ECIIA presents

Auditing Cybersecurity

within Insurance Firms

Position Paper

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING
ECIIA

Auditing Cybersecurity

within Insurance Firms

November 2019

01 Thesis

The Internal Audit function within Insurance undertakings has an important role to play in providing assurance over the effectiveness of key cybersecurity processes and controls in insurance and reinsurance undertakings and that the controls are adequate to ensure the risk remains within risk appetite. It is important that key stakeholders, including Management and the Board can place reliance on the work of Internal Audit in respect of the risk management of cyber related risks, while at the same time maintaining a reasonable expectation of the extent of the Internal Audit function's responsibilities in this area.

This paper sets out the view of the ECIIA Insurance Committee (the Committee) and is intended to provide some guidance to Chief Audit Executives in the insurance sector when auditing cybersecurity based on risks expected today.

Detailed technical guidance on Cybersecurity is referred to throughout this paper and under 'further reading'.

Insurance undertakings legitimately have the need to collect customer data (some of which can be sensitive personal medical data) and therefore there is a need for internal auditors working in insurance undertakings to be able to provide assurance over the controls deployed by management to protect sensitive customer data from loss.

In light of the increasing scale and impact of cyberattacks and the introduction of European regulation such as the General Data Protection Regulations (GDPR) Network and Information System Directive, the need for European insurance undertakings to effectively manage cyber risks is paramount.

Internal audit within insurance undertakings can play a key role in supporting management's endeavour to maintain an effective cybersecurity control environment. These guidelines are intended to provide a structured approach to the provision of third line independent assurance over this important area of control in the insurance sector.

The Solvency II Own Risk Self-Assessment (ORSA) is the insurance undertaking's own risk assessment. Therefore, in 2017 EIOPA encouraged undertakings to use their own risk categories or types based on the characteristic of the specific undertaking, its business model and risk profile and not only on the standard classification of the Solvency II Directive. In the ORSA, the undertaking needs to assess all material risks from a complete perspective including an economic and a regulatory perspective, and with regard to both non-quantifiable and quantifiable risks. It is important to assess more closely operational, emerging and potential cyber risks at an appropriate level of rigour. (EIOPA-BoS/17-097 19 June 2017).

The need for effective IT cybersecurity controls was again highlighted by EIOPA in August 2018, when it stated that "Cyber risk is a growing concern for institutions, individuals, and financial markets. In less than five years, it has surged to the top positions in the list of global risks for business. The increasing number of cyber incidents, the continued digital transformation and new regulatory initiatives in the European Union are expected to raise awareness and to boost the demand for cyber insurance".

The inherent risks may vary from firm to firm, depending on the nature, size, technology infrastructure, distribution model and geographical footprint of the firm. New insurance related 'devices' via the Internet of Things (IoT) also present additional and new cyber risks. However, many of the concepts are generic and could be applied notwithstanding the legal entity structure, country or supervisory requirements.

This paper is not intended to provide guidance over the auditing of Cybersecurity risks (e.g. operational resilience, data leakage or theft) within the operations of insurance firms. The guidance provides a framework from which to build a multi-year longer term approach to auditing cyber risk. The guidance does not include the auditing of Cyber Insurance related products and the associated Insurance risks and will be the subject of a dedicated position paper covering its underwriting risk nature.

02 Background

Cybersecurity refers to the technologies, processes and practices designed to protect an organisations information assets. Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems[1]. Cyber Security is the protection of devices, services and networks - and the information on them - from theft or damage via electronic means[2].

Financial services entities, including insurers are increasingly targeted by cyber attackers alongside other key industries such as: healthcare, government agencies, and telecommunications. The wealth of customer, financial and commercially sensitive data obtained and used by insurers makes them an attractive target.

The objective of a cybersecurity audit in insurance firms is to provide management with assurance over the effectiveness of the firm's cybersecurity governance, strategy, operating model, policies, processes and their related controls to protect its assets including the most critical asset – customer data against leakage.

Fundamental to the effectiveness of controls is the recognition that a multi-layered and well integrated approach is required. As a result, the overall control effectiveness is determined by the weakest aspect of the overall position.

The purpose of third line assurance over cybersecurity is to provide multi-year insight as to how well prepared the insurance undertaking is to identify and resist a cyberattack, to recognise when an attack has been successful and to resolve the outcomes of an attack with least consequence to the firm and its customers and partners. Fundamental to this is the firm's risk assessment, the setting of an appropriate risk appetite and the development of an effective and adaptive cyber strategy and control environment.

