confidentiality, integrity and availability, availability prevails over confidentiality and integrity. The order of ranking is as follows: availability, integrity, confidentiality. This principle does not apply to specific situations where it can be demonstrated that Bicsma BV would benefit from a different approach.

5.4 In case of doubt, Bicsma opts for low risk

Should a situation occur where it is hard to determine the risk level or should it be unclear what security measure would best suit the company, Bicsma BV opts for the alternative that implies the lowest risk.

5.5 Wherever possible, "proven technology" and "best practices" are used

The use of new technologies and methods involves new risks to reliability and efficiency. In order to exclude these risks to the greatest possible extent, Bicsma opts for methods and technologies that have already demonstrated their value in practice.

5.6 Measures are selected and implemented based on a pragmatic approach

Information security aims to reduce risks to an acceptable level. This is peformed by taking security measures. Pragmatism helps avoid working towards unrealistic ideas. Therefore, Bicsma BV adopts a pragmatic approach to the selection and implementation of measures by contemplating if the right risks are being addressed, if the measures are being implemented in an appropriate manner, or if there is an alternative to a given measure. Bicsma BV points out that the implementation of a measure depends on the degree of the risk in question and can, therefore, vary per environment.[1]

5.7 Reducing complexity in the selection and implementation of measures

The main reason why measures fail is enhanced complexity in their implementation. Complexity hinders the measure's effectiveness and impacts the effort required for its implementation and management. Therefore, Bicsma seeks to reduce complexity as far as possible.

[1] It may occur that the same measure has to meet different levels of security if used in different processes. For example, Transport requires a lower level of security than Storage, as Transport is exposed to a lower risk than Storage.

5.8 User-friendliness and cost-effectiveness

Information security addresses the way people and systems use information and the means by which information is generated, stored and accessed. To prevent information security from having an (unnecessary) negative influence on business operations and employees' day-to-day activities, Bicsma opts for solutions that offer the highest level of user-friendliness and / or cost-effectiveness.

5.9 Wherever possible, preference is given to "less restriction, more detection"

Restrictive measures limit users in their work and are, therefore, not user-friendly. Consequently, such measures might undermine the overall support for information security. Moreover, restrictive measures might distract attention from detective measures, which are crucial to demonstrate that Bicsma BV has sufficient control over its information security. Therefore, wherever possible and under the condition that the risk to be covered remains at an acceptable level, preference is given to less restrictive measures, possibly compensating them with additional detective measures.

6. Strategy

An implementation strategy is needed to ensure that information security is arranged in line with this Vision. The strategy is based on the following principles.

6.1 Bicsma BV adopts a risk-based approach

Information security aims to bring information security risks under control. This requires a proper identification of the risks Bicsma BV's information assets are exposed to. Consequently, risk assessment plays a crucial role in the strategy. A general risk assessment should be performed on Bicsma BV's business processes. As Bicsma BV never stands still and keeps facing new risks, risk assessment should become an inherent component of change management and project management within Bicsma BV.

6.2 Information security measures always have an owner

Risk assessments result in measures aimed at reducing risks to an acceptable level. In order to guarantee the adequate implementation of these measures, each measure should be assigned to an owner. This enables Bicsma BV to link every measure to a contact person, which facilitates monitoring quality and progress. Owners can delegate the implementation, management or enforcement of a measure to other parties, but cannot transfer accountability. The owner decides on behalf of the organisation whether or not a risk is acceptable.

6.3 Information security measures are always documented

In order to demonstrate its control over information security, Bicsma BV needs to have a clear picture of all the measures taken and all the agreements made in relation to the implementation, management and enforcement of the measures. To facilitate the process, all measures are documented in a well-structured and comprehensible manner. This documentation is also intended to facilitate communication and effectiveness tests.

6.4 Effective information security requires good reporting practices and proper follow-up of incidents

Regardless of how well information security is arranged, incidents will occur. In order to demonstrate that, in spite of eventual incidents, Bicsma BV maintains an appropriate level of security, it is crucial that Bicsma keep informed of incidents. Proper information should be provided on the impact the incident might have (had) on the business processes and/or personal safety, and the way the incident was followed up. Bicsma BV establishes a reporting system to collect information on the current status of security, the anomalies observed, and the follow-up of anomalies that have actually led to an incident.[2]

6.5 Bicsma BV seeks to benefit from audits to demonstrate its control over information security

Through demonstrating the high quality of its information management, Bicsma BV strives to enhance both internal and external parties' confidence and trust in the company. To that end, Bicsma BV intends to benefit from independent audits to demonstrate compliance with the Code of Practice for Information Security.

[2] That is not to say that Bicsma had no reporting system in place. The vision merely points out that reporting plays an essential part in the strategy.