

# Cybersecurity

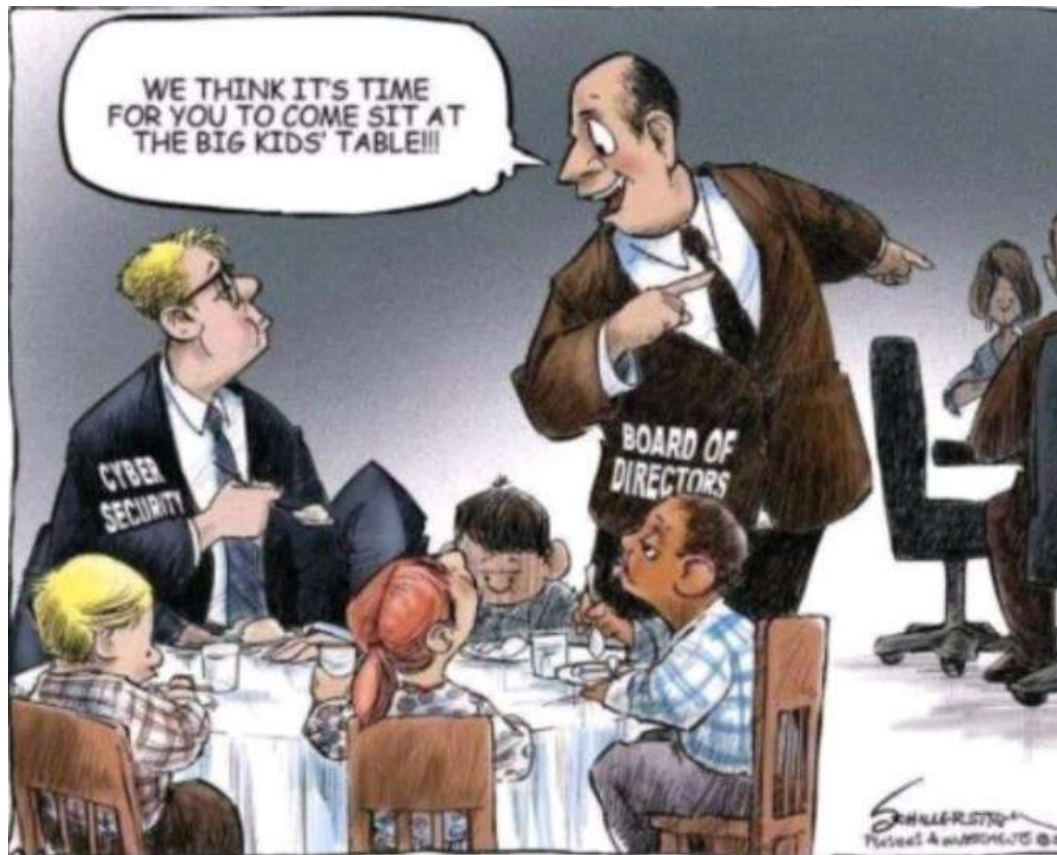
## International Frameworks and Standards

