KBC Group

Information Security Strategy

January, 2022

Information Security Strategy of KBC Group

Table of Contents

Information Security Strategy of KBC Group

Foreword

As a forward-looking bank and insurer, KBC is dedicated to its customers and fully embraces digital innovation to optimize and diversify its services. On this journey, risk and security management have become an even more important priority for all entities in the group. In today's world, organized hacker groups constantly test the defenses of companies, looking for weaknesses they can exploit to steal data or compromise internal systems. KBC is determined to stay ahead in this race, combining the strength of a multitude of proactive security controls with a detection and response capability strong enough to stop all attacks long before they have the potential to cause any harm.

The "Information Security Strategy of KBC Group" outlines the basic principles and building blocks realizing this goal. The document illustrates our comprehensive vision on information security management and the way all business entities and IT work together to live up to this commitment and protect the data of our customers.

Christine Van Rijsseghem

Chief Risk Officer, KBC Group

Erik Luts

Chief Innovation Officer, KBC Group

Information Security Strategy of KBC Group

Introduction

Today´s threat landscape provides a constant reminder to organisations that security incidents are not a possibility but a certainty. It is not a matter of *if* the organisation will experience a security incident, but *when.* This means it is paramount for every organisation to have in place a robust information security programme, which is geared to the organisation's information security strategy.

With this in mind, and in order to protect its customers and shareholders, KBC Group regards its Information Security Strategy as a key element of its Information Security Governance. By requiring all its entities to develop a security strategy with clear targets and metrics, KBC Group is proactively addressing the negative impact of security incidents, avoiding unnecessary costs and losses and, ultimately, providing a competitive differentiator at the moment of decision when choosing products, services and business partners.

This is accomplished by the information security controls that KBC Group continuously implements and maintains. It is a dynamic, living set of security controls, based on the best elements of ISO standards, the NIST Cybersecurity Framework and KBC's own experience with information security. At the same time, these controls also establish the binding legal/regulatory requirements to which KBC Group adheres, including the EU General Data Protection Regulation (GDPR) and European Central Bank (ECB) legal acts.

