ISO27032 – Guidelines for Cyber Security

Deloitte Point of View on analysing and implementing the guidelines

Deloitte LLP

Enterprise Risk Services – Security & Resilience

Contents

Foreword

A clearer way ahead for Cybersecurity

The increasing volume and sophistication of Cybersecurity threats – including Advanced Persistent Threats (APT), nation state sponsored threats and targeting phishing scams – demand that organisations, big and small, remain vigilant about securing systems and information accessible from the internet.

In August 2012, the International Organization for Standardization (ISO) released a set of guidelines for Cybersecurity (ISO 27032), providing guidance for improving Cybersecurity and drawing out the unique aspects of that activity and its dependencies on other security domains, such as information security, application security, network security and Internet security as the fundamental building blocks.

While the 62-page document leaves many unanswered questions regarding best practice Cybersecurity frameworks and implementations, ISO's central purpose remains simple: to provide stakeholders involved in Cybersecurity with a set of guidelines to refer to when implementing minimum controls across their organisations to protect against the risks of the Cyberspace.

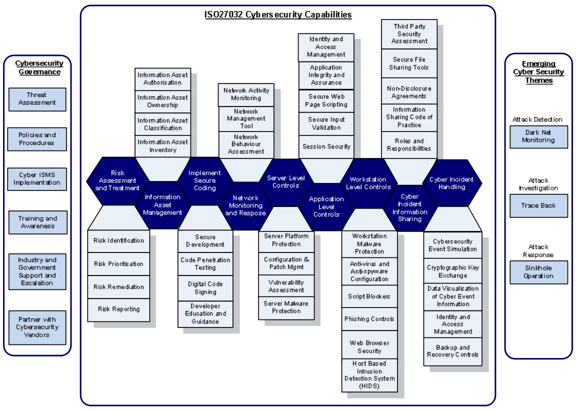
> "ISO27032 – Guidelines for Cybersecurity has not been released as an auditable international standard."
>
> **Maria Lazarte**
> Spokesman for the International Organisation for Standardization (ISO)

Even with the uncertainty, organisations involved in the Cyberspace should be encouraged that the picture surrounding Cybersecurity standards is brightening. The guidelines released contain numerous controls that indicate the International Organization for Standardization took influential industry comments into consideration.

The scale of Cybersecurity implementation based on this International Standard can be daunting as the requirements cut across business lines, functions, and geographic locations, but a good practice Cybersecurity approach is a manageable task and can be done efficiently.

Organisations involved in the Cyberspace should greet ISO27032 with vigilance and scrutiny given it is not intended to be an auditable standard but instead, a set of guidelines to ensure a standard approach to Cybersecurity implementations. In this document, Deloitte UK LLP provides a glimpse into specific provisions of the new International Standard, which is divided into framework domains and capabilities.

- Governance guidelines – adapted from the ISO27001;
- Cybersecurity technical controls – set of technical controls for addressing common Cybersecurity risks to the critical assets identified;
- Incident information sharing and handling framework guidelines;
- Emerging themes – considerations for Cybersecurity readiness.


Cybersecurity Governance
Threat Assessment
Policies and Procedures
Cyber ISMS Implementation
Training and Awareness
Industry and Government Support and Escalation
Partner with Cybersecurity Vendors
ISO27032 Cybersecurity Capabilities
Information Asset Authorisation
Information Asset Ownership
Information Asset Classification
Information Asset Inventory
Network Activity Monitoring
Network Management Tool
Network Behaviour Assessment
Identity and Access Management
Application Integrity and Assurance
Secure Web Page Scripting
Secure Input Validation
Session Security
Third Party Security Assessment
Secure File Sharing Tools
Non-Disclosure Agreements
Information Sharing Code of Practice
Roles and Responsibilities
Risk Assessment and Treatment
Information Asset Management
Implement Secure Coding
Network Monitoring and Respose
Server Level Controls
Application Level Controls
Workstation Level Controls
Cyber Incident Information Sharing
Cyber Incident Handling
Risk Identification
Risk Prioritisation
Risk Remediation
Risk Reporting
Secure Development
Code Penetration Testing
Digital Code Signing
Developer Education and Guidance
Server Platform Protection
Configuration & Patch Mgmt
Vulnerability Assessment
Server Malware Protection
Workstation Malware Protection
Anti-virus and Anti-spyware Configuration
Script Blockers
Phishing Controls
Web Browser Security
Host Based Intrusion Detection System (HIDS)
Cybersecurity Event Simulation
Cryptographic Key Exchange
Data Visualisation of Cyber Event Information
Identity and Access Management
Backup and Recovery Controls
Emerging Cyber Security Themes
Attack Detection
Dark Net Monitoring
Attack Investigation
Trace Back
Attack Response
Sinkhole Operation

The following pages will provide Deloitte UK's look at each of the areas and the interpretation of the guidelines and requirements.