1 IIA GTAG – Assessing Cyber Security Risk – Roles of the Three Lines of Defence Institute of Risk Management – Cyber Risk and Risk Management

2 UK National Cyber Security Centre – Introduction to Cyber Security for Board Members

03

Cybersecurity Essentials

ECIIA and FERMA[1] advocate that organisations establish a cyber risk governance system, supported by a cyber risk management framework. It must go beyond the implementation of IT measures, in order to efficiently protect their assets and ensure their resilience and continuity. The model is anchored in two strong sets of principles: the eight principles set out in the OECD recommendation on Digital Security Risk Management (2015) and the Three Lines of Defence model, recognised as a standard of Enterprise Risk Management (ERM).

Cyber risk preparedness and resilience requires a coordinated and collaborative approach which brings together IT, Risk, Human Resources, Finance, Legal, Communications and other business functions to support each aspect of cybersecurity: identification, protection, detection, response and recovery[2]. Building an effective cybersecurity culture across the business is an essential factor for success. This includes ensuring that a risk assessment is undertaken across business entities within a Group and geographical regions to take in to account any potential contagion risks.

Whilst organisation Boards are responsible for the overall organisation's cybersecurity strategy, the scale, complexity and speed of change makes this a significant challenge for many. Boards need the capability and knowledge to support and make risk informed decisions over strategy and its implementation.

1 FERMA - Federation of European Risk Management Associations

2 National Institute of Standards and Technology – Framework for Improving Critical Infrastructure Cybersecurity

The cybersecurity strategy should reflect a holistic assessment of cybersecurity risks faced by the organisation and its related risk appetite. The strategy should be regularly reviewed and form the basis for the on-going security programme for which the Board should receive regular updates.

To support the implementation of cybersecurity strategy, a sound governance structure is required to establish effective communication, reporting, challenge and assurance.

On-going risk management, informed by internal and external intelligence sources, is essential to the effectiveness and maturity of the cyber control environment. The result of this process should be appropriately communicated and changes to controls made in a timely and effective manner. It is important that appropriate and detailed knowledge of organisational assets, risks and controls are maintained. The risk of an unrecognised element against which the control is not applied could turn out to be the entry point for cyber-attack and result in operational, financial and reputational impact.

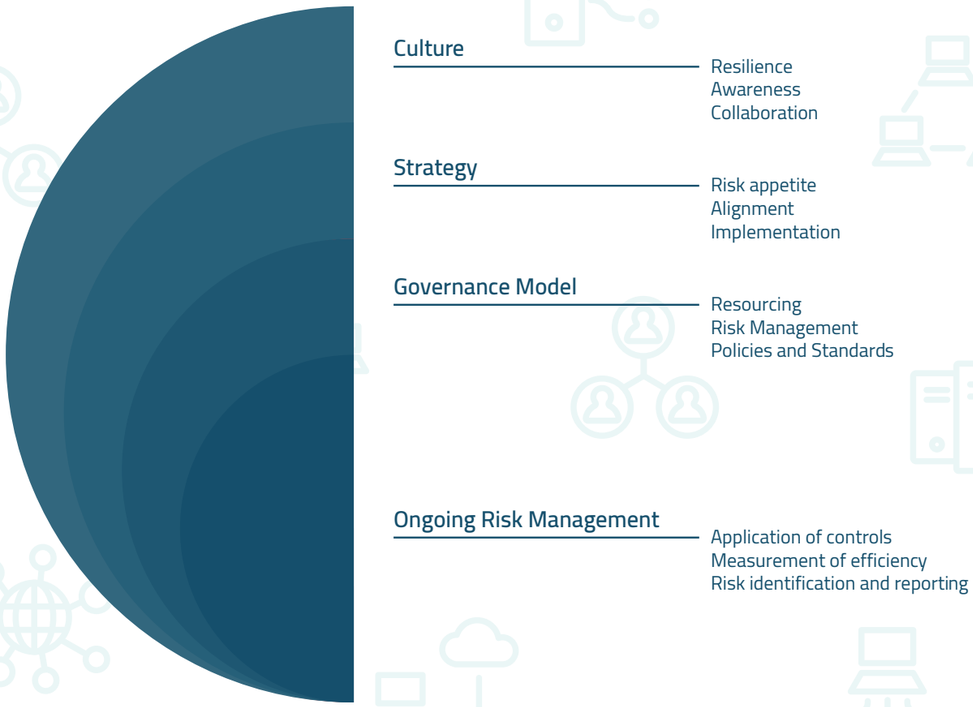


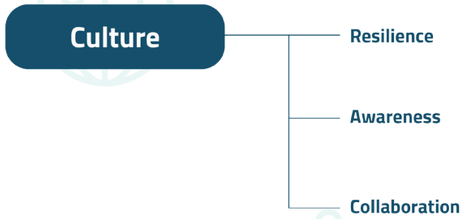
Figure 1 — Cybersecurity management model

04

Cybersecurity Audit Coverage

For the purpose of this paper, the guidelines are structured around the four elements of cybersecurity management: Culture, Strategy, Governance and Ongoing risk management.