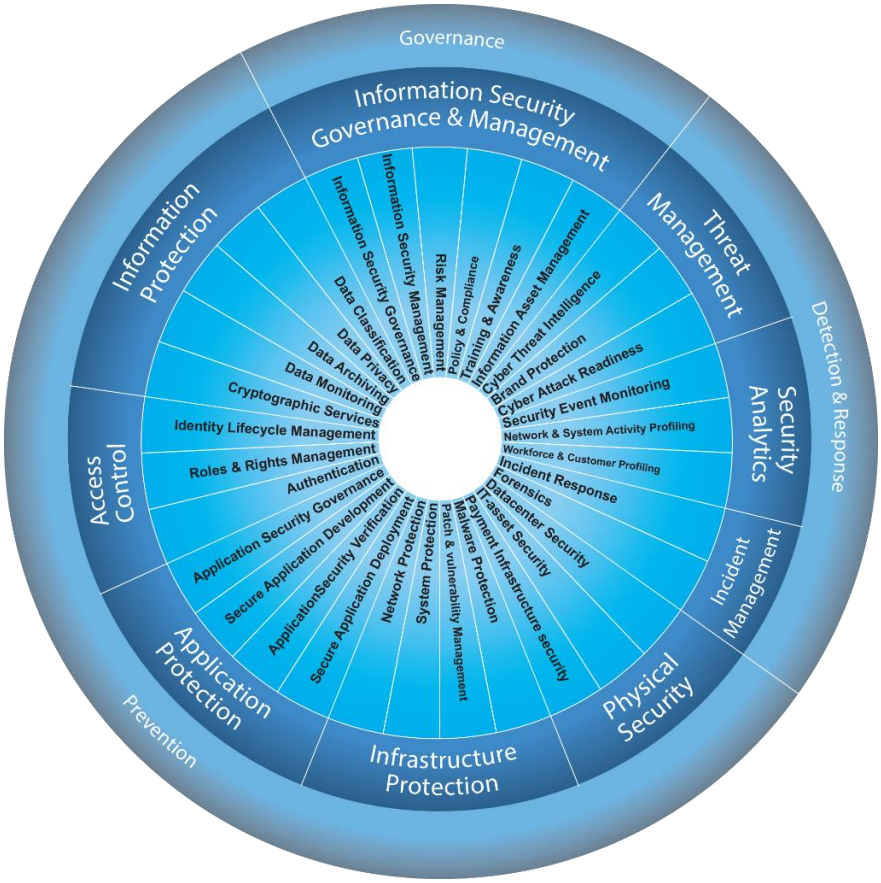

FIGURE 1 - KBC GROUP INFORMATION SECURITY UNIVERSE

Information Security Strategy of KBC Group

KBC Group Information Security Key Controls – Overview

KBC Group has defined its information security universe based on high standards. It is built around nine capabilities, subdivided into 33 sub-capabilities ('key controls'). The nature of these key controls ranges from governance, prevention, detection and response, and covers the entire information security life cycle. The key controls are:

- **Information Security Governance –** This comprises the established leadership, principles, processes and organisational structures that drive the execution of information security management within KBC Group.

- **Information Security Management** – This refers to all the requirements such as the processes, organisational structures, culture, frameworks and building blocks and resources (information, solutions, people, skills, etc.) that KBC Group applies on a day-to-day basis, in alignment with the direction set through the governance process.

- **Risk Management –** KBC Group has an effective information security risk management system in place, which correlates risk appetite with business strategy and defines relevant controls for the whole of the organisation. The effectiveness of these risk-based controls is measured in order to enable KBC Group to guarantee to its customers (and society in general), to its senior management and to its external parties (e.g. regulators) that information security risks are being properly managed.

- **Policy & Compliance –** KBC Group's comprehensive policy framework aims to create and adopt the right policies and standards and includes processes to measure knowledge of and compliance with those policies and standards. Policies and standards contain the mandatory requirements, controls, control practices, roles and responsibilities or specifications in line with best practices for information security.

- **Training & Awareness –** KBC Group considers that a comprehensive training and awareness programme is key to create awareness of the risks associated with information security, and the steps that the organisation is taking to combat those risks, across the organisation – from the board and senior management to all staff, partners and third parties. To this end, the training and awareness programmes are tailored to the audiences, updated to align with the threat landscape, and their effectiveness constantly measured. Additionally, KBC Group contributes to raising security awareness among its customers and in society as a whole – for example, through the yearly national cyber security campaigns organised by KBC Group.

- **Information Asset Management –** Information assets, in both digital and physical form, are identified and an inventory of these assets is drawn up and maintained.

- **Data Classification –** Data classification within KBC Group is based on the nature of the data (*e.g. personal identifiable information, financial information, etc.)* and on the degree of sensitivity of the data and the impact to the company if that data were to be disclosed, altered, destroyed, lost, changed, transmitted or processed illegitimately. KBC Group's classification system is simple to understand, use and apply uniformly throughout the whole of its organisation.

- **Data Privacy –** For KBC Group, it is very important to understand the privacy requirements and practices around the collection, storage, use, sharing, and transfer of personal data. For this reason, and in order to protect personal data from data thefts and fraud, this type of information is stored in a secure manner that protects it from unauthorized access.

- **Data Archiving –** Data archiving refers to the process of correctly archiving sensitive information within KBC Group: decentralised at the endpoint or server level, centralised in a collaborative space, in a dedicated archiving

solution (for 'old' information that still needs to be kept for a certain period) or in a backup system. Each of these storage areas is protected in accordance with the sensitivity of the information.

- **Data Monitoring –** Data monitoring – or, more broadly, *Data Leakage Monitoring and Prevention* – is implemented within KBC Group in order to verify whether sensitive information is securely stored, sent and used. KBC Group has several tools available not just for preventing loss of data, but also for monitoring data at rest, in use or in motion. With the advent of smartphones, tablets and personal laptops on the corporate networks, data leakage monitoring and prevention also extends beyond the walls of the KBC Group organisation, so as to prevent unintentional or deliberate data breaches.

