Cybersecurity

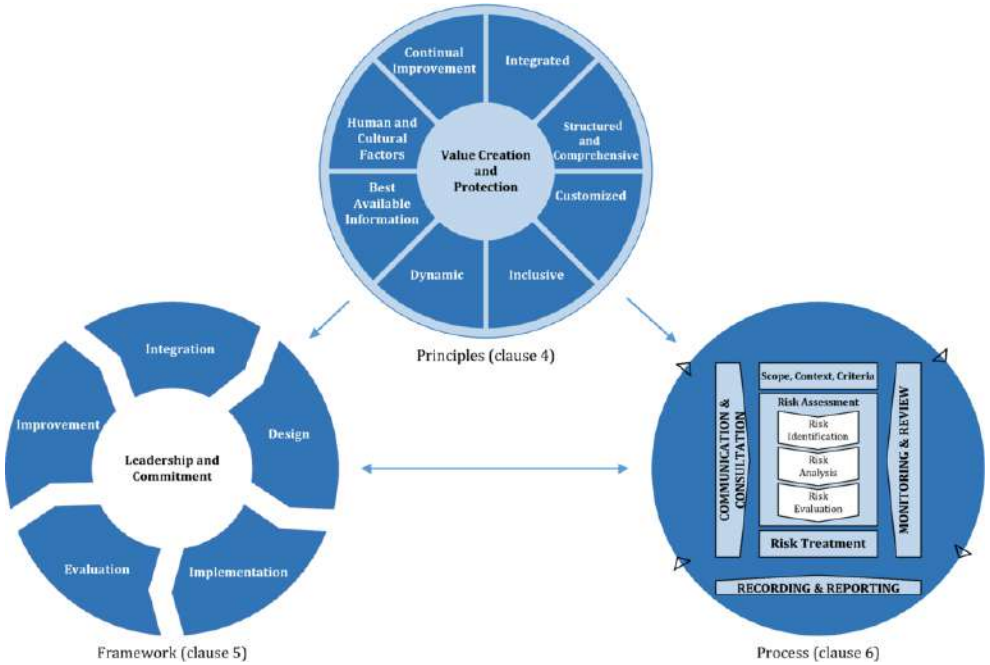
International Frameworks and Standards

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

Cybersecurity International Standards

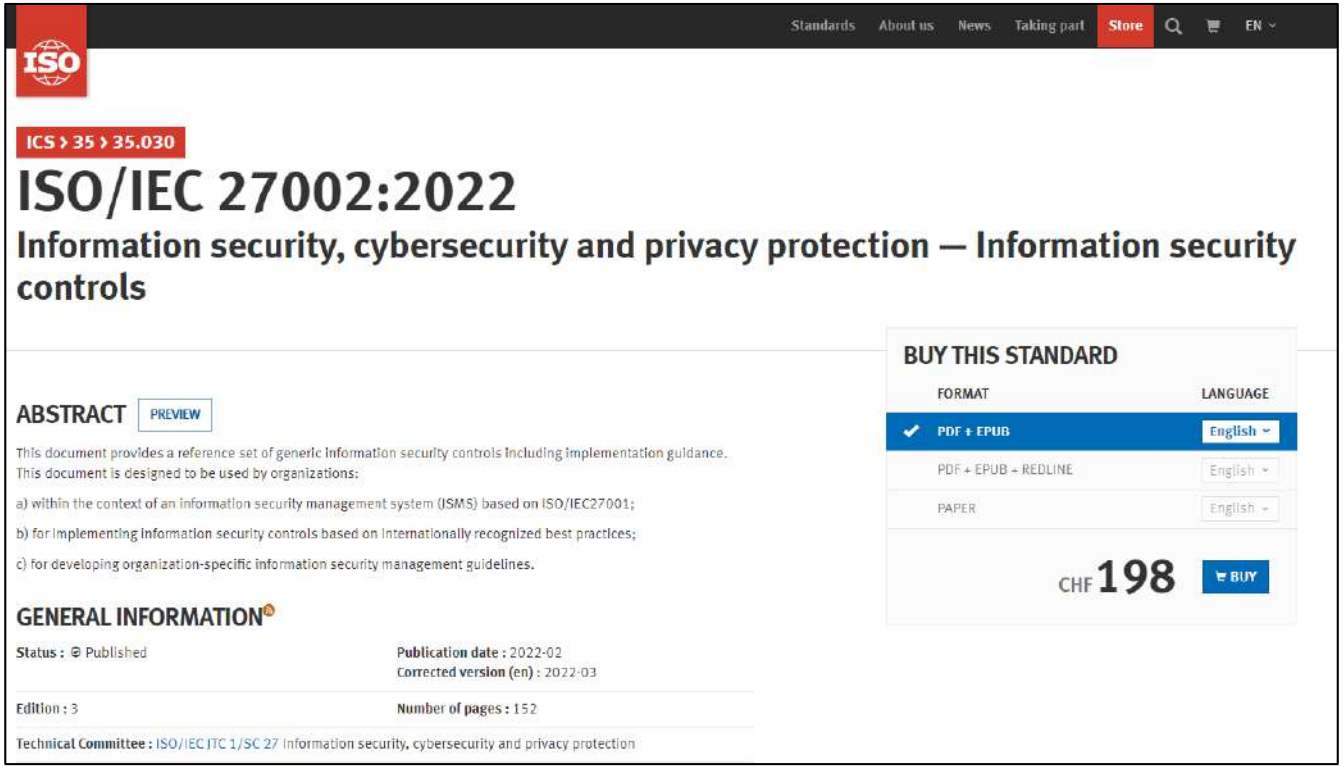

ISO
International Organization for Standardization
ABNT
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS
translate
The Open Group
Open
Open FAIR
CIS
Center for Internet Security®
Confidence in the Connected World

