Cerious Cybernetics Corps

A Crucial Assessment Report

Right now the creator draws consideration of the official to the individual and hierarchical dangers they face, how data confirmation and hazard the board best practices can prepare for ever-expanding digital security dangers, and in what way Cerious Cybernetics Corp can make openings through clients and providers who esteem free consolation

Table of Contents

1. Overview

'Cerious Cybernetics Corp.' (CCC) is a personal firm which engaged in the Domain of Research and development. Company encourages for the broad and robust policy for information assurance and risk management which safeguard their present business environment as well as a future business risk by adapting specific practice and procedure designed under the ISMS policy

The CCC has its control centre in London, England, and they centrally manage its core function in different areas such as HR, finance, IT, Data Governance, legal provision, service level contracts [including agency and Customer staff] with the help of 60 Full-time employee and additional 20 Agency representative, United States Department and UK Ministry of Defence both are the utmost valued client are managed by CCC

The CCC engaged in critical analysis and research domain and also held the Critical information of DoD and MoD, so they are expecting the operational framework which can assess their present and future requirements which is detailed and critically documented which guide the cybernetic corp executive about information assurance from a technical perspective as well business perspective .the documentation enhance their understanding about various aspects of the organization and which ultimately bring more clarity in deciding a policy, methods, review mechanism and it also ensures the adaptivity any associated resources

The CCC. representative has additionally stated an example Service Enhancement Plan inside the white paper as an element of the more extensive survey; explicitly, they want the documented clarification to concentrate on the condition of ransomware. CCC is quick to build up enhancements or actions which will ensure their IT work, including structure and information, is kept secure.

2. Executive brief

Matching to company act 2006, **Chapter 2 Section 175**, (legislation.gov.uk, 2017) The company director personally held liable if They have made any influence decision for their interest which diminished the organization reputation and assets such as intellectual property or failure of company insolvency service 2011, So In the case of severe data leakage customer lost the faith on the Company, which result to a sharp decrease in the company assets and market reputation

Conveniently, Director and officials subsidize and guide measures to make sure about the Security of information and plan accordingly to manage the risk, with sensible consideration, ability, and determination.

3. Scope

This document intends to clearly explain the boundaries of the Information Security Management System in Cybernatic Corp This document relates to all documentation and activities within the ISMS. Users of this document are members of CCC management, members of the project team applying the ISMS, and the Employee of the iT department

Company is engaged in the research development arena and serving to the Ministry of Defence and Department of Defence, so, therefore, ISMS process implementation need to be very rigorous considering the Client nature of work and implement the confidentiality, integrity and availability by Following the ISO standard 27001and Additionally CCC needs to Implement NIST Cyber Security Framework (Nist.gov, 2018)as it Deals With USA DoD

The Data in the form of the research paper is the critical assets for the Company so no matter whether data store in the cloud or on-premise location or its access by the local networks or manged by remotely, they have to protect information confidentiality.CCC is Fully liable if the information related to their customer leaked by any of the Employee, vendor or through any electronic communication Systems loophole (gov.uk, 2018)

The ISMS scope is defined considering legal, contractual, regulatory and other requirements as specified in the following items:

3.1. Processes and services

CCC is developing research for their Client which means the processed information is critical assets for the Company and no matter they store electronically or kept in the form documents; confidential data need to protect and handle sensibly, whether the data-in-transit or data in rest

3.2. Locations

CCC has his headquarters at Uk where it develops the research for the Ministry of defence, and they also operate and work for USA Department of defence under the contract. Thus they have to comply with Uk Law and regulations such as [**Computer Misuse Act. Data Protection Act, GDPR**]and also need to obey the USA Law regulations for example [computer security Act, Security And Exchange Act] under contractual agreements however the USA and UK clients infrastructure remains to be Out of scope of the ISMS [Visit **Appendix A for laws and regulation applicable to UK and USA**]

3.3. Organizational units

Every department such as HR, IT, Data Governance, Director, Finance and legal Bodies,20 Ad-Hoc Staff are under ISMS Scope