**Alberto Bastos**, CISSP, CDPSE, CGEIT, CRISC, GRCP, MCRM, MCSO, PMI-ACP

**Founder & CEO Modulo Security**

**abastos@modulo.com**

**@albastos**





Standards

# Cybersecurity International Standards





# ISO 31000 – Risk Management

**PUBLICATIONS**

## ISO 31000:2018 - RISK MANAGEMENT

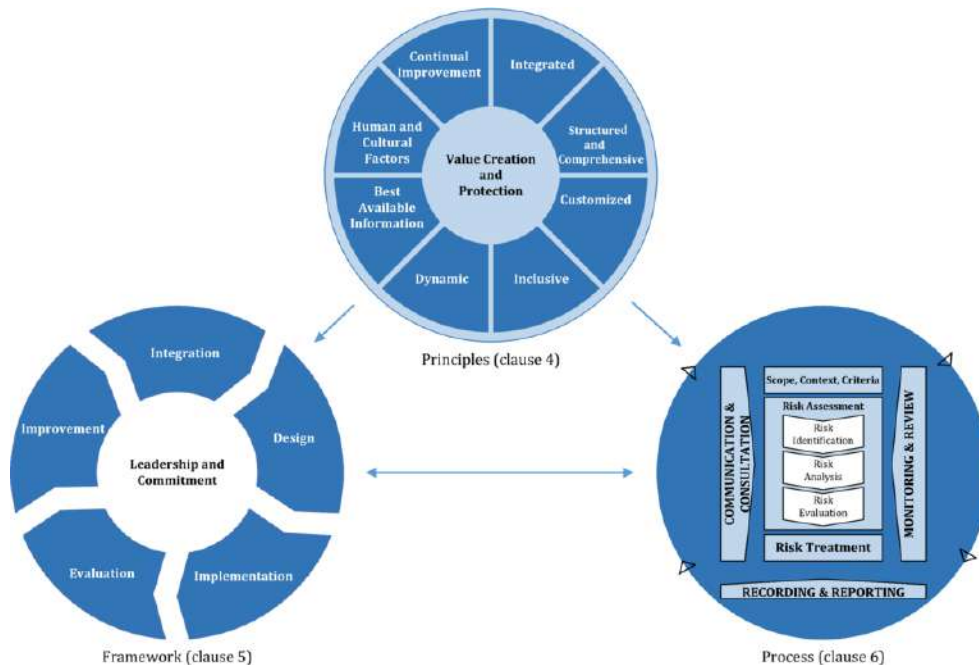
### A PRACTICAL GUIDE

Year of publication: 2021 | Edition: 1

Every organization faces risks that could impact its objectives. Organizations that have identified risks and committed to the effective management of those risks will be better prepared to deal with them. This handbook, published jointly by ISO and UNIDO, provides valuable insights into the implementation of ISO 31000 Risk management – Guidelines.

[PREVIEW](#)

ISO 31000



# ISO 27001 Serie



Standards About us News Taking part Store Q Shopping cart EN MENU

ISO

POPULAR STANDARDS

## ISO/IEC 27001

### INFORMATION SECURITY MANAGEMENT

When it comes to keeping information assets secure, organizations can rely on the ISO/IEC 27000 family.

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

**MANAGEMENT SYSTEM STANDARDS**

Providing a model to follow when setting up and operating a management system, find out more about how MSS work and where they can be applied.

# Controls – Best Practices

Standards About us News Taking part Store Q 🛒 EN ▾

ISO

ICS > 35 > 35.030

## ISO/IEC 27002:2022

### Information security, cybersecurity and privacy protection – Information security controls

**ABSTRACT** [PREVIEW](#)

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- a) within the context of an information security management system (ISMS) based on ISO/IEC27001;
- b) for implementing information security controls based on internationally recognized best practices;
- c) for developing organization-specific information security management guidelines.

**GENERAL INFORMATION**

Status :  Published	Publication date : 2022-02 Corrected version (en) : 2022-03
Edition : 3	Number of pages : 152
Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	

#### BUY THIS STANDARD

FORMAT	LANGUAGE
<input checked="" type="checkbox"/> PDF + EPUB	English ▾
<input type="checkbox"/> PDF + EPUB + REDLINE	English ▾
<input type="checkbox"/> PAPER	English ▾

CHF **198** [BUY](#)

# Privacy Information Management

Standards About us News Taking part Store

ISO

TC > ISO/IEC JTC 1/SC 27

## ISO/IEC 27701:2019

### Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

**ABSTRACT** [PREVIEW](#)

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

#### GENERAL INFORMATION

Status :  Published	Publication date : 2019-08
Edition : 1	Number of pages : 66
Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	
ICS : 35.030 IT Security	

#### BUY THIS STANDARD

FORMAT	LANGUAGE
<input checked="" type="checkbox"/> PDF + EPUB	English
<input type="checkbox"/> PAPER	English

CHF **178** [BUY](#)



# Information Security Risk Management



The screenshot shows the ISO website page for ISO/IEC 27005:2018. The page features the ISO logo, navigation links (Standards, About us, News, Taking part, Store), and a search bar. The main heading is "ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management". Below the heading, there is an "ABSTRACT" section with a "PREVIEW" button. The abstract text describes the document's purpose and applicability. To the right, there is a "BUY THIS STANDARD" section with options for format (PDF + EPUB, PDF + REDLINE, PAPER) and language (English). The price is listed as CHF 178, and there is a "BUY" button. At the bottom, there is a "GENERAL INFORMATION" section with status and publication date.