Cyber governance guidelines

The new governance guidelines in this International Standard put more focus on stakeholder roles and responsibilities, policies and procedures

The proposed guidelines regarding governance of Cybersecurity are a direct adaptation of the ISO27001 – Information Security Management System (ISMS) – requirements with the suggestion of extending the scope of the existing ISMS to include the transfer and sharing of information via the Cyberspace.

The biggest and, for many, the most welcoming adaptation of the ISO27001 standard in ISO27032 is the dependency on the Risk Assessment process organisations implement to comply with ISO27001. As an organisation in the Cyberspace you are still required to identify your critical assets, identify your threats and vulnerabilities and prioritise the risks to your critical assets which will, in turn, give you a framework for Cybersecurity investment. For organisations aligned or certified to ISO27001, the risk assessment process should be a straightforward activity given the framework is established and implemented.

Organisations implementing an ISMS in accordance with ISO27001 will be aligned to the Governance guidelines of ISO27032 once the scope of the ISMS is extended to include Cybersecurity.

Technical controls

A new approach to technical controls

Technical controls defined in this International Standard rely on organisations having a good practice Cybersecurity framework in place leveraging existing ISO/IEC 27001 information security frameworks and control implementations at the organisation. The process of implementing the technical controls is simplified if an organisation complies with the ISO/IEC 27001 standard. This International Standard introduces Cybersecurity technical controls to protect against:

- Social engineering attacks;
- Hacking;
- Malicious software (malware);
- Spyware; and
- Other unwanted software

The technical controls include:

Secure coding:

Secure coding controls must be implemented to secure information collected by products in the Cyberspace.

Network monitoring and response:

Controls must be implemented to ensure network services remain reliable, secure and available. The Cyberspace should not compromise the quality of network services.

Server level controls:

Controls must be implemented to ensure servers are securely accessible from the Cyberspace and protected against unauthorised access and malicious content.

Application level controls:

Implement controls to protect against unauthorised data edits, carry out transaction logging and error handling.

End user workstation controls:

Controls must be implemented to protect the end user infrastructure across organisations against known exploits and attacks.

Organisations should train and educate users on the use of suitable technical controls to protect against known exploits and attacks. As a general guide, technical controls defined in this section of ISO27032 should be implemented.

Information sharing and incident handling

A formalised framework is suggested to share Cybersecurity information and handle incidents

This section in the International Standard provides guidelines for the implementation of a secure, reliable, effective and efficient information sharing and cyber incident response framework. The framework includes the following areas:

- Policies;
- Methods and processes;
- People and management controls; and
- Technical controls.

This International Standard introduces the concepts of IPO and IRO which the ISO advise should feature heavily in the framework developed for information sharing and incident handling.

- IPO: Information Providing Organisation – the sender of the Cybersecurity related information; and
- IRO: Information Receiving Organisation – the recipient of the Cybersecurity information.

Framework Entity	Description
Policies	Policies should be defined to address the lifecycle of the Cybersecurity incident information from creation to transfer and destruction to ensure its confidentiality, integrity and availability are maintained.
Methods and Processes	To implement the policies defined in the framework and ensure consistency in practices of information sharing and incident handling, the appropriate methods and processes should be in place which all parties involved in the information sharing practices follow.
People and Management	Identify the stakeholders involved in the information sharing and cyber incident handling framework and enable the process by implementing training and awareness controls and investigating potential alliances based on technology, industry or specialist area.
Technical	Specific techniques for implementing the policies, improving the information sharing processes and automating the management controls to deal with the changing Cybersecurity risk environment.

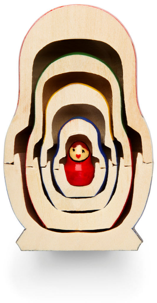
Emerging cyber themes

The digital revolution is driving business innovation and growth, yet also exposing us to emerging Cybersecurity threats. This International Standard gives focus to three main themes of Cybersecurity that Intelligence agencies and national bodies concerned with the protection of critical national infrastructure are dedicating research time in understanding in order to provide practical solutions organisations can implement to help mitigate these threats.