1. Culture



A successful cybersecurity programme requires engagement at all levels. “Tone at the top”, oversight, collaboration, detection and response to cybersecurity incidents are all important cultural elements of cybersecurity strategy implementation. The following should be considered as part of a cybersecurity audit:

1.1 Cybercompetence

It is important that staff with the appropriate technical qualifications, experience and authority support the management of cyber risks in both the first and the second line. Cybersecurity management requires expert and timely decisions to be made, which can only be achieved through an appropriate level of training and experience. Given the ever present risk of cyberattacks, staffing resilience should support the full operation of the business particularly for those for digitally operated businesses. The audit should assess the capability and capacity of retained team, the level of training provided and how ongoing competence is maintained;

1.2 Awareness programme

It is important that the awareness of cyber risks is regularly communicated and their understanding tested particularly given that social engineering (e.g. voice phishing or email phishing) is one of key vectors for cyber-attacks. The audit needs to evaluate the effectiveness of awareness programmes, e.g. training, tests and exercises executed, frequency and communication channels, feedback of results and lessons learnt. Together the outcome of these processes should be used to inform a continuous improvement of the programme;

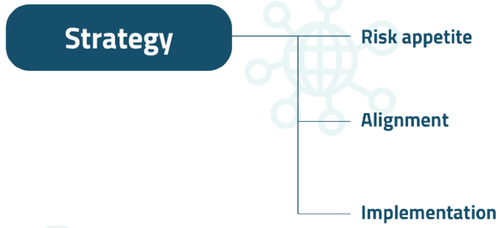
1.3 Collaboration

The multidisciplinary and pervasive nature of cybersecurity requires that the responsibility of cybersecurity is not the only objective of the IT function. It is critical that all business functions work

together, communicate and take responsibility for their part in managing cybersecurity risks. This collaboration should include both internal and external partners and industry groups.

2. Strategy

Internal Audit assurance work needs to focus on understanding the basis for the information security strategy of which cybersecurity is part, and its alignment to the business and IT strategy and how the strategy is further cascaded to the cybersecurity programme.

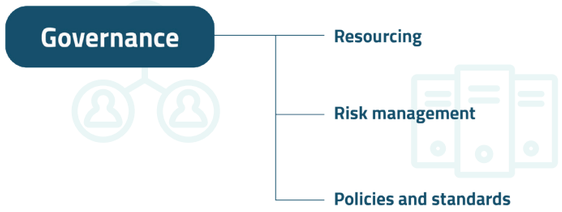


The cybersecurity programme should be regularly measured against Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) and the organisational risk appetite. The audit should take into account cyber specific and other business changes programmes when considering the position and effectiveness of any cyber strategy. Key questions and considerations for an audit also include:

- Does the organisation have a common understanding of strategy requirements? The audit should assess how high level strategy requirements are cascaded and put into actions and their consistency of management and oversight across the organisation;
- Inclusion of business functions into the delivery of the cyber programme, their responsibilities and ownership of (i) processes (ii) data, (iii) risk recognition and reporting, (iv) application inventory, (v) vendor management processes etc.

3. Governance

Review of the cybersecurity governance model helps Internal Audit to understand the formal responsibilities, resourcing, reporting and information cascading structure, which further impacts both the short and long term commitments made to the Board.



3.1 Definition and resourcing of the governance model

A cybersecurity audit should confirm whether responsibilities are clearly defined, agreed and delivered, whether resourcing at 1st and 2nd line of defence is adequate to support the successful implementation of the cybersecurity programme. The audit should also assess whether relevant stakeholders are included into the governance model;

3.2 Risk management

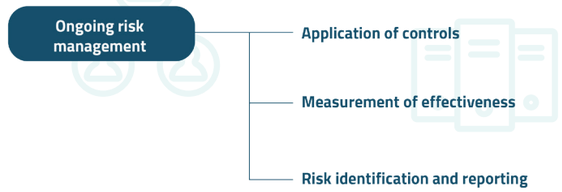
It is important to review (i) processes and inputs for risk identification (ii) appropriate documentation of risks and their assessment (iii) whether risks are adequately communicated at all levels from the detailed operational level to enterprise level risks, (iv) how risk assessments by first line of defence are reported and challenged by second line, (v) whether adequate and timely treatment for material risks are applied. It is also important to assess the consistency of independent risk evaluations and response by the second line functions, including (i) Operational risk and (ii) CISO, who is directly steering the strengthening and maturity of cybersecurity environment in organisation;

3.3 Policies and standards

The audit should include a detailed review of policies and standards to assess the coverage of relevant cybersecurity domains and how policy requirements address the risk to defined risk appetite and alignment to the cybersecurity strategy.