**TC** → ISO/IEC JTC 1/SC 27

## ISO/IEC 27005:2018

### Information technology – Security techniques – Information security risk management

**ABSTRACT** [PREVIEW](#)

This document provides guidelines for Information security risk management.

This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of Information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.

This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

**BUY THIS STANDARD**

FORMAT LANGUAGE

PDF + EPUB  English

PDF + REDLINE  English

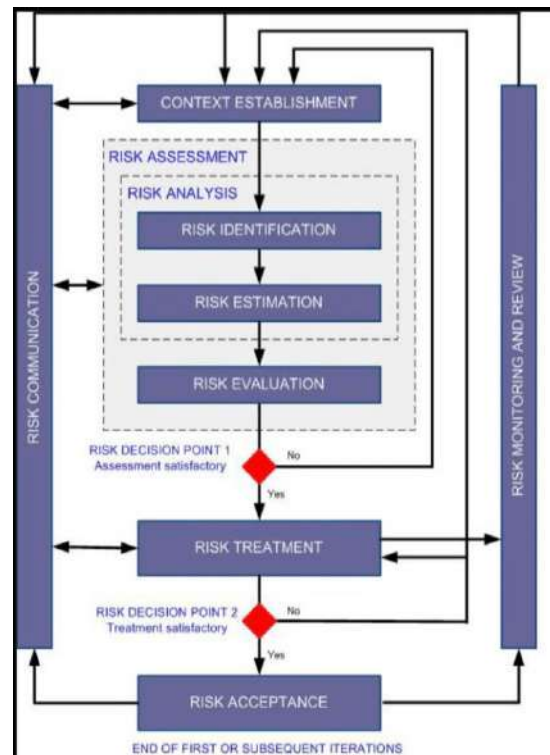
PAPER  English

CHF **178**

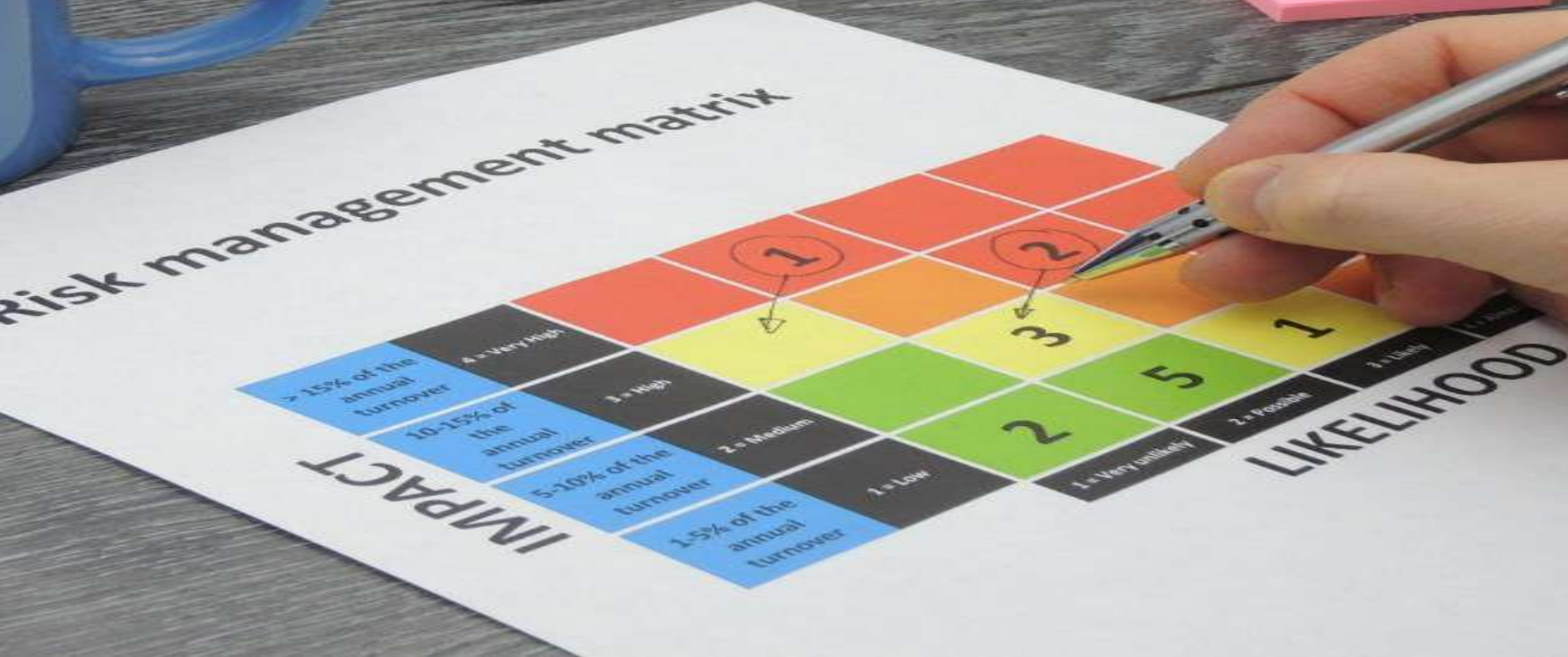
[BUY](#)