- **Cryptographic Services –** Besides requiring the use of cryptography to protect information based on its sensitivity and exposure, KBC Group also applies cryptographic techniques where needed, including encryption, certificate management, secure key management procedures and integrity checks. Also, KBC Group defines when and how information is encrypted in order to provide effective and efficient protection.

- **Authentication –** To determine whether someone is in fact who they declare themselves to be, KBC Group has several security controls in place. One example is the use of multi-factor authentication, which is used to improve the certainty that a user is actually who they claim to be, and to avoid unauthorised manipulation of credentials.

- **Identity Management –** Identity management within KBC Group entails the management of users' digital identities and credentials throughout the lifecycle of their membership of KBC Group systems or applications. Identity lifecycle management also addresses generic accounts and machine accounts, which also require an owner who is responsible for them.

- **Roles & Rights Management –** KBC Group has a rights management process in place that governs which actions an authenticated identity can or cannot perform within an application. To limit the risk of unwanted or accidental changes, the rights that are assigned to an identity are aligned to the business need, but also support the principle of least privilege and separation of duties.

- **Application Security Governance –** Application security governance within KBC Group comprises the processes and activities through which overall software development objectives and targets are achieved.

- **Secure Application Development –** KBC Group defines the goals and creates software within development projects. In general, this includes product management, performing threat assessments, defining security requirements and gathering, high-level secure architecture specification, detailed design, and implementation.

- **Application Security Verification –** For the verification of application security, KBC Group checks and tests artefacts produced throughout the software development process. This typically includes quality assurance work such as security testing, but also other design and implementation reviews.

- **Secure Application Deployment –** This consists of the processes and activities that KBC Group carries out in order to manage software releases which have been created. This can involve shipping products to end users, deploying products to internal or external hosts, and normal operations of software in the runtime environment, such as environment hardening and issue management.

- **Network Protection –** KBC Group network protection is based on a network security policy and related standards to prevent and monitor unauthorised access, misuse, modification or denial of computer networks and network-accessible resources. Network protection covers both internal and external networks and network zones connecting the two.

Information Security Strategy of KBC Group

- **System Protection –** In order to reduce the risk of systems being compromised, KBC Group's system protection hardens the systems based on their exposure and sensitivity. Validation of system protection baselines gives assurance on the current level of protection. The security of endpoint computers or mobile devices requires careful attention as these devices are also exposed to cyber threats: in many cases end-user devices are the entry point for hackers.

- **Patch & Vulnerability Management –** KBC Group has patch and vulnerability management processes in place to prevent the exploitation of vulnerabilities that exist within information systems. Not all vulnerabilities have associated patches; thus, system administrators are not only aware of applicable vulnerabilities and available patches, but also of other methods of remediation that limit the exposure of systems to vulnerabilities.

- **Malware Protection –** KBC Group infrastructure is protected against malware. This protection is based on a layered approach using both signature-based and behaviour-based controls, with functionalities such as detection, prevention and recovery. Furthermore, KBC Group promotes appropriate user awareness on a daily basis.

- **Data Centre Security -** All data centres and technology rooms containing KBC Group's IT equipment are physically protected from unauthorised access and environmental risks by implementing a combination of access controls and applying several safety measures, which are reviewed and updated on a regular basis. KBC Group has also implemented a 2x2 data centre methodology, and frequent disaster recovery tests are carried out.

- **IT Asset Security –** Valuable IT assets located at KBC office sites are protected from loss, theft and destruction.

- **Payment Infrastructure Security –** Appropriate physical and information security measures are implemented across KBC Group to protect its assets and the sensitive payment data of its customers. These measures focus both on the security of physical assets and on the ICT systems used to provide payment services.

- **Incident Response –** KBC Group tracks, responds, measures and collects the metrics of information security incidents across the whole of its organisation. This encompasses the planning, coordination, and execution of any and all appropriate mitigation and recovery strategies and actions. To improve its effectiveness, incident response is aligned with the business objectives, regulatory obligations and the overall culture.

- **Forensics –** KBC Group examines information systems in a forensically robust manner in order to identify the root cause of information security incidents, thus enabling the discovery of details regarding attack types, methodologies and behaviour. This information can then be applied to other controls to detect and prevent similar events from occurring in the future.

