BLACK CELL
Protecting critical infrastructures

Compliance and Audit Whitepaper

Table of Contents

1. Introducing Black Cell Compliance

Black Cell's Compliance (hereinafter referred to as Black Cell Compliance) division has the capabilities and experience to deliver the answers an organization needs to hear to enhance their electronic information systems and processes in order to warrant the confidentiality, integrity and availability of their information assets. Black Cell Compliance offers a variety of tailor-made consultancy services which helps organizations to comply with European Union and Member State cybersecurity and privacy legislation, international standards; to perform risk assessments and to ensure appropriate procedures are in place to guarantee business continuity and disaster recovery. Black Cell Compliance professionals combine the best domestic practices with international experience to provide objective advice and execution.

2. Compliance with EU legislation

2.1 General Data Protection Regulation (GDPR) – Data protection and privacy EU-wide

The General Data Protection Regulation (hereinafter referred to as GDPR) is justifiably the most progressive change in the last twenty years of EU data protection law, which significantly exercises influence on daily operations of data controllers and processors both from an information security and a legal point of view.

„The new rules will ensure that the fundamental right to personal data protection is guaranteed for all. The General Data Protection Regulation will help stimulate the Digital Single Market in the EU by fostering trust in online services by consumers and legal certainty for businesses based on clear and uniform rules." –European Commission statement 16/1403.

By replacing the 95/46/EC Data Protection Directive, GDPR is a regulation that meets the requirements of the 21st century' digital environment and is applicable to all organizations controlling and/or processing personal data in all member states of the European Union and European Economic Area, entered into force in May 2018.

In order to harmonize the GDPR with the national data protection law, Act CXII of 2011 on Information Self-determination and Freedom of Information was amended in July 2018. However, until the adoption of Act XXXIV. of 2019 in March 2019 the compliance of the sectoral legislation with the GDPR was not warranted. The adoption of the sectoral data protection legislation created another compliance compulsion for data controllers and processors to fine-tune their data protection procedures and documentation.

The combined application of the abovementioned sources of law is necessary to ensure the adequate level of compliance of the data controllers and processors with the GDPR. Full compliance with the GDPR and the sectoral data protection legislative acts is an ongoing procedure and definitely not a one-off event. The compliance must be continually reviewed, fine-tuned and amended to comply with the requirements set forth in the respective legislative acts. It is therefore of particular importance that data controllers and processors allocate the adequate human, administrative and technological resources to carry out their tasks, if necessary, with the assistance of 3rd party experts.

The territorial scope of the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU/EEA, regardless of whether the processing takes place in the EU or not. The material scope of the GDPR applies

to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. This also underpins that virtually every organization is affected by the obligations arising from GDPR.

Unlike the 95/46/EC Data Protection Directive, under GDPR the personal data breaches must be directly announced to the supervisory authority (in Hungary to the Hungarian National Authority for Data Protection and Freedom of Information) and in some cases the data controller shall communicate the personal data breach to the data subject. This necessitates the organizations to have a proper privacy incident management procedure that is well-known across the organization.

Black Cell Compliance assists all existing and prospective clients in achieving full compliance with the GDPR and the sectoral data protection legislation by developing adequate processes, privacy policies, data registers and by setting the appropriate level of controls in the information security systems.

Black Cell's GDPR-related services:

- Comprehensive privacy audit, including particularly but not exclusively exploration of data controlling and processing procedures, examination of the lawfulness of processing, purposes of processing, processing of special categories of personal data, conditions for consent.
- Reviewing and implementing the GDPR principles into the relevant data controlling and processing procedures.
- Performing data protection impact assessments.
- Maturity assessment of information technology systems and services supporting the data controlling and procedures. Proposing technical controls to ensure the confidentiality, availability and integrity of the controlled personal data.
- Privacy assessment of the internal documentations and policies.
- Assessing the detection, identification, communication and remediation capabilities of personal data breaches. Developing or fine-tuning the existing incident management procedure.
- Preparing the adequate documentation and record framework in accordance with the provisions set forth in GDPR.
- Supporting the data protection officer or outsourced DPO-as-a-Service.

Our main goal is to help create a GDPR compliant and well-operable data protection management system that effectively supports (and without doubt not hinders) the business goals of the organizations and that has an organic link to the existing or planned ISO-based information security and/or quality management systems.

2.2 NIS Directive – Cybersecurity for critical infrastructures

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (hereinafter referred to as NIS Directive) is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity of critical infrastructures in the EU. In the past decades, as the political-economic integration of the EU has been on a significantly lower level, the different member states have historically had very uneven levels of cyber-defence readiness, as well as completely different approaches to regulating the protection of their respective critical infrastructure.