**GENERAL INFORMATION**

Status : Published Publication date : 2018-07

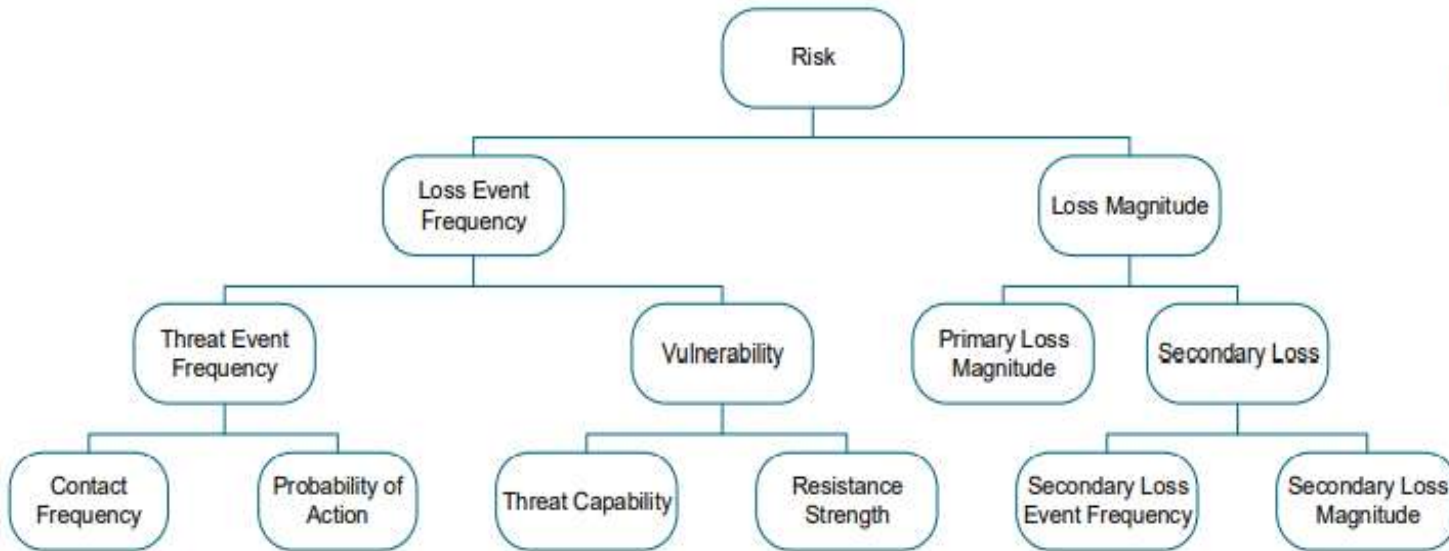


# Quantitative Risk Management



# Open FAIR™

## Factor Analysis of