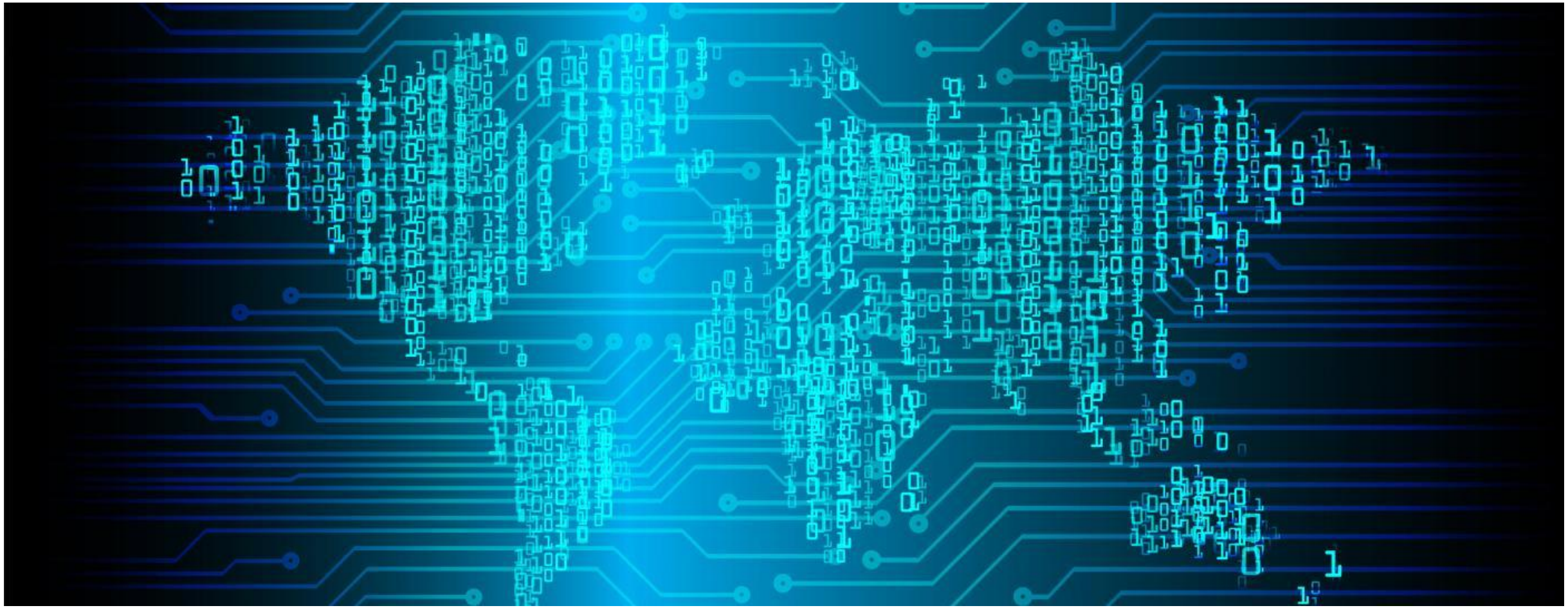


Ciber-resiliência e Governança

João Barbas
Joao.barbas@defesa.pt

Agenda

Enquadramento | Background

- Ciberespaço | Cyberspace
- Segurança da Informação | Information Security (InfoSec)
- Cibersegurança | Cybersecurity (CySec)
- Ciberdefesa | Cyber Defence

Ciber-resiliência | Cyber Resilience

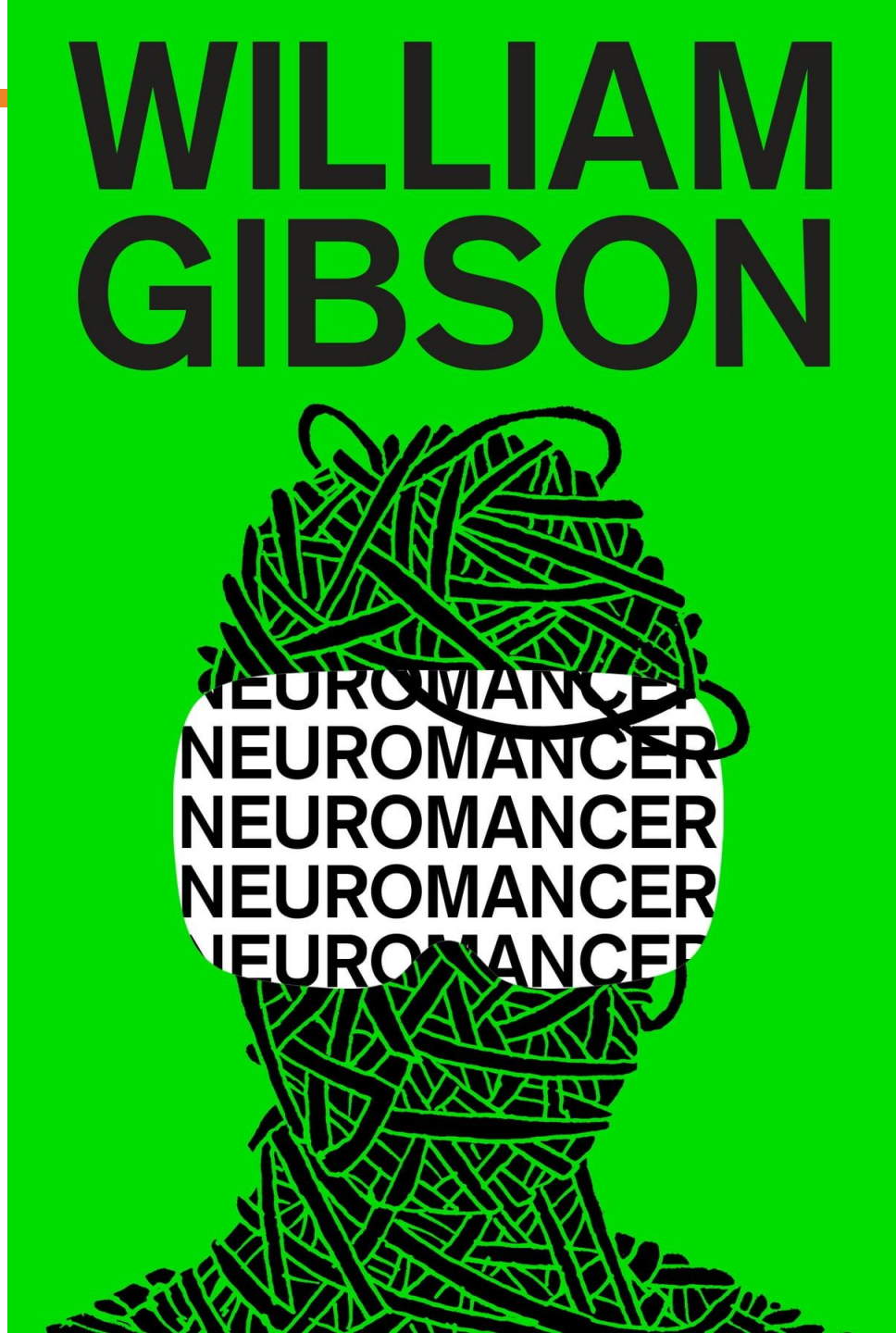
- O que é? | What is…?
- WEF Cyber Resilience Framework
- Princípios | Principles
- Gestão do Risco | InfoSec/CySec Risk Management