- **Security Event Monitoring –** KBC Group collects and analyses security events to maintain visibility of all aspects of KBC Group´s information security footprint. This encompasses people, processes and technology that continually assess the level of visibility afforded by the collected data, in order to proactively identify gaps in coverage, opportunities for improvement of data logging, and to optimise the technologies used to generate, collect and correlate log event data.

- **Network and System Activity Profiling –** KBC Group defines the normal activity within KBC Group networks and systems; hence network or system activity which deviates from this expected activity (anomalies) can indicate a potential cyber attack. Since KBC Group proactively gathers information related to network anomalies, detailed information regarding malware behaviour, infection vectors, attack methods, Operating System (OS) changes, communication protocols, interaction with botnet infrastructure, and other data pertinent to the way in which cyber-criminals operate, this capability evolves into a predictive system capable of providing data that can be used to pre-empt cyber attacks.

- **Workforce and Customer Behaviour Profiling –** Workforce and customer behaviour profiling enables KBC Group to detect cyber attacks by defining the normal behaviour of human beings and looking for deviations from this expected behaviour.

- **Cyber Threat Intelligence** – KBC Group collects, correlates and analyses information from a variety of sources concerning the latest cyber attacks and employs derived intelligence to help detect, prevent and respond to attacks. KBC Group constantly and actively observes evolutions in cybercrime with a view to gaining an insight into the evolving criminal attack modus operandi as well as criminal motives and targets. The ultimate goal is to anticipate and disrupt the business case of cyber criminals in a timely fashion.

- **Brand Protection –** In terms of cyber security, brand protection consists of the continuous monitoring of internet references to KBC Group and its brands in order to gather relevant information that might compromise the organisation's image, reputation or security of information systems, including the detection of fraudulent websites associated with phishing or malware.

- **Cyber Attack Readiness –** KBC Group promotes cyber-attack preparation to test the response to a possible cyber attack in order to assess the preparedness and the response capabilities, and to provide a more realistic picture of the cyber security readiness. One example of how this is accomplished is via ethical hacking exercises.

KBC Group Information Security Organisation - Risk Management Framework, Roles & Responsibilities

Within the KBC Group Operational Risk Management Framework (ORMF), which sets the standards for efficient and effective management of operational risks throughout KBC Group, a scheme of three lines of defence is in place across the organisation. For reference, see 'Three Lines of Defence' model (kbc.com).

First Line of Defence: The business itself. The business operations side is fully responsible for all the risks in its area of activity and has to ensure that effective controls are in place. In so doing, it ensures that the right controls are performed in the right way, that self-assessment of the business side is of a sufficiently high standard, that there is adequate awareness of risk and that sufficient priority/capacity is allocated to risk themes. In terms of Information Security, responsibility for the first line of defence lies with the Information Security Officers and Local Operational Risk Managers.

***Second Line of Defence*:** The main goal of the second line of defence is to provide reasonable assurance to the Group CRO and local CROs. They are supported by the local risk officers, who are responsible for implementation of the ORMF within their scope. Also, the Centres of Competence (CoC) within Group Risk, supported by various other expert second-line group functions, are responsible for defining the Group-wide ORMF and related group standards, the follow-up of implementation, the group operational risk reporting and the supporting group tools. As part of KBC Group Risk, the Group Information Risk Management (IRM) unit focuses on information risks, including information security, IT-related risks and Business Continuity Management at Group level. It also includes the KBC Group Cyber Expertise and Response Team (CERT).

Third Line of Defence: Internal Audit. – As the independent third-line of control, Internal Audit is responsible for the quality control of the existing business processes. It performs risk-based and general audits to ensure that the internal control and risk management system, including Risk Policy, are effective and efficient, and to ensure that policy measures and processes are in place and consistently applied within the group to guarantee the continuity of operations. In terms of information security, Internal Audit provides independent reasonable assurance on the adequacy and effectiveness of the control environment.