Information Risk



# Open FAIR™ – ISO/IEC 27005 Cookbook

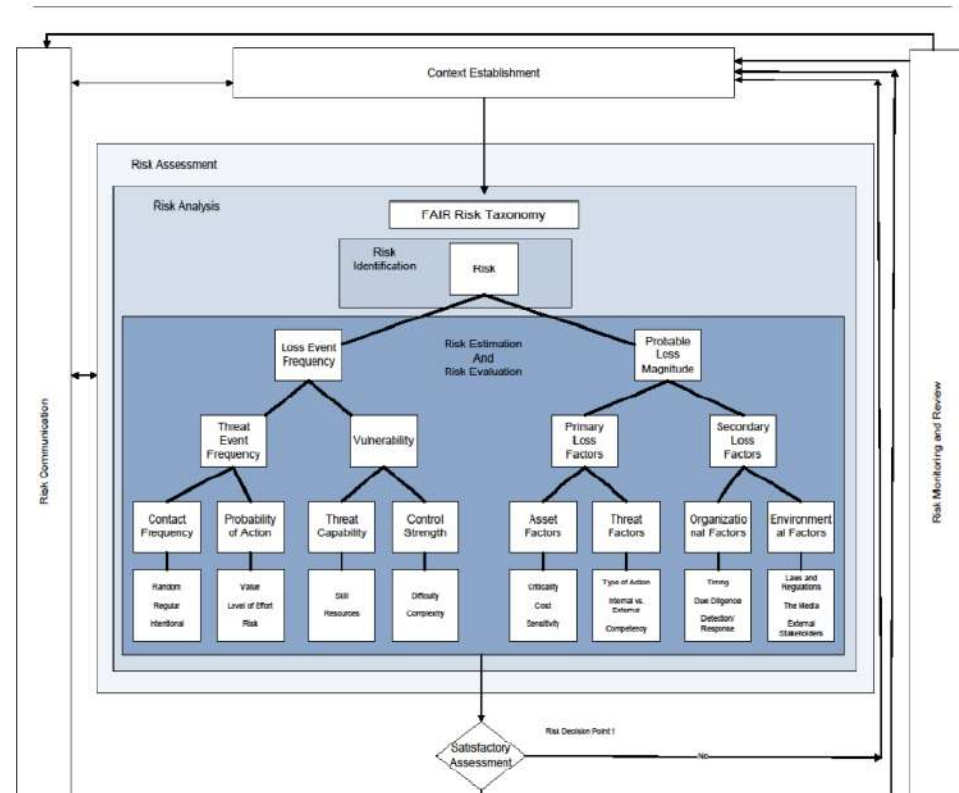
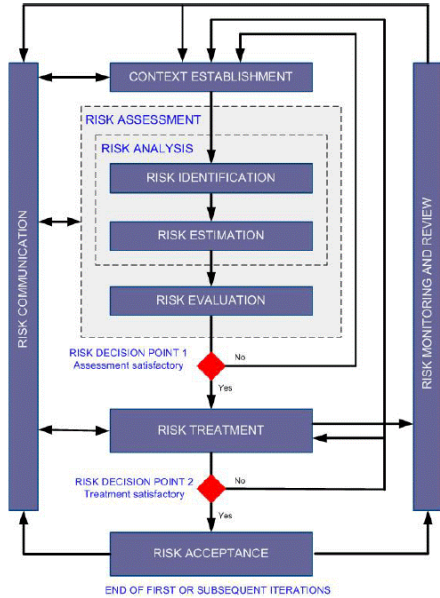
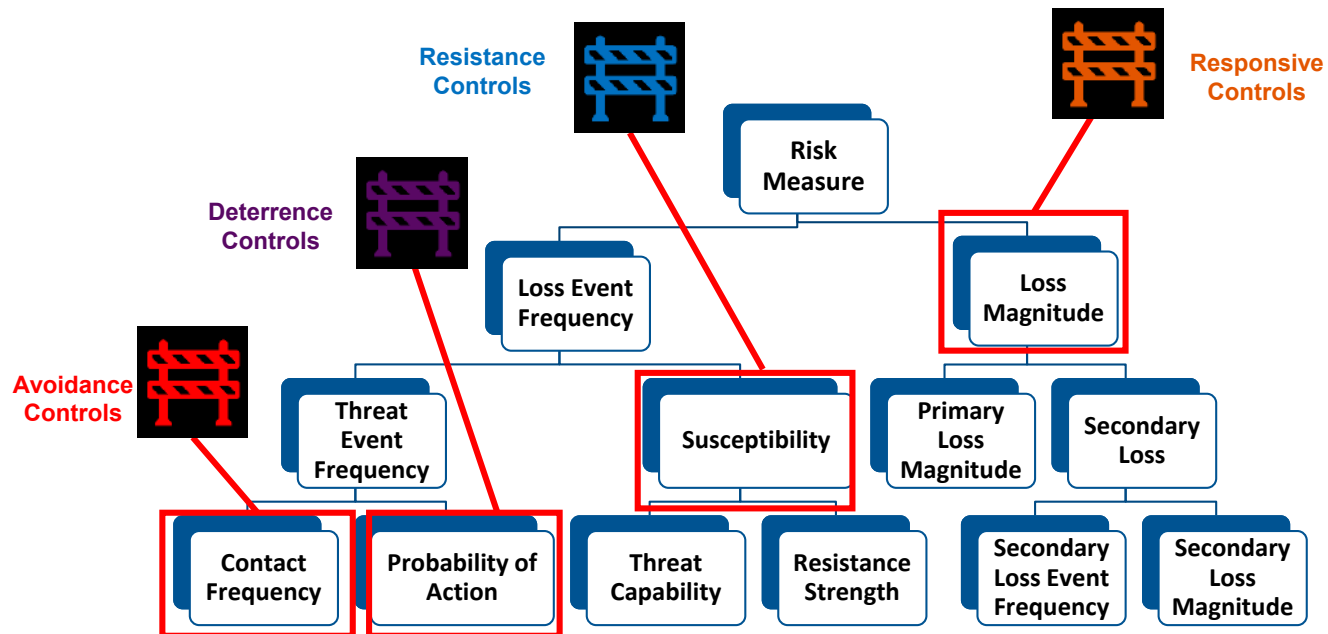