This legislative fragmentation in itself was considered as a vulnerability. The NIS Directive strives to strengthen the overall cyber-defence preparedness of the EU as a digital single market firstly by amplifying cooperation among all the member states ("EU Security Network"), in order to support and facilitate strategic cooperation and the exchange of information, secondly by establishing equivalent cyber defence requirements across the EU, and thirdly by adopting a member state strategy that defines security goals as well as relevant policy and regulations needed to enforce the envisaged cybersecurity strategy set forth in the NIS Directive.

The scope of the NIS Directive applies to traditional critical infrastructures, such as energy, transport, drinking water supply, financial market infrastructure, digital infrastructure, banking and healthcare as well as to key digital service providers, such as online search engines, cloud computing services and online marketplaces. These organizations must comply with the security and notification requirements under the NIS Directive, that member states adopted in separate legislative acts.

In accordance with the provisions of Government Decree 270/2018. (XII. 20.) Black Cell COMPLIANCE focuses on assisting digital service providers achieving compliance with the Government Decree and the NIS Directive. The digital service providers, as essential services, must

- register at Special Service for National Security (SSNS), as this authority is the appointed national competent authority,
- conduct a risk assessment, implement and apply adequate security measures,
- notify the national competent authority about a security incident,
- review the adequate security measures at least annually, and following the occurrence of a security incident, implement necessary changes to the security measures based on deficiencies identified during the review.

3. Risk Advisory

Organizations can carry out risk assessments to support various business needs: to minimize financial loss, to avoid reputational loss, to evade work force risks or to prepare for natural disasters and cyber threats. Black Cell Compliance primarily helps organizations identify various risks that could cause business damage due to a loss in confidentiality, integrity or availability of information assets and electronic information systems.

Why carry out a cyber risk assessment? Besides the direct obligations arising from legislative acts – e.g. the NIS Directive – or vendor evaluation programmes – usually conducted by SMEs, large multinational organizations and government agencies – risk assessment is the only way to ensure that the cyber security controls an organization has in effect are appropriate to the cybersecurity threats the organization faces. Risk assessments are the foundation of every security best practice and are the first step of an effective risk management programme.

Organizations may need to comply with a variety of sectoral compliance regimes, such as PCI DSS, FFIEC, PSD2, ISO/IEC 27001 or NIS Directive. Carrying out a risk assessment is the foundation for the business actions an organization will take to achieve and retain compliance with these regimes. Black Cell COMPLIANCE offers an appropriate risk assessment procedure to all and every business need, either arising from a legislative requirement or a market

demand, to determine of quantitative and qualitative estimates of the impact of an event, related to a recognized threat.

3.1 Crown Jewels Analysis – To identify business mission critical cyber assets

Crown Jewels Analysis (hereinafter referred to as CJA) is a multipurpose tool that can be used as a risk assessment methodology by identifying the cyber assets (critical data and electronic information systems) that are most critical to the accomplishment of an organization's business mission. Nowadays the biggest threats to the electronic information systems are the targeted attacks, i.e. the Advanced Persistent Threats (APT). Organizations have to identify all of the IT assets, that may cause critical operational dependency in order to be aware of the possible targeted IT assets by outsider cyber attackers. In case of critical IT asset failure, the organizational mission objectives may become inaccessible.

The first step of CJA is setting up a dependency map, which shows the operational tasks that support the mission objectives (executives defines the missions and objectives priority) to the executives. Achieving a mission objective depends on one or more tasks being performed as intended, performance of a task depends on one or more system functions executing as intended, execution of a system function depends on one or more cyber assets operating as intended.

Based on the CJA dependency map, starting from cyber assets to achieve the mission objectives, via the dependencies the executives can define different kind of impacts (financial, operational, legal/regulative, reputational, health/safety) with the measures of the impacts. After the CJA and the MIA executions, the organization will be able to identify the real crown jewels, the most critical cyber assets according to the CJA and MIA. To establish a robust and resilient cybersecurity within the organization, the first step is the crown jewels identification.

With Crown Jewels Analysis Black Cell Compliance helps organizations to quickly and easily find their mission-critical cyber assets, including data and electronic information systems. With CJA, organizations can assign risk, business and monetary value to their assets, effectively monitor and report the crown jewels, and discover relationships between disparate assets that turn out to be the crown jewels of the organization.