Information Security Strategy of KBC Group

KBC Group's cooperation with regulators

KBC Group is under the scrutiny of multiple regulators, including the European Banking Authority (EBA), the European Central Bank (ECB) and national regulators in the countries KBC is active in.

KBC Group reports to and cooperates with these regulators to address information security risks and posts publicly available reports at Risk reports (kbc.com).

Current and future Information Security initiatives of KBC Group

KBC Group's commitment to information security is also reflected in its own information security initiatives to address current and future challenges and risks posed by the increasing reliance on IT. However, not only does technology continue to develop at a staggering pace (*AI, Internet of things, 5G*), but the threat landscape is also becoming more and more sophisticated. In addition, further enhancements are being introduced into existing information security regulations across the globe, with new regulations set to come into force while the oversight by regulators of information security compliance is steadily increasing.

Against this backdrop, KBC Group constantly reviews and adapts its own security posture, focusing among other things – but not exclusively – on:

- *User Awareness* – As well as an increase in cybersecurity awareness campaigns in KBC Group, there is a growing focus on enhancing the skills of its employees in the information security realm. This allows KBC Group employees to acquire deeper knowledge of information security, leading them to practise better information security hygiene, while at the same time developing a strong internal information security community within KBC Group.

- *Information Security Climate Monitoring* – Along with the promotion of user awareness, KBC Group also tracks the information security climate within the organisation. This means looking at individual perceptions of the value of information security based on the policies, procedures and practices in the work environments. To this end, KBC Group is developing new methodologies and tools to identify and deploy measures that facilitate employee's compliance with the policies and procedures and to avoid practices which could lead to security incidents.

- *Tackling Targeted Phishing Threats* – Phishing attacks are one of the main security threats to organisations. Attackers are employing ever more advanced methods in the execution of the attacks, which are also being carried out with an ever higher degree of personalisation. Alongside its ongoing comprehensive information security awareness programmes, KBC group is accordingly upgrading its data leakage prevention mechanisms, enhancing the security analytics processes (including predictive security) and further expanding network segmentation across the organisation. In addition the implementation of multi-factor authentication on every KBC Group device and system remains a must.

- *Ethical Hacking* – Ethical hacking is the consent-based performance of penetration testing with a view to detecting potential vulnerabilities in order to improve the security of an organisation's information system. KBC Group has been vigorously promoting ethical hacking exercises, as they help to mitigate against possible security gaps, while leading to the adoption of new preventive measures against attackers and, more fundamentally, improving the whole of its security systems.

- *Vulnerability Management* – KBC Group regards vulnerability management as fundamental to its cyber security strategy. With this in mind, not only are the practices around identification, prevention, mitigation

and vulnerability classification being improved, but new vulnerability management tools are also being integrated into the organisation to detect such vulnerabilities and develop patches and/or remedial measures to mitigate them.

- *Cloud Security* – KBC Group, in collaboration with its cloud services partners, continually reviews the security of the clouds in which it operates. Encryption and authentication methods, audit logging and segregation of data must be always be in place, both for data-in-motion and data-at-rest.

- *Governance Structure* – KBC Group regularly reviews its own governance to ensure that the roles, responsibilities and processes related to information security are coherent and that the execution of its Information Security Management framework remains efficient. Simultaneously the policies, standards and guidelines in relation to information security are continually reviewed and where necessary adapted to new challenges and risks, including regulatory compliance. Further information can be found at Corporate Governance (kbc.com).

- *Machine Learning* – Machine learning is being developed as a means to anticipate and respond to active attacks in real time. Machine learning is also being used to analyse threat patterns and learn more about cyber-delinquent behaviour so that similar attacks can be prevented in the future and in order to reduce the amount of time needed for information security specialists to deal with information security incidents.

- *Insurance* - KBC Group has a comprehensive insurance programme in place to mitigate the possible financial impact of a cyber event.

References

European Banking Authority (www.eba.europa.eu)

European Central Bank (www.ecb.europa.eu)

Financial Services and Markets Authority (www.fsma.be)

General Data Protection Regulation (www.eur-lex.europa.eu)

International Organization for Standardization (www.iso.org)

KBC Group (www.kbc.com)

National Bank of Belgium (www.nbb.be)