4. Ongoing risk management

The detailed assessment of the operation of controls enables Internal Audit not only to review the effectiveness of specific domains of Cybersecurity but also provides insight over the timeliness and quality of information provided to senior management and adherence to new and existing regulations. Understanding the details of specific controls is therefore key to the assurance outcome.



Some aspects of this assessment will need to be undertaken using skilled resources and if these resources are not available the use of co-sourcing may be necessary to complete the assessment.

The audit should consider the following elements of detailed controls:

Asset and configuration management. The audit should review the asset management lifecycle controls including the introduction, maintenance and decommissioning of assets.

4.1 Network architecture and controls

Whilst network perimeter controls including the processes and technical implementation on network support devices should be examined, the audit should also include the review of the processes supporting the internal network architecture and test the effectiveness of the network segmentation or segregation controls.

4.2 Extended IT estate management

It is increasingly difficult to clearly define the IT boundaries of an organisation (particularly in a large insurance Group) given the widespread use of 3rd party outsourcing, digitised products running on different websites, use of social networks, multiple hosting platforms including the widespread adoption of cloud computing. The audit should review the processes and technologies that supports both the Group and the individual company's secure presence on the internet, the procedures and controls over managing vendor risks (including cloud network providers) as well as processes and technologies in place to recognise and limit the exposure of "shadow IT[1]" that in turn could lead to significant data leakage risk;

4.3 Identity management and access control

Identity and access management is one of the fundamental IT controls for cybersecurity effectiveness. It is also the control where interaction amongst business departments as initiator, Human Resources as process owner and IT as support, plays an instrumental role. The audit should review the effectiveness of (i) process for granting, (ii) revoking and changing access rights, (iii) managing the least privilege principle and segregation of duties, (iv) privileged account management, (v) processes to identify unauthorised privilege escalation, (vi) authentication controls and (vii) logging and monitoring controls;

4.4 Data security

Data management and security remains one of the main security concerns in the insurance industry, particularly where personal private data is being processed or maintained. Because of the number of different data formats used across multiple database and unstructured data platforms, data security management becomes a complex task. It is therefore important to keep the inventories of data, ownership and classification accurate so that appropriate protection for sensitive data can be applied e.g. encryption and data leakage prevention. The audit should review the details of processes and data inventories in place, effectiveness of applied technological controls that support the organisation's risk appetite and regulatory requirements such as GDPR;

1 Shadow IT refers to information technology services provided outside of and without knowledge of central IT department.

4.5 Patch management

Timely application of security and other software patches is considered one of the basic hygiene controls in IT; however firms can experience difficulties in managing patching effectively. The audit review should cover the timeliness and coverage of the patch management process, inclusion of relevant software and supporting tooling. It should also include review of the discovery processes to identify, manage and escalate any non-compliance identified;

4.6 Vulnerability management

Vulnerability management includes processes to identify infrastructure and application level vulnerabilities of assets and network configuration. The audit should evaluate the coverage of vulnerability assessments, outputs and vulnerability resolution (e.g. the use made of penetration testing and the results and actions resulting from test activity);

4.7 Malware protection

Malware remains one of the key cyberattack vectors and can be a source of both targeted and non-targeted attacks. The audit should assess the effectiveness of malware protection covering preventive, detective and corrective measures across the IT estate. Malware protection by design at device build stage, regular anti-malware signature database updates, exception reporting and inputs to incident management process are all key elements to consider for the audit;

4.8 Cyber threat intelligence

Regular monitoring of threats, threat intelligence gathering and sharing is important to improve the overall security management process and raise awareness. There are a number of sources to support internal threat intelligence – from inter-

nal monitoring, vulnerability management tools to external threat libraries, monitoring services and events. The audit should evaluate the usage of different sources for intelligence gathering, effectiveness and consistency of internal communication which helps enhance the overall cybersecurity awareness and control environment;

4.9 Security over software development life cycle

Implementing the security by design principle into application development, change management and application operation are key controls. The audit should assess the secure development controls, including the secure coding controls, dynamic application security testing prior to the application being released to production. The audit should also review the security controls within the change management process, e.g. segregation of environments and strong access controls and source code controls. Regular security testing should be reviewed by Internal Audit;