Governança | Governance | InfoSec/CySec

- O que é? | What is…?
- Tendências | Trends on…
- Eixos da Governança | Axes of Security Governance
- Sintomas de Ineficiência | Inefficient or inappropriate Governance
- Princípios | Principles

ENQUADRAMENTO

BACKGROUND

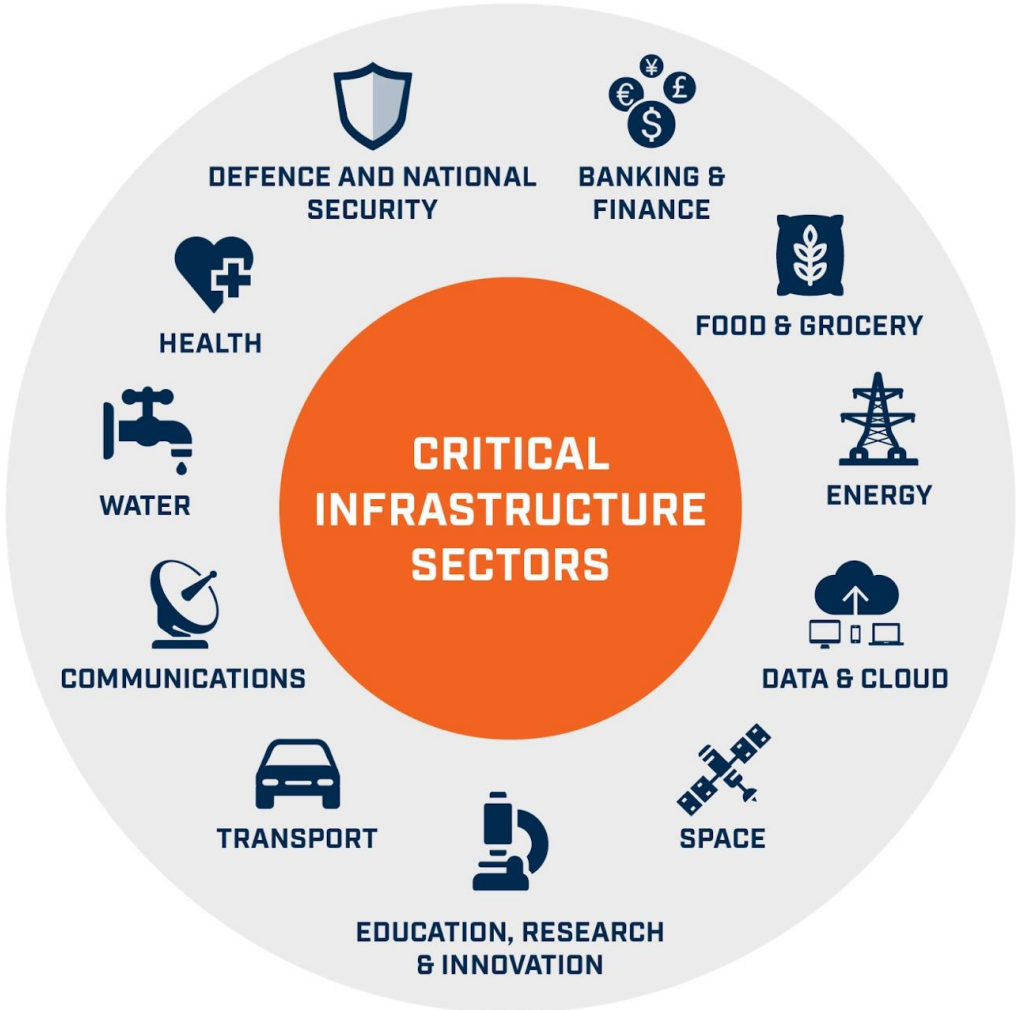

WILLIAM
GIBSON
NEUROMANCER
NEUROMANCER
NEUROMANCER
NEUROMANCER

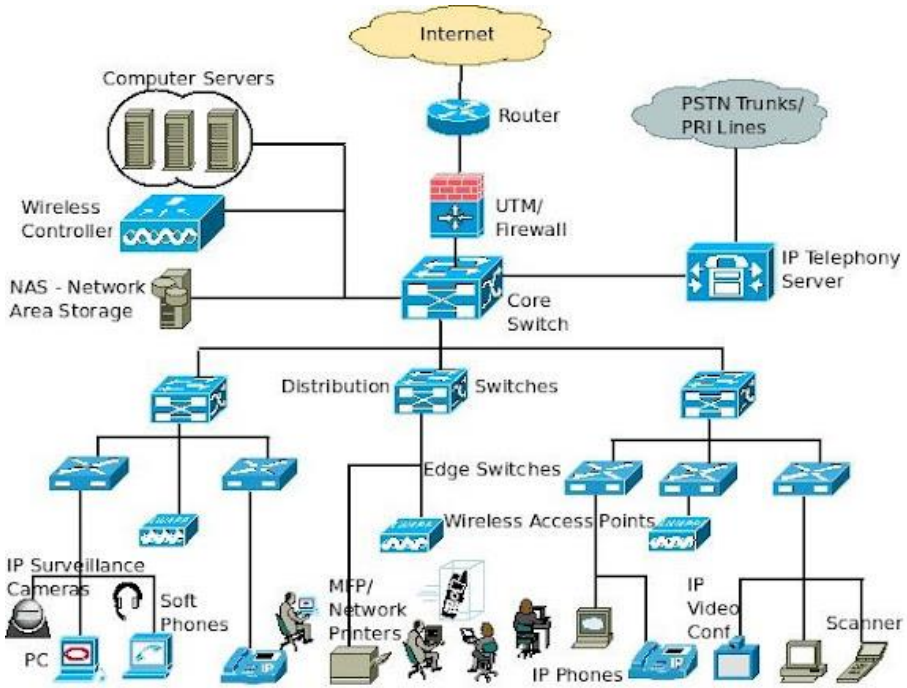
CIBERESPAÇO

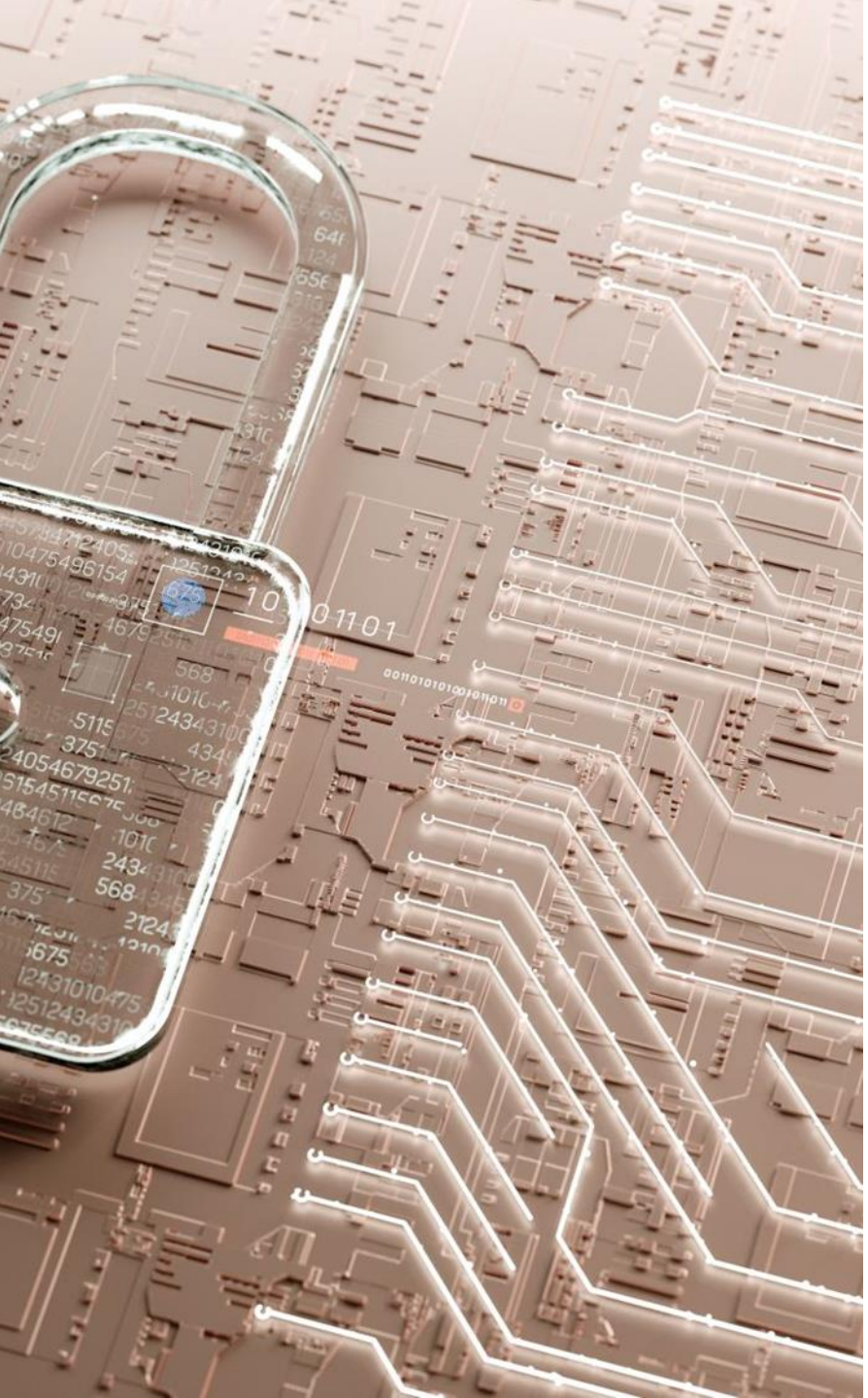
“ (…) A global domain within the information environment consisting of the **interdependent network of information technology infrastructures**, including **the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”**

“Um domínio global do ambiente de informação consistindo numa **rede interdependente de infraestruturas de Tecnologias de Informação**, incluindo a **Internet, redes de telecomunicações, computadores e processadores e controladores embebidos**.”

Joint Publication 1-02, DOD Dictionary of Military and Associated Terms


CRITICAL INFRASTRUCTURE SECTORS
DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
FOOD & GROCERY
ENERGY
DATA & CLOUD
SPACE
EDUCATION, RESEARCH & INNOVATION
TRANSPORT
COMMUNICATIONS
WATER
HEALTH


Internet
Computer Servers
Router
PSTN Trunks/ PRI Lines
Wireless Controller
UTM/ Firewall
NAS - Network Area Storage
Core Switch
IP Telephony Server
Distribution Switches
Edge Switches
Wireless Access Points
IP Surveillance Cameras
Soft Phones
PC
MFP/ Network Printers
IP Phones
IP Video Conf
Scanner



SEGURANÇA DA INFORMAÇÃO (InfoSec)

Proteção da Informação e dos Sistemas de Informação contra o acesso não autorizado, utilização, divulgação, disrupção, modificação ou destruição.

Andress, J. 2014. The basics of information security : understanding the fundamentals of InfoSec in theory and practice. Second edition. ed. Amsterdam ; Boston: Elsevier/Syngress