3.4. Networks and IT infrastructure

All Electronic Devices, which are part of the business communications such as a router, switches, firewall, desktop, laptops, computer, Hard drives, Network-attached storage devices are Cover Under the ISMS scope however internet leased line and Employee personal Mobile and laptop are out of the scope

4. The validity of the document

This document is valid for one year from the Date organization approved it

The owner of this document is [**IT Officer+ Decision maker+legal Bodies+HR**], must re-assess the document at least one time in the year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to evaluate

- number of events occurring from the unclear definition of the ISMS scope
- number of remedial actions taken due to an inadequately defined ISMS scope
- time spent by employees for implementing the ISMS to resolve problems concerning the unclear scope

5. Internal/External factor effect the Outcome of ISMS

It is very much essential for the CCC to evaluate the Internal and External factor which may Impact ISMS framework for managing risk

5.1. Internal factors

The internal issue which interacts with people, processes, organizations, system and deals with information assets The understating of internal issues provide help to comply with the requirements of the Standard and also align the ISMS policy with Business tactics and guide to the determine the roles and responsibilities (clause 5.3), resources (clause 7.1), and capabilities (clause 7.2).

5.1.1. **Information as Assets:** CCC created, handled, stored, managed critical and sensitive information for their Military standard clients such as MoD and DoD, hence Personal Data, sensitive customer ideas, financial information, are required to manage under the ISMS Policy standard

5.1.2. **People Related issue:** It is not shocking that HR Security plays vital roles in ISMS execution as separate annexe A 7 devoted In the ISO certification. Hence, all the significant rules, controls and management are to be expected to be with people in mind, both in-house members as well as external resources like suppliers. Hence it quite challenging for the HR to recruit the competent staff and provided appropriate information security management training

5.1.3. **Available resources:** Resources such as equipment, technologies, systems, capital, time and knowledge needs to assess for the development and solutions to design the Information security framework

5.2. External factors

5.2.1. laws and regulations: CCC needs to practice the laws and regulation applicable to across all geographical locations they serve their clients, for instance, they have headquarters in the UK, so CCC required to comply with EU GDPR, Data Protection Act, and Computer Misuse Act and they also need to satisfy the USA Laws under contractual agreements

5.2.2. Political and Economic Conditions: Elections and war both are the most prominent way to impact the ISMS framework, because it shifts the currency and policy trends directly

5.2.3. Technical Innovations: Innovations in the technology trends or case of significant threats ISMS framework need to adjust accordingly to enhance information protection

6. Understanding the expectations and needs of the internal and external parties

The DoD and MoD is the crucial player which majorly contribute to CCC revenue, So Employee, Director, legal resources, IT department Key focus to safeguards critical information of the Client and also want to maintain business continuity plan using ISO standard clause **ISO 22301:2019 8.3 and 8.5** (ISO, 2019), so In this way, CCC can manage the availability as well integrity which directly increases the revenue and reputation of the organization in the market

Cybernetics wants the ISMS Policy, which addresses the management concerns such as market reputation, disaster recovery, business loss, loss of confidential data, legal liability and Implements security controls procedure which are technical, procedural, physical, logical and managerial on the Business

Interested party	Requirements of the interested party appropriate to the ISMS
External	
Clients	Maintain Client Confidentiality,availability,Integrity
Ministry of Defence UK	Comply with the Data Protection Act, GDPR, Computer Misuse Act, Company Act 2006
Department of Defense USA	Computer Fraud and Abuse Act 1986 (FTC – Federal Trade Commission Computer Security Act of 1987
Internet connectivity/ ISP	Be Security compliant Maintain Confidentiality
Ad Hoc staff of CCC	Inform them of correct processes, rules

Interested party	Requirements of the party concerned to the ISMS
Internal	
Board of Directors	Complete service with accuracy, profitability and integrity Comply with legal requirements Protect the reputation of the organization .achieve business goals, standardize the process Protect company information (financial data, intellectual property
Staff	Provide policies, processes and relevant training Provide systems, software and tools that are fit for purpose and provide feedback mechanisms where performance is not as required

7. High-level Information security Policy

The Panel and Management of CCC located at the UK and delivering service to USA DOD, hence they are devoted to preserving the confidentiality, integrity and availability of all the physical and electronic information properties throughout their organization.