Figure 3: ISO/IEC 27005 – FAIR Integration Model



# Risk Reduction with Treatment Options



Alberto Bastos  
Me

Aaron Piper

Layout

Viewing CIS Controls V8 ...



## Welcoming CIS Controls Version 8!

Learn about v8 creation, changes, updates in resources and tools, and more.

Center for Internet Security

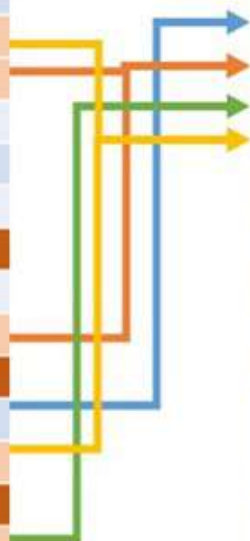
May 18, 2021

Proprietary

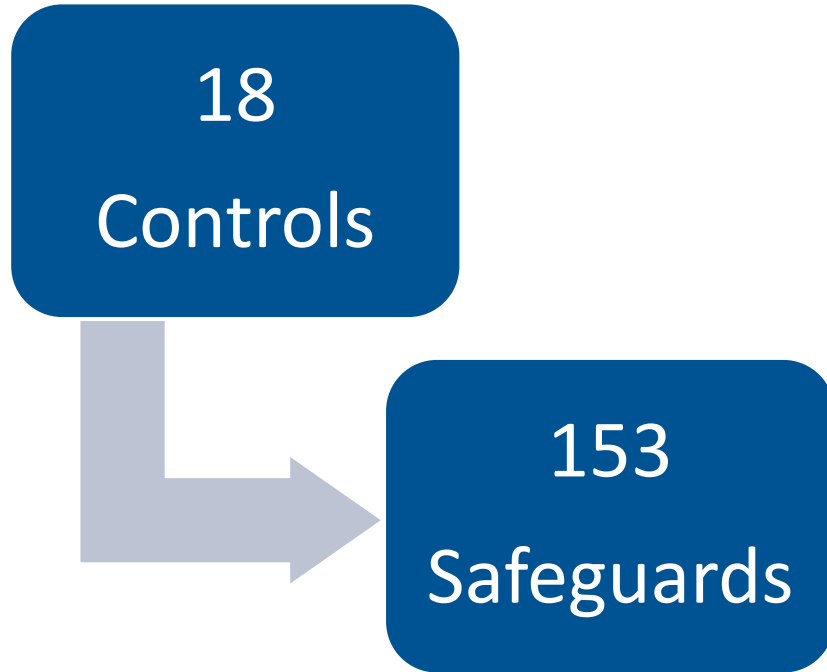


#	Description – CIS Controls v7
1	Inventory of Hardware
2	Inventory of Software
3	Continuous Vulnerability Management
4	Control of Admin Privileges
5	Secure Configuration
6	Maintenance and Analysis of Logs
7	Email and Browser Protections
8	Malware Defenses
9	Limitation of Ports and Protocols
10	Data Recovery
11	Security Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

#	Description – CIS Controls v8
1	Inventory and Control of Enterprise Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Management
9	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing



# Critical Security Controls v8





# Top 18 Controls

CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing



# Implementation Groups (IGs)

CIS defines Implementation Group 1 as Basic Cyber Hygiene



**IG1** is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56**  
Cyber defense  
Safeguards



**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

**74**  
Additional  
cyber defense  
Safeguards



**IG3** assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

**23**  
Additional  
cyber defense  
Safeguards

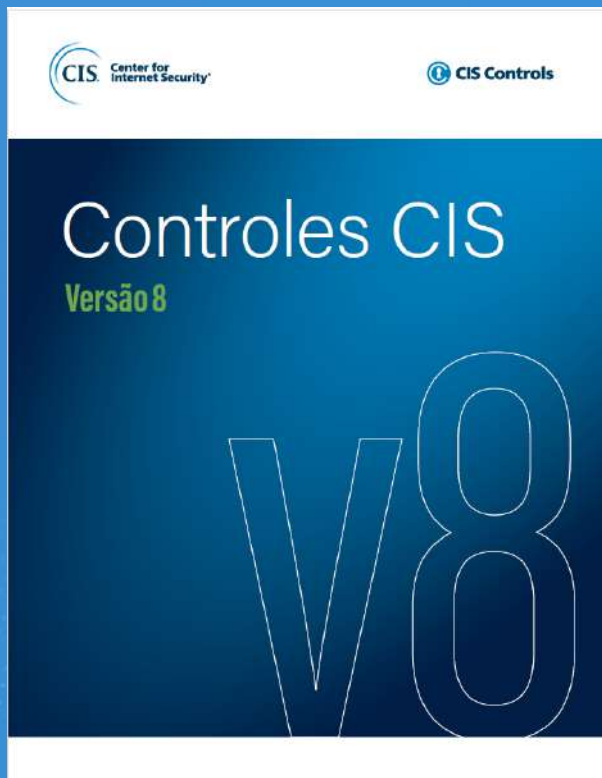
Proprietary

Total Safeguards **153**

10

<input checked="" type="checkbox"/>	Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3
<b>CIS Control 3 - Data Protection</b>							
Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.							
<input checked="" type="checkbox"/>	3.1	<a href="#">Establish and Maintain a Data Management Process</a>	Data		●	●	●
<input checked="" type="checkbox"/>	3.2	<a href="#">Establish and Maintain a Data Inventory</a>	Data		●	●	●
<input checked="" type="checkbox"/>	3.3	<a href="#">Configure Data Access Control Lists</a>	Data		●	●	●
<input checked="" type="checkbox"/>	3.4	<a href="#">Enforce Data Retention</a>	Data		●	●	●
<input checked="" type="checkbox"/>	3.5	<a href="#">Securely Dispose of Data</a>	Data		●	●	●
<input checked="" type="checkbox"/>	3.6	<a href="#">Encrypt Data on End-User Devices</a>	Devices		●	●	●
<input checked="" type="checkbox"/>	3.7	<a href="#">Establish and Maintain a Data Classification Scheme</a>	Data			●	●
<input checked="" type="checkbox"/>	3.8	<a href="#">Document Data Flows</a>	Data			●	●
<input checked="" type="checkbox"/>	3.9	<a href="#">Encrypt Data on Removable Media</a>	Data			●	●
<input checked="" type="checkbox"/>	3.10	<a href="#">Encrypt Sensitive Data in Transit</a>	Data			●	●
<input checked="" type="checkbox"/>	3.11	<a href="#">Encrypt Sensitive Data at Rest</a>	Data			●	●
<input checked="" type="checkbox"/>	3.12	<a href="#">Segment Data Processing and Storage Based on Sensitivity</a>	Network			●	●
<input checked="" type="checkbox"/>	3.13	<a href="#">Deploy a Data Loss Prevention Solution</a>	Data				●
<input checked="" type="checkbox"/>	3.14	<a href="#">Log Sensitive Data Access</a>	Data				●

# CIS v8 in portuguese



## Reconhecimento

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



# CIS RAM (Risk Assessment Method)



Política Definida?

5 - Política escrita aprovada

- 1 - Não existe Política
- 2 - Política informal
- 3 - Política parcialmente escrita