Preservação da confidencialidade, integridade e disponibilidade da informação; Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidas.

(ISO 27001: 2005)

“Segurança significa proteger nossos ativos. Isso pode significar protegê-los de invasores que invadem nossas redes, vírus / worms, desastres naturais, condições ambientais adversas, falhas de energia, roubo ou vandalismo ou outros estados indesejáveis. “

(Andress, 2014)

Cibersegurança (Cybersecurity) [CySec]

" (…) the collection of **tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies** that can be used to protect the cyber environment and **organization and user's assets**.* "

" (…) strives to ensure the **attainment and maintenance of the security properties** of the organization and user's assets* against relevant security risks in the cyber environment."

(International Telecommunication Union, 2016)

* connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

INFRESTRUTURAS CIS

DEFENSIVAS

ISR

OFENSIVAS

CIS &
INFOSEC

CIBERDEFESA

CIBER-RESILIÊNCIA

CYBER RESILIENCE

Ciber-resiliencia

Capacidade de **antecipar e adaptar-se, resistir ou recuperar rapidamente de um evento potencialmente perturbador**, seja ele natural ou causado pelo homem.

(ISO 15392:2019)

(...) a capacidade da organização para **resistir a impactos negativos devido a ameaças conhecidas, previsíveis, desconhecidas, imprevisíveis, incertas e inesperadas** de atividades no ciberespaço.

(Information Security Forum)

(…) é a capacidade de **antecipar, resistir, recuperar e adaptar-se a condições adversas, tensões, ataques ou comprometimentos** em sistemas que utilizam ou são possibilitados por recursos cibernéticos.

(NIST Special Publication 800-160, Volume 2)

(…) a capacidade dos sistemas e organizações de **resistir a eventos cibernéticos, medida pela combinação de tempo médio de falha e tempo médio de recuperação**.