Information security necessities will continue to be aligned with CCC goals and strategic objectives. CCC is committed to implementing a Secure Operating Framework structured and conformant with the internationally recognized requirement for an ISMS Method **ISO 27001:2013**.**NIST 800-171**, **Cyber Essentials Plus certification**

The security management controls are required over, and above the ISMS baseline, the policy of the Company is to review the risks which will inform CCC of any improvement potential to the ISMS.

Policies for Information Security

CCC should have written documents, detailing security policies, standards, guidelines and procedures, and these should be readily accessible to staff and other relevant parties. There are two "levels" of documents you should keep. The first level is the Information security policy which gives a high-level view of our security objectives. It displays the reasoning for our security policies and how they tie into the organization's goals. It describes the Security we have and shows that senior management supports the organizations' security initiatives, which can be very important for gaining employee compliance. This policy provides direction for an organization, with regards to Security, and it may reference regulations, legislation and other lower-level organization policies. It should also guide how deviations to policy requirements are handle by management.

The second "level" includes lower-level policies that are simple, easy to understand and highly specific. They may describe Acceptable Use of IT systems and resources, how a company deal with the identity and access, backups data lose issue that needs to define in the policies

Standard policies

- Backup and Disaster Revival
- Access management,
- Information categorization
- Privacy and protection of directly identifiable information,
- Physical and environmental Security,
- Safeguard from malware,
- Acceptable use of resources,
- Information transmission,
- Mobile gadgets and teleworking,
- Constraints on software installation and use,
- Management of technical vulnerabilities,
- Cryptographic mechanisms,
- Communications protection,
- Supplier relations
- Clear desk Policy

8. Evaluate and Selecting Standards

ISO 27001 certification Recognized worldwide, and it can be adapt by the small organization, security firms, and even federal organizations .it is often a requirement of federal or governmental data related contracts . and if CCC match the Standard by Complying the ISO standards, then they achieve optimum information security goal. It demonstrates higher trust to clients, plus it also offers the reputation of being a safe and secure partner in the market which do not have any potential threats to Business, from either internal or external problems. ISO standards can Bring Indirect benefits to the CCC by reducing operational costs and introducing a review process into their business management, The CCC benefits when they include the cybersecurity protection visible to the team and clients include a recognized framework for addressing legal requirements to avoid the penalty from CCC business culture that is flatter where fewer intrusion threats and employees intrusion and optimize IT usage and Implement

safety policy which ensures the sustainable growth for Upcoming year; however, there are other Standards [NIST 800-171]to evaluate under the USA Legislation while CCC handle USA Department of Defence and Cyber Essentials Plus certification also proved their clients they are up-to-date to mitigate new threats and challenges for the Future

According to **TenderInfo Article**, ISO 22301, assess resilience and Security in Business continuity management systems Needs of CCC, and it is the Standard for implementing and maintaining an effective business continuity plan. It enables CCC to have a more effective response and a quicker recovery, thereby reducing any impact on people, products and the organizations' bottom line. (TendersInfo, 2019)

Following are the standards, that CCC needs to Implement in the organization to achieve the information security goal

1. **ISO 27001**
2. **Cyber Essentials Plus**
3. **NIST 800-171**

9. Risk Mitigation

CCC risk management structure applies to all risks recognized as part of the tactical business planning process and is anticipated to enable the organization to pursue and achieve the information security objectives set out in its Information Security Policy

According to **Dejan Kosutic,** managing risk is accessible in the ISO standards **ISO 27005-2018** for Information security evaluation. It is concentrated on the subsection that mentions in the **ISO 31000-2018** risk management standards and procedures document, and **ISO 31010:2010** risk assessment methods. (Kosutic, 2017)

ISO 31000, this Standard is not concentrated solely on information security risks; it can be used for any type of risks including business stability, market, credit, currency, operational, and other (Kosutic, 2017)

Figure: 1 Relationship between enterprise risk management and information security management (Kosutic, 2017)

Mostly, information security is part of the overall (i.e. enterprise) risk management in a company, with areas that overlap with cybersecurity, business continuity management, and IT management.