4.10 Security Operations Centre and event monitoring

Event monitoring at application and infrastructure level operated through a Security Operations Centre (SOC) arrangement provides proactive defence and response capability for the cybersecurity environment. It is therefore important for Internal Audit to evaluate whether there is appropriate alignment in place to capture, analyse, monitor and report risk based security events at infrastructure, database and application layers. The review of sources and types of events being recorded, processes and actual treatment of recorded events and root cause analysis for incidents are typical areas to focus on during an audit;

4.11 Incident management and response

Recognising and responding to security incidents is key not only to limit the risk of exposure, but also to limit the damage in case of successful attack. Firms should design and test their security incident management procedures and incident response plan to contain and respond to incidents with internal and external stakeholders. The audit should assess the adequacy of the incident response plan, assess incident readiness, review and evaluate the relevant training obtained by internal teams through table top and practical “red team” exercises;

4.12 Resilience and recovery

Preparing for disaster and developing and testing disaster recovery plans is a critical activity for all organisations. Based on robust business impact assessments, Internal Audit should review the arrangements of backup processes, recovery plans in place for different scenarios, including the specifics of cyberattacks. It is also important to review the architecture and redundancy of the IT estate and arrangements in place for Denial of Service protection.

05

Planning the cybersecurity audit

Scoping the audit

The scoping of the audit should be based on:

(i) identifying the organisational systems and assets,

(ii) contextualising the supporting business processes, applications or systems with different security requirements,

(iii) understanding the existing hosting arrangements, especially where a number of elements are hosted in commoditised cloud environments; and

(iv) managing expectations of the regulatory requirements and internal stakeholders.

Considerations around scoping out and delivering separate assurance work around larger areas, e.g. (i) external hosting and cloud, (ii) Security Operations Centre controls, (iii) logical access management etc. should be considered. Furthermore, for regular Cybersecurity audits maturity level and development trends can be assessed.

Assurance over operational effectiveness

Whilst the cyber strategies, policies, frameworks, standards and reports confirm the framework for managing cyber risks, it is critically important that the audit considers appropriate levels of controls testing to enable the provision of assurance over operational effectiveness. Sampling and testing key operational details of software and hardware, process inputs and outputs are critical activities and should be supported by appropriate tooling where required.

Further Reading

- National Institute of Standards and Technology – Framework for Improving Critical Infrastructure Cybersecurity
- ISO 27001 standard
- ISACA Cobit 4.1 and Cobit 5
- SANS Institute Top 20 Cybersecurity risks
- National Cybersecurity Centre – Cybersecurity guidance
- Information Security Forum research library

06

About ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the voice of internal audit in Europe. Our role is to enhance corporate governance through the promotion of the professional practice of internal auditing. Our members comprise 34 national institutes of internal auditing from countries that fall within the wider European region, representing 48.000 members and around 12.000 active in the insurance sector. The ECIIA mission is to further the development of good Corporate Governance and Internal Audit at European level, through knowledge sharing, developing key relationships, and impacting the regulatory environment, by dealing with for the European Union, its Parliament and any other European regulators and associations representing key stakeholders.

The insurance Committee

The Committee is made up of CAEs from the insurance sector in Europe. The Committee is responsible for ensuring the internal audit profession for the insurance sector in Europe is heard by the EIOPA, the European Insurance Regulator.

The Committee promotes the professionalism of the internal audit function in the European insurance sector through knowledge sharing between the member institutes and the practitioners.

Contributors

This paper was prepared by the ECIIA Insurance Committee, with the strong support of Girts Kronbergs, CISA, CISM, Senior Audit Manager at Legal and General.

The delegates from the different countries are:

- Hervé Gloaguen, Chair (Germany, Allianz SE)
- Thierry Thouvenot (Luxembourg, ECIIA President)
- Martin Studer (Switzerland, Zurich Insurance Company Ltd.)
- Amaury de Warenghien (France, AXA Group)
- Stephen Licence (UK & Ureland, Legal and General Group)
- Manfred Schuster (Austria, Uniqa Group)
- Ann-Marie Andtback (Sweden, Sampo Group)
- Nora Guertler (Italy, Assicurazioni Generali S.p.A)
- Pascale Vandenbussche (Belgium, ECIIA Secretary General)

We would like to thank everyone involved.

Head Office
Avenue des Arts 41
1040 Brussels
Bruxelles, Belgium
www.eciia.eu

Contacts
Email: info@eciia.eu
Twitter: @EciiaInfo

Design: pedromiguelxarepe.com