(Symantec)

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Partnering for Cyber Resilience

Risk and Responsibility in a Hyperconnected World - Principles and Guidelines

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Agenda

Partnering for Cyber Resilience
Towards the Quantification of Cyber Threats

In collaboration with Deloitte

January 2015

Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions

Guidance on cyber resilience for financial market infrastructures

June 2016

BANK FOR INTERNATIONAL SETTLEMENTS

OICV-IOSCO

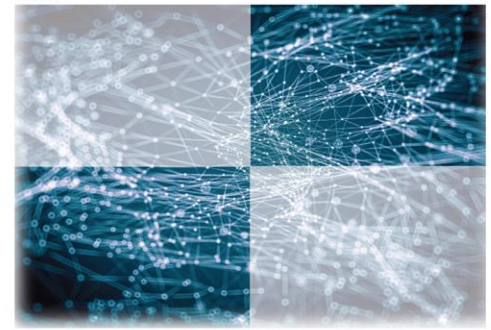
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Future of Digital Economy and Society System Initiative

Advancing Cyber Resilience
Principles and Tools for Boards

In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

January 2017



EUROPEAN CENTRAL BANK
EUROSYSTEM

Cyber resilience oversight expectations for financial market infrastructures

December 2018

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

Cyber Resilience for Financial Market Infrastructures

NOVEMBER 2019

In Collaboration with Kearney

WORLD ECONOMIC FORUM

The Resiliency Compass: Navigating Global Value Chain Disruption in an Age of Uncertainty

WHITE PAPER
JULY 2021

In collaboration with Accenture

WORLD ECONOMIC FORUM

The Cyber Resilience Index: Advancing Organizational Cyber Resilience

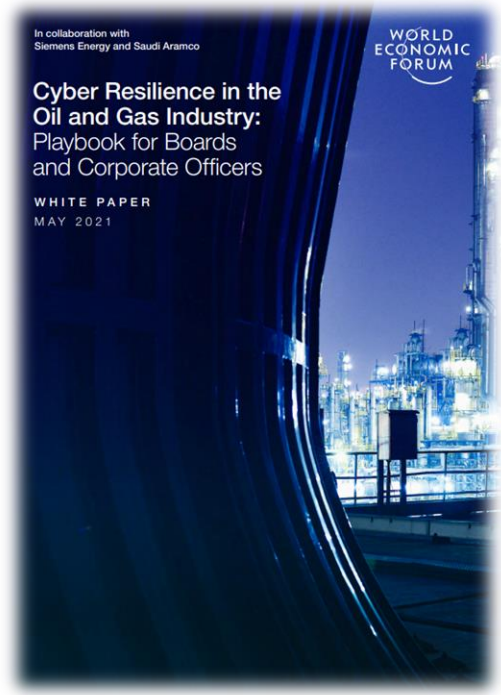
WHITE PAPER
JULY 2022

In collaboration with Siemens Energy and Saudi Aramco

WORLD ECONOMIC FORUM

Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers

WHITE PAPER
MAY 2021



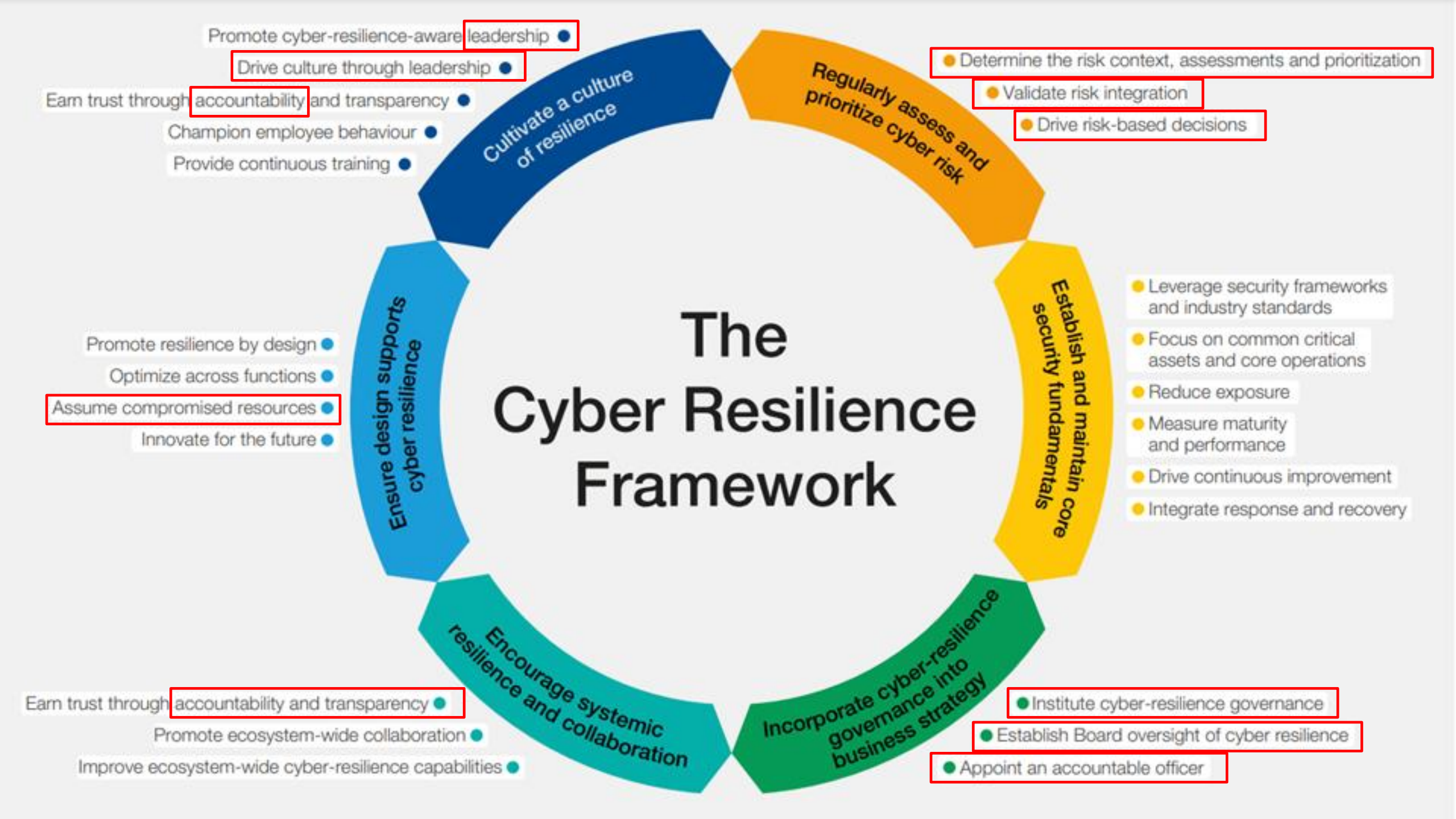
NACD
INTERNET SECURITY ALLIANCE

WORLD ECONOMIC FORUM

Principles for Board Governance of Cyber Risk

INSIGHT REPORT
MARCH 2021

In Collaboration with PwC


The Cyber Resilience Framework
Cultivate a culture of resilience
Promote cyber-resilience-aware leadership
Drive culture through leadership
Earn trust through accountability and transparency
Champion employee behaviour
Provide continuous training
Regularly assess and prioritize cyber risk
Determine the risk context, assessments and prioritization
Validate risk integration
Drive risk-based decisions
Establish and maintain core security fundamentals
Leverage security frameworks and industry standards
Focus on common critical assets and core operations
Reduce exposure
Measure maturity and performance
Drive continuous improvement
Integrate response and recovery
Incorporate cyber-resilience governance into business strategy
Institute cyber-resilience governance
Establish Board oversight of cyber resilience
Appoint an accountable officer
Encourage systemic resilience and collaboration
Earn trust through accountability and transparency
Promote ecosystem-wide collaboration
Improve ecosystem-wide cyber-resilience capabilities
Ensure design supports cyber resilience
Promote resilience by design
Optimize across functions
Assume compromised resources
Innovate for the future

PRINCÍPIOS PARA A CIBER-RESILIÊNCIA

Responsabilidade pela ciber-resiliência. O conselho de Administração, no seu conjunto, assume a **responsabilidade final pela supervisão do risco cibernético e da resiliência**. O conselho pode delegar a atividade de supervisão primária num comité, ex. comité de risco, segurança, etc.