ISO 31000 – Risk Management

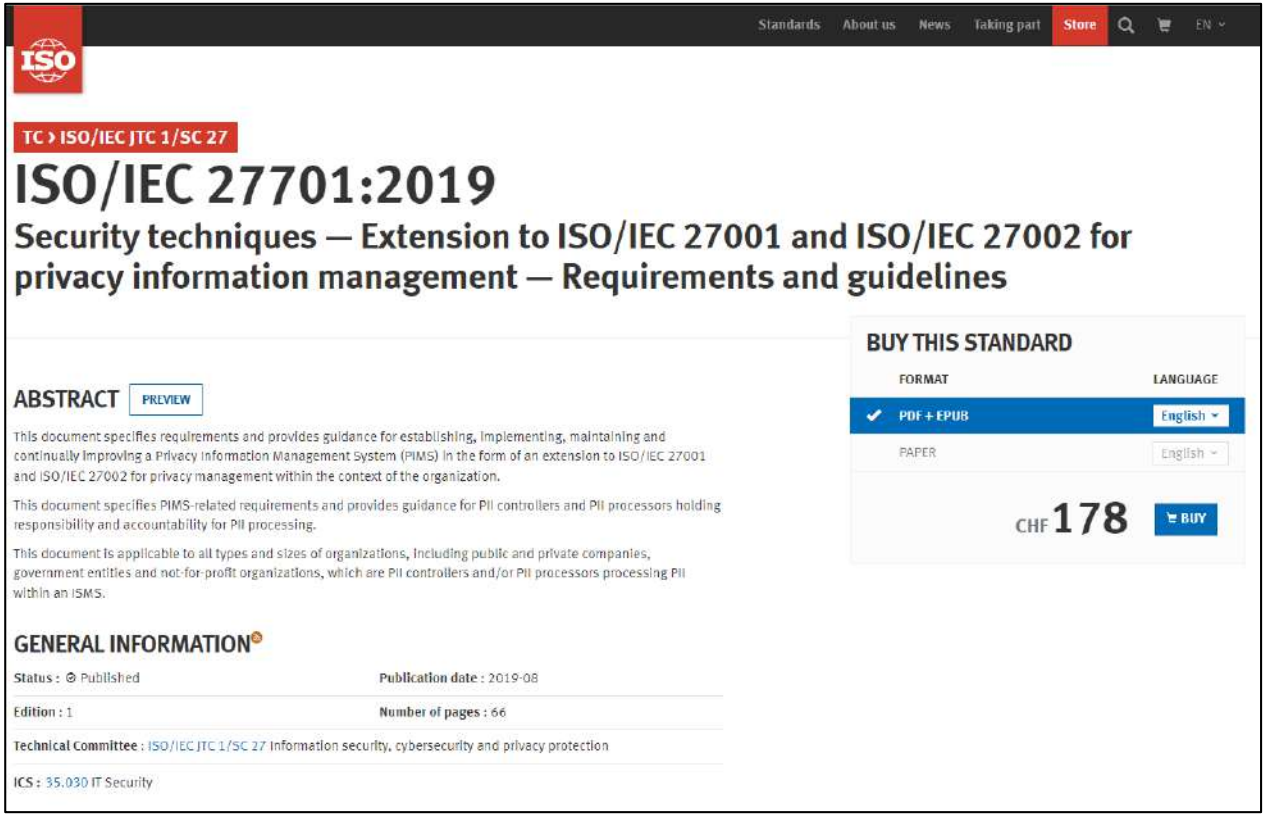


ISO 27001 Serie

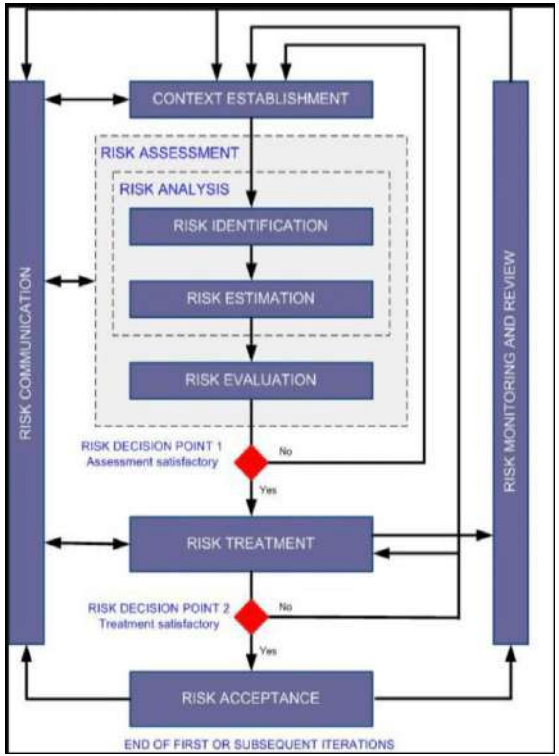