- 4 - Política escrita
- 5 - Política escrita aprovada
- Desconhecido / Não se enquadra
- N/A

Controle Implementado?

3 - Implementado em alguns sistemas

- 1 - Não Implementado
- 2 - Partes da Política implementadas
- 3 - Implementado em alguns sistemas
- 4 - Implementado na maioria dos sistemas
- 5 - Implementado em todos os sistemas
- Desconhecido / Não se enquadra
- N/A

Controle Automatizado?

3 - Automatizado em alguns sistemas

- 1 - Não automatizado
- 2 - Partes da Política automatizadas
- 3 - Automatizado em alguns sistemas
- 4 - Automatizado na maioria dos sistemas
- 5 - Automatizado em todos os sistemas
- Desconhecido / Não se enquadra
- N/A

Controle Reportado?

3 - Reportado para alguns sistemas

- 1 - Não reportado
- 2 - Partes da Política reportadas
- 3 - Reportado para alguns sistemas
- 4 - Reportado para maioria dos sistemas
- 5 - Reportado para todos os sistemas
- Desconhecido / Não se enquadra
- N/A

Privacy Law

LGPD



## Relatório de Impacto à Proteção de Dados Pessoais

Setembro de 2020

 BANCO CENTRAL  
DO BRASIL

## GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)



Agosto/2020



# Accountability

WHO IS  
ACCOUNTABLE



# GDPR Violations

Violation	Number of Fines
Insufficient legal basis for data processing	403 (with total € 447,383,631)
Non-compliance with general data processing principles	257 (with total € 825,250,574)
Insufficient technical and organisational measures to ensure information security	228 (with total € 100,606,719)
Insufficient fulfilment of data subjects rights	110 (with total € 17,748,370)
Insufficient fulfilment of information obligations	99 (with total € 235,798,875)
Insufficient cooperation with supervisory authority	50 (with total € 296,129)
Insufficient fulfilment of data breach notification obligations	23 (with total € 1,482,591)
Insufficient involvement of data protection officer	12 (with total € 350,600)
Insufficient data processing agreement	8 (with total € 1,048,080)
Unknown	6 (with total € 22,704,400)
Insufficient fulfilment of data subject rights	3 (with total € 89,000)



 Newsletter



# Cybersecurity e Boas Práticas

Atualidades, tendências e boas práticas em segurança cibernética, privacidade, gestão de riscos e compliance



De **Alberto Bastos**  
CEO & CTO na Modulo Security Solutions

Publicada semanalmente  
**5.381 assinantes**



# Thank you!

**Alberto Bastos, CISSP, CDPSE, CGEIT, CRISC, GRCP, MCRM, MCSO, PMI-ACP**  
**Founder & CEO Modulo Security**  
**abastos@modulo.com**  
**@albastos**