Capacidade de Comando. Os membros do conselho **recebem orientação** [sobre resiliência cibernética] e **são regularmente atualizados sobre ameaças e tendências recentes** – com aconselhamento e assistência de peritos externos independentes disponíveis conforme solicitado.

Responsável [Diretor de Segurança, CSO, CISO, etc..]. O conselho garante que existe **um responsável corporativo é por reportar sobre a capacidade da organização para gerir a Ciber-resiliência e o progresso na implementação dos seus objetivos**. O conselho assegura que este responsável tem acesso regular ao conselho de administração, autoridade suficiente, comando, experiência e recursos para o desempenho destas funções.

Integração da resiliência cibernética. O conselho garante que **a gestão integra a Ciber-resiliência e a avaliação de riscos cibernéticos na estratégia global de negócio** e na **gestão de riscos a nível empresarial, bem como na orçamentação e alocação de recursos.**

Apetite pelo risco. O conselho **define e quantifica anualmente a tolerância ao risco empresarial em relação à resiliência cibernética**_e garante que isso é **consistente com a estratégia corporativa e o apetite pelo risco. O conselho é aconselhado sobre a exposição ao risco atual e futuro, bem como os requisitos regulamentares e referências da indústria/sociedade para o apetite de risco**

PRINCIPIOS PARA A CIBER-RESILIÊNCIA (II)

Avaliação de risco e reporte. O conselho de administração assegura a responsabilização da administração pela avaliação do reporting dos riscos cibernéticos, ameaças e eventos na agenda permanente da reuniões do conselho de administração. E valida estas avaliações com a sua própria avaliação estratégica de risco.

Planos de resiliência. O conselho garante que a administração apoia o responsável pela resiliência cibernética / CISO através da criação, implementação, teste e melhoria contínua dos planos de resiliência cibernética, que são adequadamente harmonizados em todo o negócio. Requer que o oficial encarregado monitorize o desempenho e apresente-se regularmente ao conselho.

A comunidade. O conselho incentiva a administração a colaborar com outras partes interessadas, conforme relevante e apropriado, de forma a garantir a resiliência cibernética sistémica.

Revisão. O conselho garante que uma revisão formal e independente da resiliência cibernética da organização é realizada anualmente.

Eficácia. O conselho revê periodicamente o seu próprio desempenho na implementação destes princípios ou procura aconselhamento independente para melhoria contínua.

AVALIAÇÃO E GESTÃO DO RISCO

É um **exercício sistematizado,** no âmbito do qual a organização identifica possíveis **ameaças** que possam construir sobre as **vulnerabilidades dos ativos**, bem como quais os **níveis do risco associado**, avaliando-se a **probabilidade de ocorrência** e **possíveis impactos**.

A gestão do risco, quando efetuada de **forma sistematizada** e numa lógica de melhoria, é uma prática que permite às organizações **identificar, quantificar e estabelecer as prioridades** face a **critérios de aceitação do risco e objetivos relevantes** para a organização.

A gestão do risco de uma organização pode ser entendida como a **gestão da incerteza e determinação das ações necessárias, para que esta possa ser minimizada para níveis considerados aceitáveis por parte da organização.**

CNCS. 2019. Quadro Nacional de Referência para a Cibersegurança. [Online]. Disponível em: https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf [Acedido em: 28/1/2021]

QUADRO REFERÊNCIA PARA A AVALIAÇÃO E GESTÃO DO RISCO

Tolerância/apetite ao risco da organização no contexto dos riscos cibernéticos e da estratégia de negócio da organização

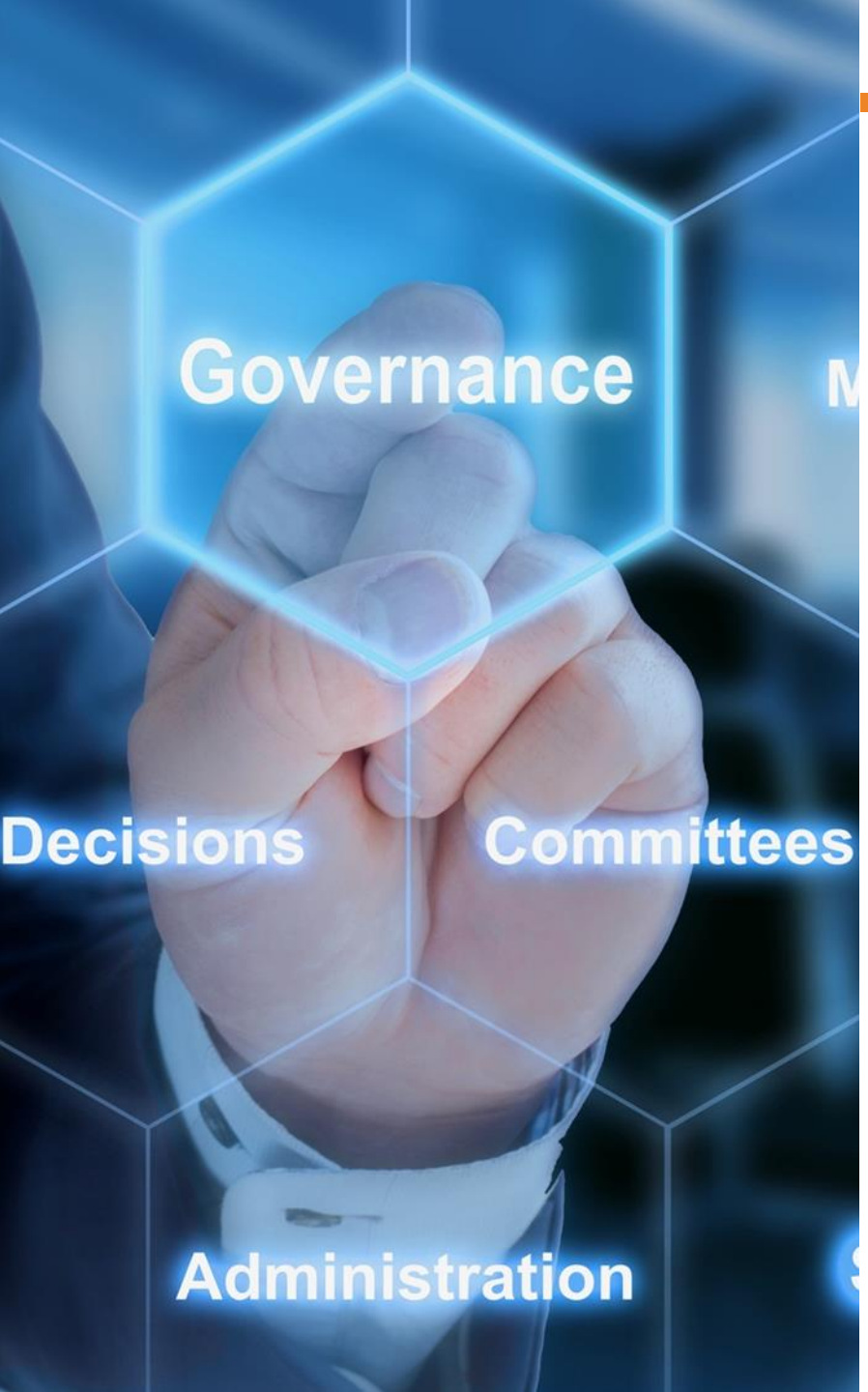
Riscos cibernéticos que a organização enfrenta – não tendo em conta quaisquer ações de gestão ou mitigação de riscos neste momento