Controls – Best Practices



Privacy Information Management



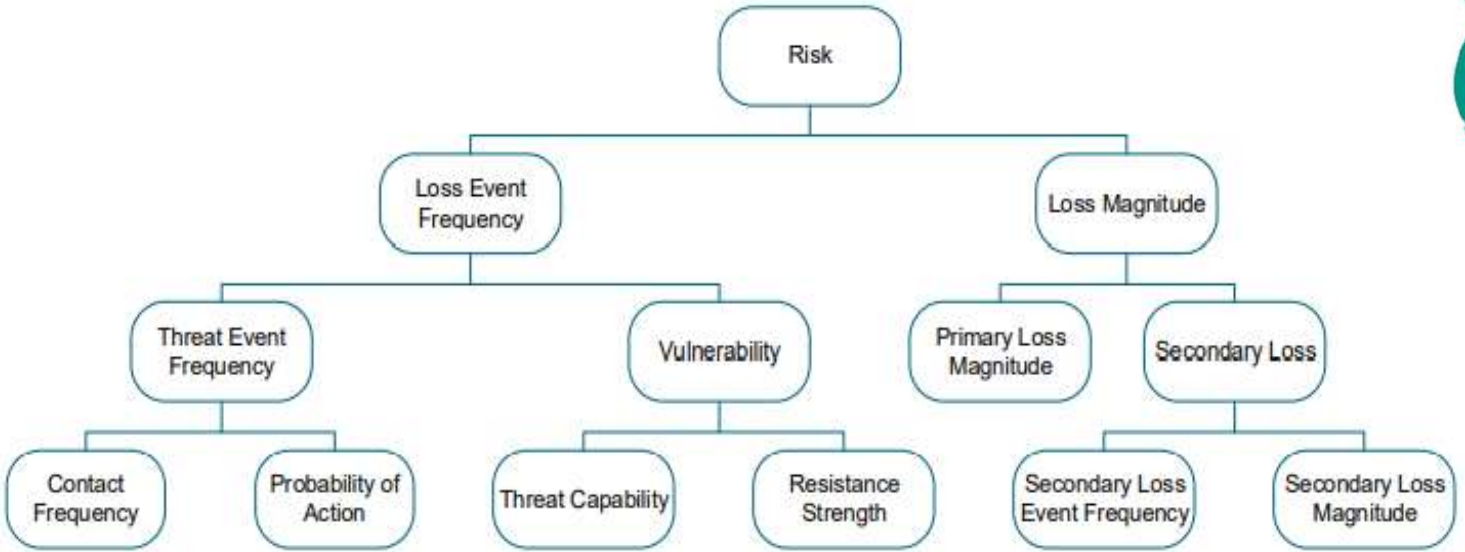
Information Security Risk Management