3.2 Information Security Risk Assessment – Traditional approach to risk management

Assessing risks and potential threats is an important factor in running any organization, but risk assessment is vital for IT departments (or IT-focused service providers), as they have extensive control over electronic information systems and information assets processed in these systems. The international standard ISO/IEC 27001:2013 provides the specifications of a best-practice information security management system. Assessing the relevant control points of the international standard within an organization is the risk-based approach to organizational information security risk management that addresses people, processes and technology.

Information security risk assessments expresses the details around each risk scenario, assigns a likelihood and impact rating and document the final (inherent) risk score. The organizations identify cybersecurity controls that can either reduce the likelihood or reduce the impact. These control effectiveness scores should reduce the risk, resulting in the residual risk being lower than the inherent risk. The organization shall determine whether the residual risk is within the organization's risk appetite. If the specific risk exceeds the risk tolerance, the organization shall

implement a control to reduce the likelihood of occurrence, shall avoid the risk by ceasing any activity that creates it, share the risk with a third party or retain the risk.

An information security risk assessment procedure begins with a clear understanding of the business goals, potential threats that could hinder these respective goals, the likelihood of compromise and the impact of the loss. This is achieved with a comprehensive interview process performed by Black Cell COMPLIANCE experts involving all relevant stakeholders of the organization, such as senior management and IT subject matter experts. Once the organization is well-known by Black Cell COMPLIANCE consultants, the threat landscape and business risk appetite are defined, the current security control levels and potential security gaps must be discovered and documented. Armed with the documented information in-hand about the current state of the organization's risks, Black Cell COMPLIANCE can provide proactive guidance on the best security controls to mitigate the risks.

This proactive guidance, based on the combination of people-, process- and technology-oriented controls, results in a granular Risk Treatment Plan (RTP). The Risk Treatment Plan as an action plan contains the specific security controls to implement connected to a responsible stakeholder, with a strict deadline and required resources to successfully complete the implementation of the control.

3.3 Control Maturity Assessment

Black Cell Compliance recommends the performance of a control maturity assessment for every organization that intends to deploy security controls to meet the specific requirements of the organization and to have an accurate picture of the steps to be taken (e.g. the controls to be implemented) to achieve the desired control maturity. Black Cell COMPLIANCE experts have professional experience in control maturity assessments based on the controls of the international standard ISO/IEC 27001:2013, NIST SP 800-54 Rev.4, NIST Cybersecurity Framework (CSF) and FFIEC.

Structural shifts in an organization's lifecycle often result in heavily modified electronic information systems and procedures connected to the management of the organization's GRC. Therefore, it is recommended that the modification of the control environment is performed in a controlled and structured manner, in accordance with the provisions of a widely recognized standard. Thus, before any structural shift (e.g. Security Operations Centre implementation, replacement of the base IT infrastructure) the control maturity of the organization or the affected department must be assessed.

4. Business Continuity Management System

An established Business Continuity Management System (hereinafter referred to as BCMS) integrates the disciplines of crisis management, disaster recovery (information technology continuity) and business continuity (organizational/operational continuity). If a priori not required by legislation or by customers, it is a competitive business advantage for organizations to be resilient to incidents affecting their business and technology continuity. A successful BCMS will not only maintain operations during times of crisis or disaster, but also minimise cost and reduce damage and recovery time.

In the development of the BCMS, three key components need to be considered. The first critical step of a successful BCMS is in defining the scope of what to protect and how to prioritise those assets. This can be done through a business impact assessment (BIA), with the support

of the abovementioned Crown Jewels Analysis (CJA). Once the organization had identified the mission-critical cyber assets, the second step is about setting up a suitable framework for the BCMS.

Black Cell COMPLIANCE recommends a framework that consists of three main procedures. A crisis management plan provides the key communication mechanisms necessary to ensure employee and customer safety, provide initial information and direction, and organize ongoing actions. A disaster recovery plan refers to the processes in place to restore essential information technology systems and applications that enable critical business processes. The business resumption plans are specific to each critical business function and articulate the specific steps necessary to enable the respective process. These three mutually supportive procedures are essential to a successful Business Continuity Management System.

Thirdly a well-functioning BCM framework heavily relies on documented provisions and measures. It is therefore crucial to have documents which are clear-cut and easy-to-execute in the midst of a crisis, such as a guidance on authority and roles, call sheets and system-specific disaster recovery plans.

Black Cell Compliance assists organizations in their business continuity planning, as well as in the development of a robust Business Continuity Management System that includes a Disaster Recovery Plan (DRP) in accordance with the provisions of international standard ISO 22201:2012. The focus of the service is on helping organizations to reduce the effects of an incident, re-establish operations, and deliver key business services in the aftermath of a disruptive event.