Ações de gestão ou mitigação de riscos sugeridas pela equipa executiva e custos associados

A **carteira residual de riscos cibernéticos** após ações de gestão ou mitigação de risco e como se compara com a tolerância/apetite pelo risco

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) 2018. ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management.


Rules
Governance
Mission
Ethics
Decisions
Committees
Administration
Staff



"(…) Information Security Governance is the process of directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions), treating adequate security as a non-negotiable requirement of being in business.

"(…) A Governança de Segurança da Informação é o processo de direcionar e controlar uma organização para estabelecer e sustentar uma cultura de segurança na conduta da organização (crenças, comportamentos, capacidades e ações), tratando a segurança adequada como um requisito inegociável do negócio.

"Governing for Enterprise Security (GES) Implementation Guide", Jody R. Westby, Julia H. Allen, SEI Carnegie Mellon University 2007

TENDÊNCIAS ATUAIS…

Falta de **consciência da estratégia da InfoSec/CySec** e do seu **grau de alinhamento com as estratégias empresariais**.

Ignorância dos problemas e preocupações da InfoSec pelo executivos superiores.

Falta de um processo formal de avaliação para o desempenho da InfoSec/CySec ou do **retorno dos investimentos (ROI)** em segurança.

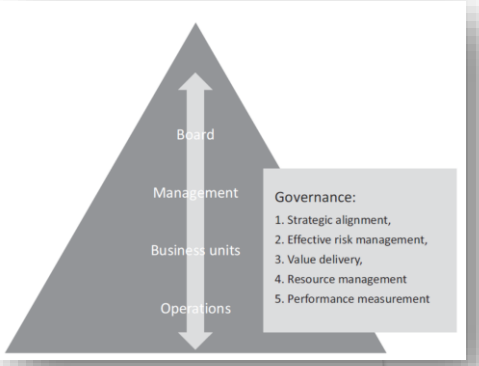
Prioridade para **soluções técnicas sem ajustar estruturas organizacionais**.

Falta de envolvimento da gestão na priorização dos tratamentos de risco.

Falta de requisitos no desenho de arquitetura de segurança da InfoSec .

Fonte: Volchkov, Andrej - Information Security Governance: Framework and Toolset for CISOs and Decision Makers. Auerbach Publications, 2018. ISBN: 042943653X

GOVERNANÇA DEVE CONTRIBUIR PARA…



Alinhamento estratégico da segurança da informação com estratégia empresarial para apoiar objetivos organizacionais.

Uma **gestão eficaz dos riscos**, executando medidas adequadas para gerir e mitigar riscos e reduzir os impactos potenciais nos recursos de informação para um nível aceitável.

Entrega de valor, otimizando investimentos de segurança da informação em apoio a objetivos organizacionais.

Gestão dos recursos, utilizando conhecimentos de segurança da informação e infraestruturas de forma eficiente e eficaz.

Avaliação de desempenho, através da medição, monitorização e reporte de métricas da segurança da informação para garantir a realização de objetivos organizacionais.

Information Security Institute, Guidance for Information Security Managers, ITGI 2008

SINTOMAS DE GOVERNANÇA DESADEQUADA…

A responsabilidade pela implementação de **medidas ou controlos da InfoSec concentra-se num único departamento**.

Os gestores de intermédios consideram a **InfoSec responsabilidade exclusiva do Diretor de segurança da informação [CISO ou CIO],** cabendo-lhes assegurar o nível de proteção adequado.

O conselho de administração não se envolve em decisões estratégicas da InfoSec e delega essa responsabilidade, considerando-se não qualificada para dar parecer.

O responsável pela da InfoSec [CISO/CIO] não dispõe de meios para assegurar a adequação e aplicação de políticas e diretivas de segurança.

As **iniciativas e projetos empresariais não são avaliados préviamente para garantir o seu alinhamento com a estratégia de segurança ou permitir identificar riscos de segurança.**

O **conselho de administração não tem relatórios sobre a InfoSec** , a sua adequação e a eficácia das medidas em vigor. Não pode avaliar o valor acrescentado da segurança para o negócio.

Os responsáveis de segurança sentem que não são ouvidos nem apoiados pelos seus superiores. As suas prerrogativas são reduzidas a ações para **combater novas ameaças ou restaurar a situação após incidentes repetidos**.

Fonte: Volchkov, Andrej - Information Security Governance: Framework and Toolset for CISOs and Decision Makers. Auerbach Publications, 2018. ISBN: 042943653X

BOA GOVERNANÇA …

Toda a empresa está envolvida:

- Os ativos a proteger são conhecidos e o nível de segurança é definido.
- InfoSec/CySec é considerado indispensável pelas unidades de negócio.
- Medidas de segurança apoiam operações empresariais.

As responsabilidades são definidas:

- O conselho e a administração estão envolvidos no processo de tomada de decisão do programa de segurança.
- Os gestores de unidades de negócio validam medidas de segurança que apoiam as suas operações, projetos e estratégia de desenvolvimento.
- Os proprietários de dados e processos são identificados e em funcionamento.
- Os especialistas de InfoSec/CySec implementam o programa de acordo com estratégias e políticas definidas.