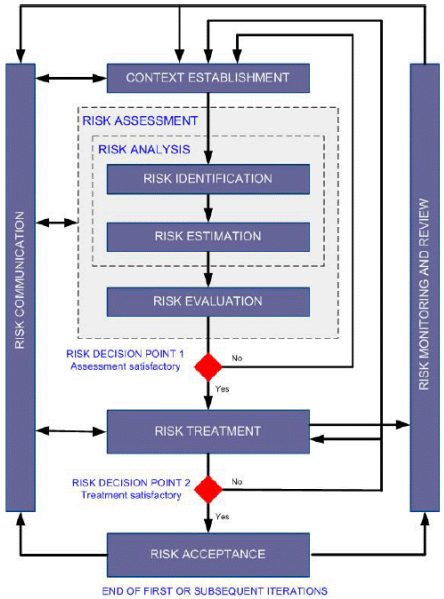
Quantitative Risk Management

Open FAIR™

Factor Analysis of Information Risk



Open FAIR™ – ISO/IEC 27005 Cookbook



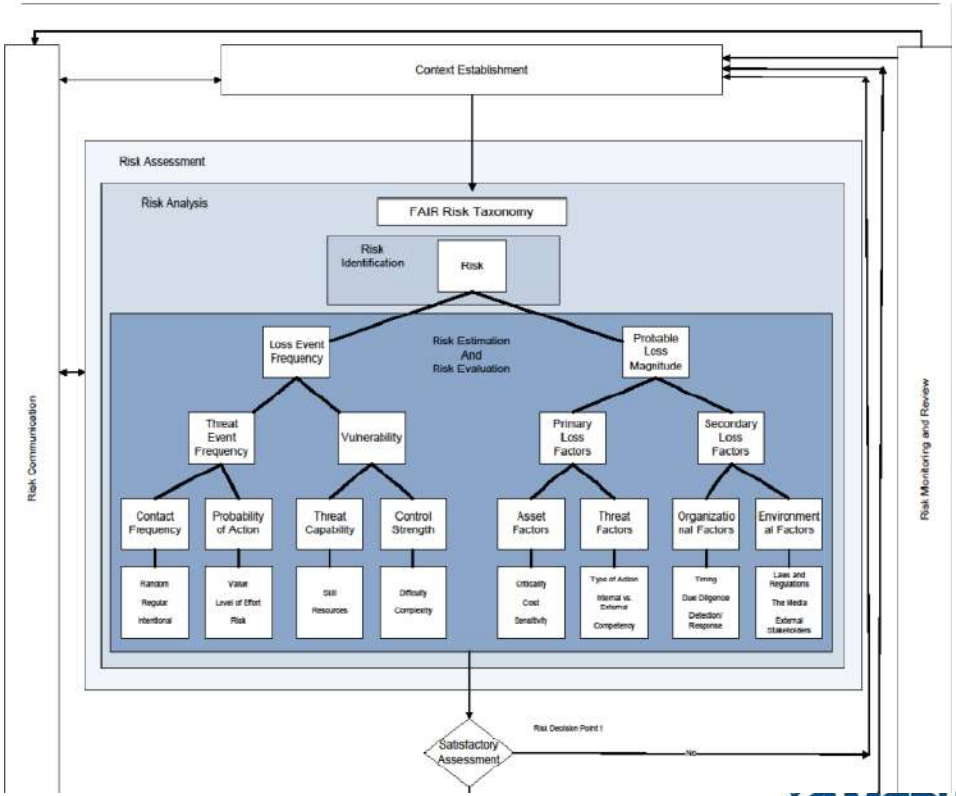
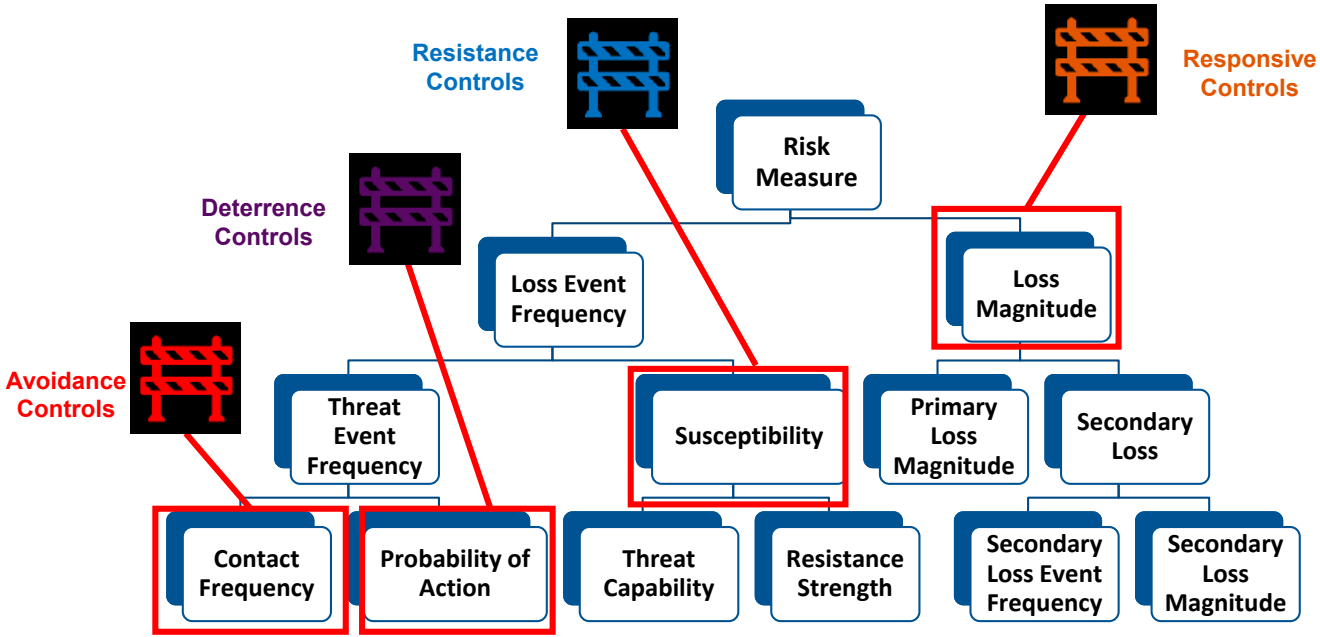
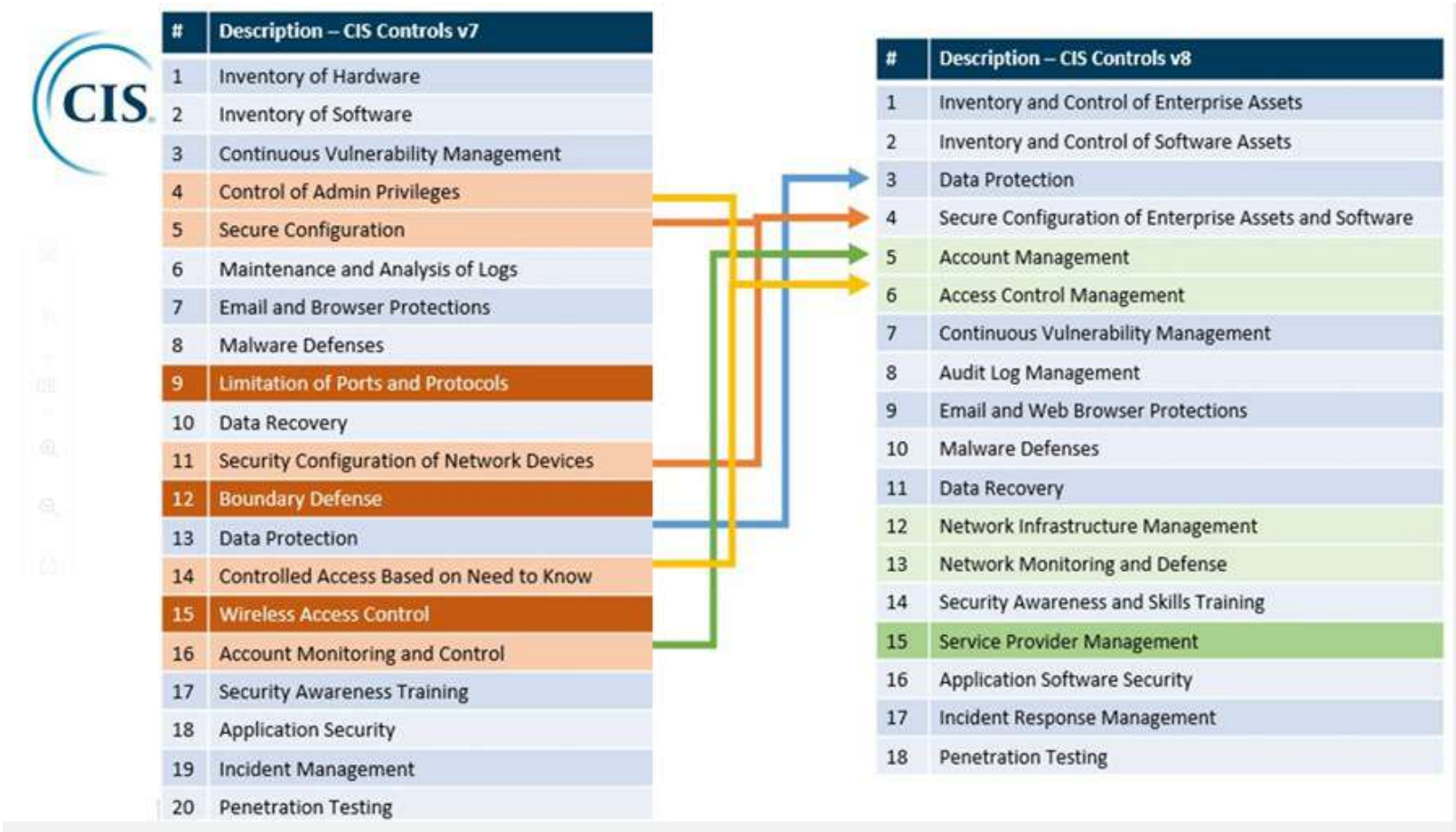