Dark Net Monitoring

Cybersecurity Attack Detection

Dark net monitoring is an effective method to analyse malicious traffic. Any traffic on dark net hosts is confirmed as malicious given the IP addresses are not in use. Why the name Dark net? Because there is nothing “lit up” inside these networks. The real world example of Dark net attacks, is receiving a bill from a company that has gone into administration years ago (e.g., receiving a bill from Woolworths). The bill is obviously illegitimate and does not come from a valid source therefore the person sending this information is a confirmed scammer or attacker. Monitoring these addresses will allow organisations to respond promptly to any illegitimate activity carried out through these network addresses.



Trace Back

Cybersecurity Attack Investigation

Trace back is tracking the attack back to a source hacker/criminal so that one has the ability to punish them and/or ensure they do not conceal themselves and launch new attacks. This will help significantly reduce the number of attacks organisations face every day. The controls are currently very difficult to implement in a practical sense. One reason is that today’s Internet is stateless. There is too much data in the Internet to record it all. Another reason is attackers can use IP spoofing and can therefore, for example, through unauthorised access, send millions of emails using a valid organisation’s email address resulting in the mailbox being bombed with millions of replies.

Sinkhole Operation

Cybersecurity Attack Response

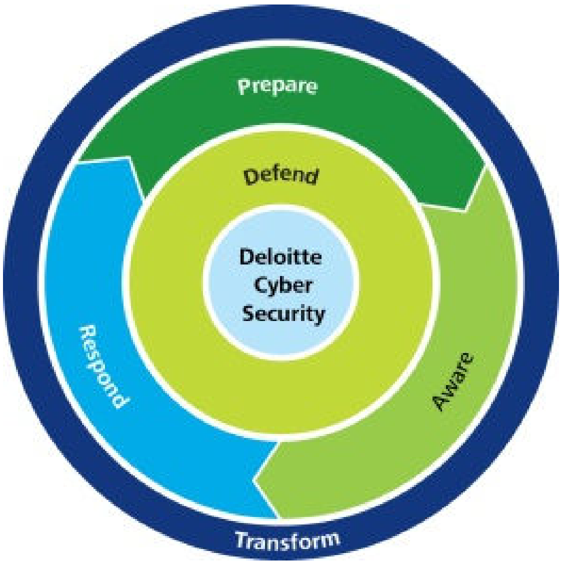
A sinkhole operation is defined as a method in which organisations redirect specific IP network traffic that could be malicious for different security reasons including analysis, diversion of attacks and detection of irregular activities. This technology has long been deployed by Tier-1 ISPs globally usually to protect their downstream customers. This International Standard suggests organisations globally should also consider implementing Sinkhole Operations to monitor specific IP traffic without informing the potential attacker, providing valuable intelligence regarding the security threats their networks are facing.

About Deloitte

Deloitte UK's capabilities

We help organisations to **prepare** for, be **aware** of and **respond** to Cybersecurity threats.

Deloitte's ability to draw upon a broad range of in-house expertise, insight from the Deloitte global network and strategic relationships with market leading vendors allows us to offer a complete Cyber capability to organisations.



Prepare

Our skilled practitioners have a track record of delivering strategic cyber simulations and crisis management exercises based on methodologies adopted from military war-games.

The team pressure-tests cyber incident management strategy and planning so that hidden errors, false assumptions, gaps in plans and unrealistic expectations are exposed and eliminated before plans have to be deployed in the real world.

Aware

Our unique relationship with a number of key security technology vendors, combined with our technical expertise and proprietary Cyber Threat Intelligence portal, allows us to offer a tailored view of an organisation's threat landscape. We are able to go beyond standard risk feeds or static reviews, to give organisations actionable, timely and integrated cyber threat intelligence.

Respond

Effective cyber incident response requires flexibility and the ability to make proactive decisions, often with limited intelligence. Deloitte's ability to draw upon a broad range of in-house expertise allows us to provide the incident management and response services along with investigation and remediation to help steer organisations through cyber incidents.

For more information, please see our online resources:

http://www.deloitte.co.uk/cyber

Or contact us:

cybersecurity@deloitte.co.uk

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Member of Deloitte Touche Tohmatsu Limited