O nível de proteção depende do apetite pelo risco:

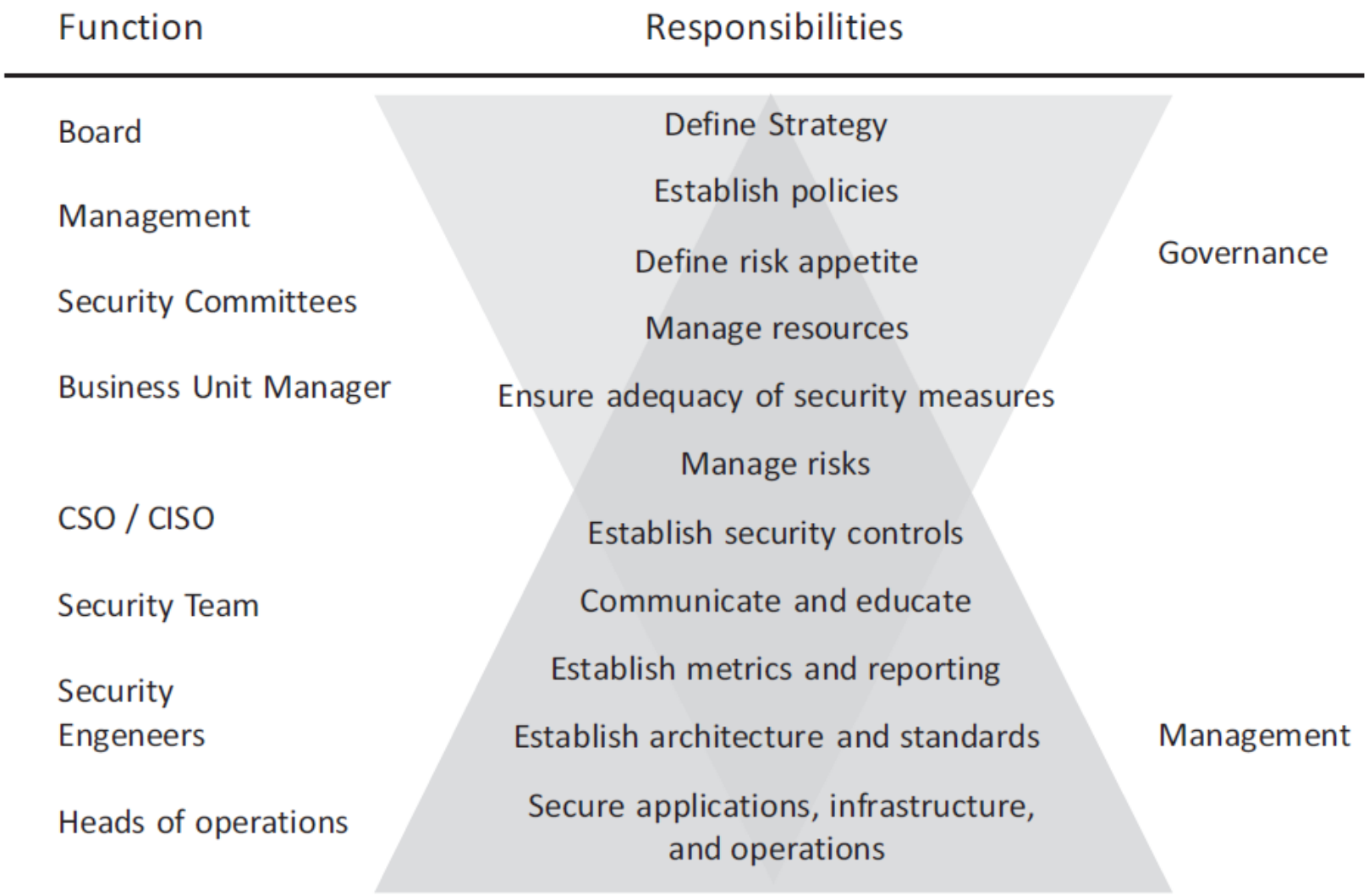
- Os riscos de InfoSec/CySec são avaliados e tratados sistematicamente.
- O apetite pelo risco é definido, e a gestão proativa do risco está em vigor no que diz respeito a todas as atividades da empresa, tanto operações como projetos de mudança.
- Os controlos de InfoSec/CySec são geridos e associados a riscos.

A segurança é gerida ativamente:

- Estratégia de segurança, políticas e diretrizes são estabelecidas para atender às necessidades da organização.
- Os ativos a proteger são identificados e definidas responsabilidades.
- A gestão aloca recursos adequados de acordo com um processo de avaliação e tomada de decisão repetitivo.
- As responsabilidades são definidas a todos os níveis.
- O sistema de reporte apoia o processo de tomada de decisão e baseia-se em indicadores-chave. Um sistema de gestão de incidentes está em vigor.
- Os colaboradores são treinados e conscientes do risco.
- O programa de segurança é supervisionado, auditado e ajustado às necessidades da empresa

Fonte: Volchkov, Andrej - Information Security Governance: Framework and Toolset for CISOs and Decision Makers. Auerbach Publications, 2018. ISBN: 042943653X

RESPONSIBILIDADES DE GOVERNANÇA E GESTÃO



Fonte: Volchkov, Andrej - Information Security Governance: Framework and Toolset for CISOs and Decision Makers. Auerbach Publications, 2018. ISBN: 042943653X