Figure 3: ISO/IEC 27005 – FAIR Integration Model

Risk Reduction with Treatment Options





#	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

18
Controls

153
Safeguards

CIS Controls

Top 18 Controls

MODULO

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

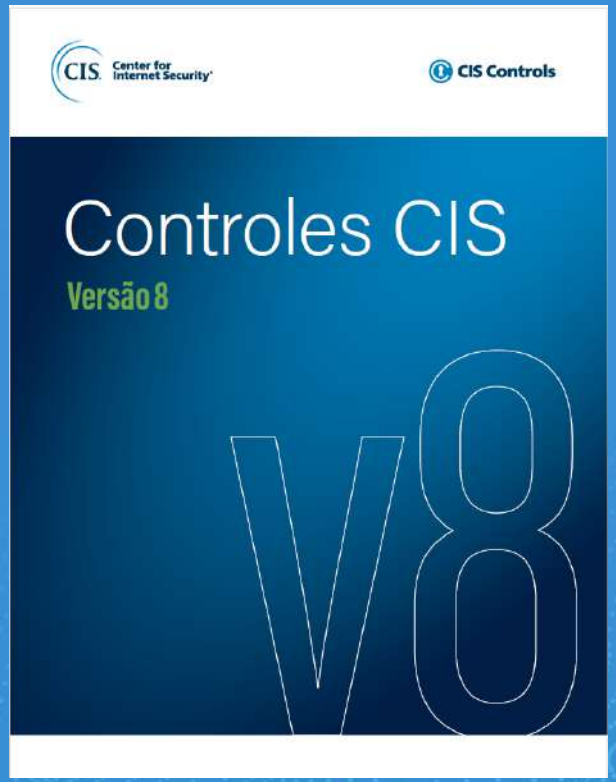
IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

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

CIS v8 in portuguese



Reconhecimento

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

MODULO

Privacy Law

LGPD

Accountability

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)
Insuffcient 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