Security

Contents

1 Introduction

Here we spend some words for Cyber Security.

2 Keywords

- Russia

- Hacking

- Single Point of Failure

- DDoS

- Firewall

- Man in the middle

- Dictionary

- Kali Linux

- Trojan/Backhorse

- Password policies

- internal

- VPN

- identity

- integrity

- confidentiality

3 BCS Questions

3 main security control that relate to delivering any IT solution

- People

- processes

- technology

how would you improve cyber security awareness

- documentation

- education

- newsletters

- seminars, talking about real life scenarios

- social engineering

4 ISMS 27001

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS). It enables organizations manage the security of *assets* such as financial information, intellectual property, employee details or information entrusted by third parties

4.1 ISO 22301 and differences

ISO 22301 is an internationally recognised standard that is designed to allow businesses to implement, maintain and improve a business continuity management system (BCMS). The ISO 22301 standard helps you understand and prioritise threats to your organisation. Its BCMS specifies the steps you need to take to reduce the threat of disruption, protect your assets if something does go wrong, and recover quickly from any incidents.

ISO 27001 is much more prescriptive, with organisations required to choose which of the information security control objectives and controls should apply to their organisation and to justify any exclusions that they chose to adopt, and then deciding how they would implement any controls, with detailed guidance given in ISO 27002.

5 Environmental 14001

ISO 14001 sets the standard for Environmental Management Systems.

If you want to reduce waste management costs and demonstrate your commitment to protecting the environment, you need ISO 14001 certification. Implementing this global standard will also help you building trust with customers.

6 Quality 9001

ISO 9001 is used by businesses to continually monitor, manage and improve the quality of their products and services.

It is a powerful business improvement tool, providing the framework and guidance you need to help you consistently meet your customer's expectations and regulatory requirements.

7 BCM

Business continuity management (BCM) is defined in ISO 22301:2012 as "an holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities".

7.1 Impact analysis

The impact analysis phase consists of:

- **Business impact analysis (BIA)**: differentiating between critical (urgent) and non-critical (non-urgent) organisational functions, and determining the recovery requirements for each critical function.

- **Threat and risk analysis (TRA)**: determining any unique recovery steps that may be required to respond to each potential threat. In addition, impact scenarios should be considered and documented for each identified threat.

7.2 Solution design

The solution design phase identifies the most cost-effective disaster recovery solution that meets the main requirements from the impact analysis stage, and determines:

- Crisis management command structure

- Secondary work sites

- Data replication methodology between primary and secondary work sites

- Applications and data required at the secondary work site

7.3 Implementation

This stage of the lifecycle concentrates on executing the agreed strategies and tactics through the process of developing a business continuity plan (BCP).

7.4   Testing and organisational acceptance

The purpose of testing is to make sure it meets the organisation's requirements.

The 2008 book Exercising for Excellence, published by the British Standards Institution, identified three types of exercises for testing BCPs:

- **Tabletop exercises**: Typically involving a small number of people, tabletop exercises tend to concentrate on a specific aspect of a BCP.

- **Medium exercises**: A medium exercise is conducted within a *virtual world* and typically concentrates on multiple BCP aspects, prompting interaction between teams. Realism may extend to simulated news broadcasts and websites.

- **Complex exercises**: A complex exercise incorporates all the aspects of a medium exercise and aims to have as few boundaries as possible. Exercises might include no-notice activation, actual evacuation and actual invocation of a disaster recovery site.

7.5   Maintenance

Maintenance of a BCP ensures that plans remain aligned with current business practices, and can be broken down into three periodic activities:

- Confirmation of information, roll out to staff for awareness and specific training for critical individuals.

- Testing and verification of technical solutions established for recovery operations.

- Testing and verification of organisational recovery procedures.

Issues identified in the testing phase often need to be reconsidered as part of the impact analysis phase.

Following the BCM lifecycle guarantees your organisation can continue to deliver its key products and services during a disaster, and ensures that it survives thereafter.