PRINCIPIOS

Estabelecer a **segurança da informação (InfoSec/CySec) em toda a organização**

Adotar uma **abordagem baseada no risco**

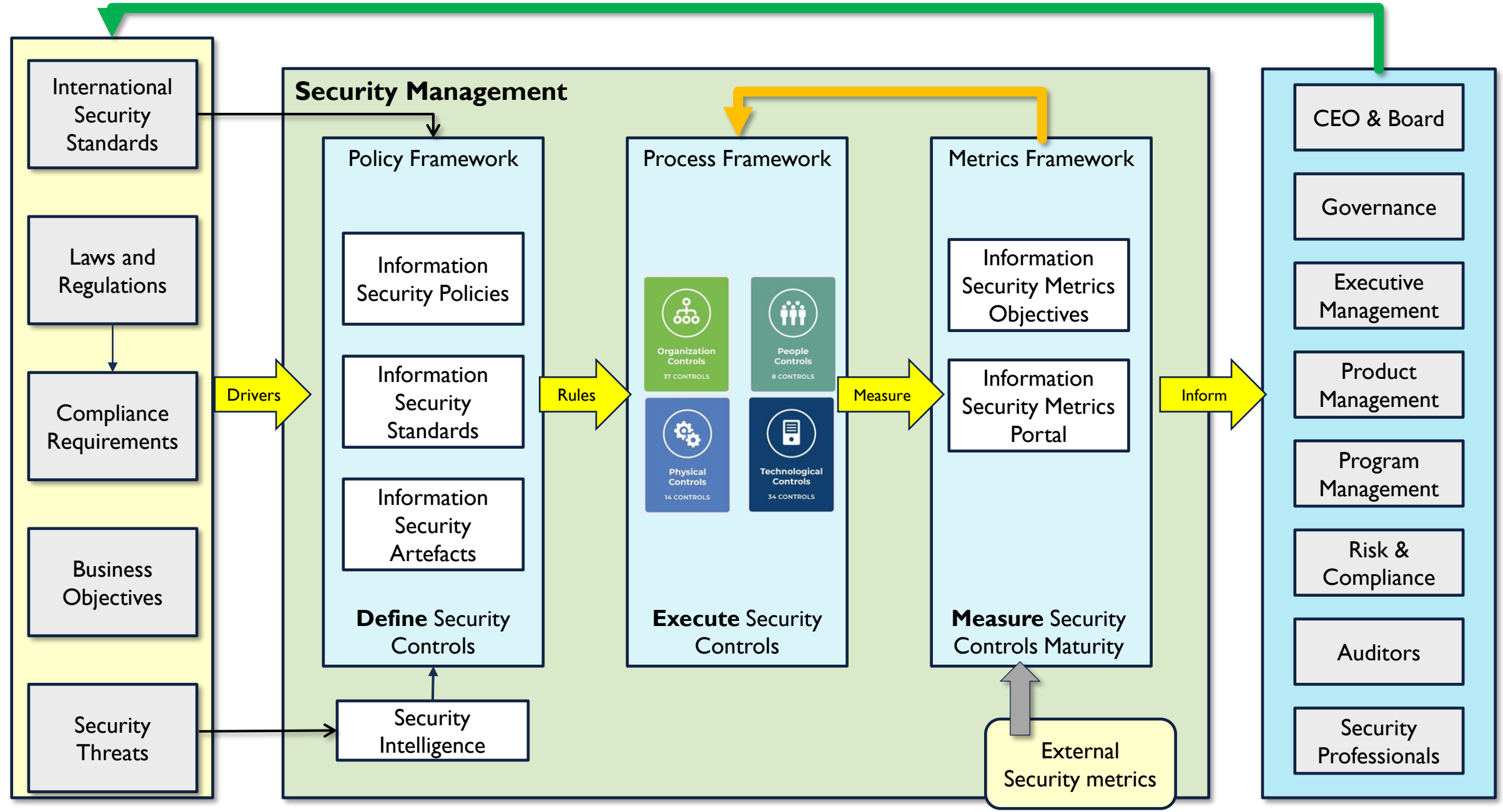
Definir a direção das decisões de investimento

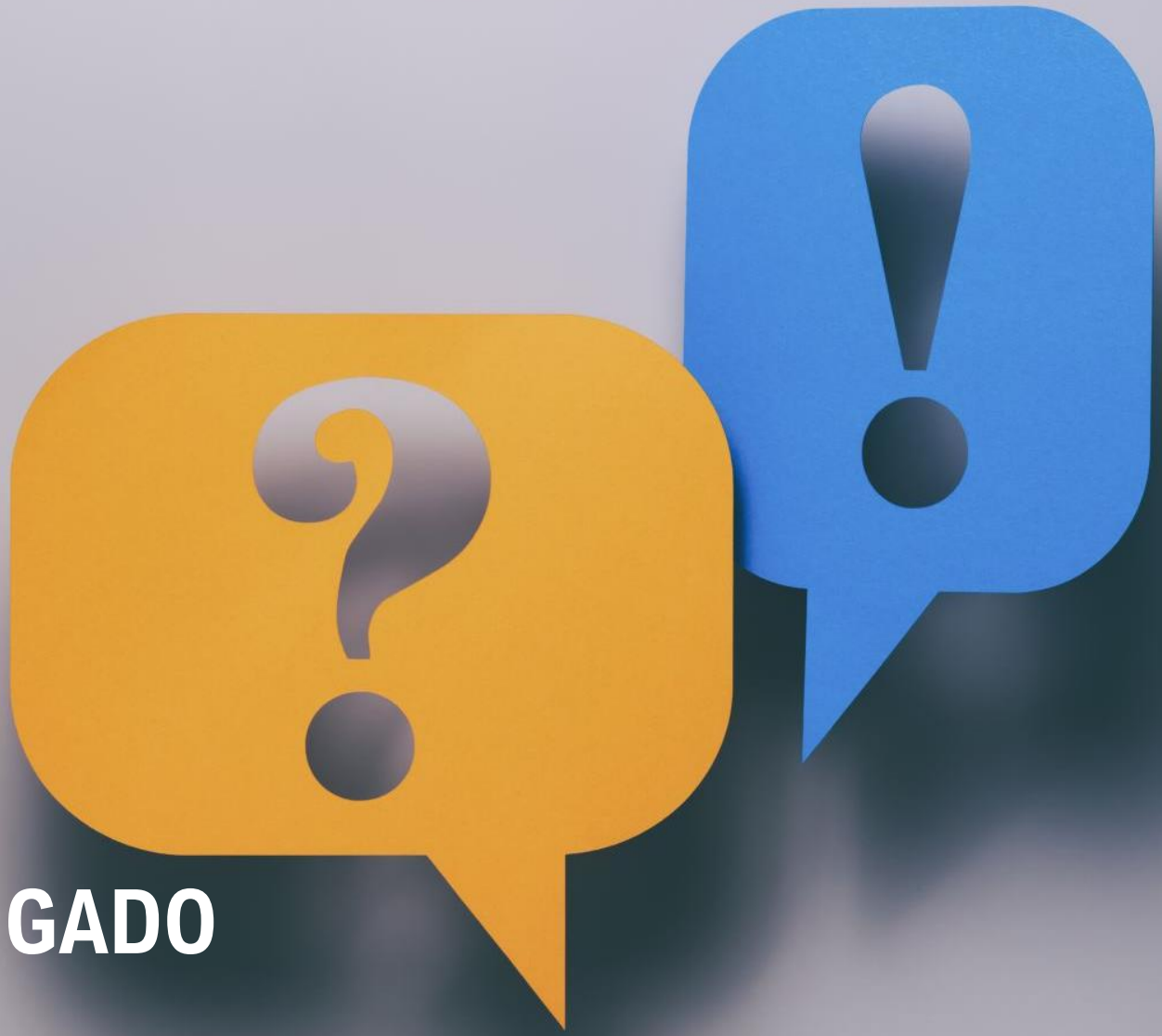
Garantir a conformidade com os requisitos internos e externos

Promover um **ambiente positivo para a segurança**

Analisar o desempenho em relação aos resultados do negócio

ISO - Information technology — Security techniques — Governance of information security. 2013. ISBN/ISSN:


International Security Standards
Laws and Regulations
Compliance Requirements
Business Objectives
Security Threats
Drivers
Security Management
Policy Framework
Information Security Policies
Information Security Standards
Information Security Artefacts
Define Security Controls
Security Intelligence
Rules
Process Framework
Organization Controls
37 CONTROLS
People Controls
8 CONTROLS
Physical Controls
14 CONTROLS
Technological Controls
34 CONTROLS
Execute Security Controls
Measure
Metrics Framework
Information Security Metrics Objectives
Information Security Metrics Portal
Measure Security Controls Maturity
External Security metrics
Inform
CEO & Board
Governance
Executive Management
Product Management
Program Management
Risk & Compliance
Auditors
Security Professionals



MUITO OBRIGADO