A day in the life of a CISO

What does a CISO do anyway, and why do I need one?

Prepared by:
Ian Bowell

September 2024

Ian Bowell

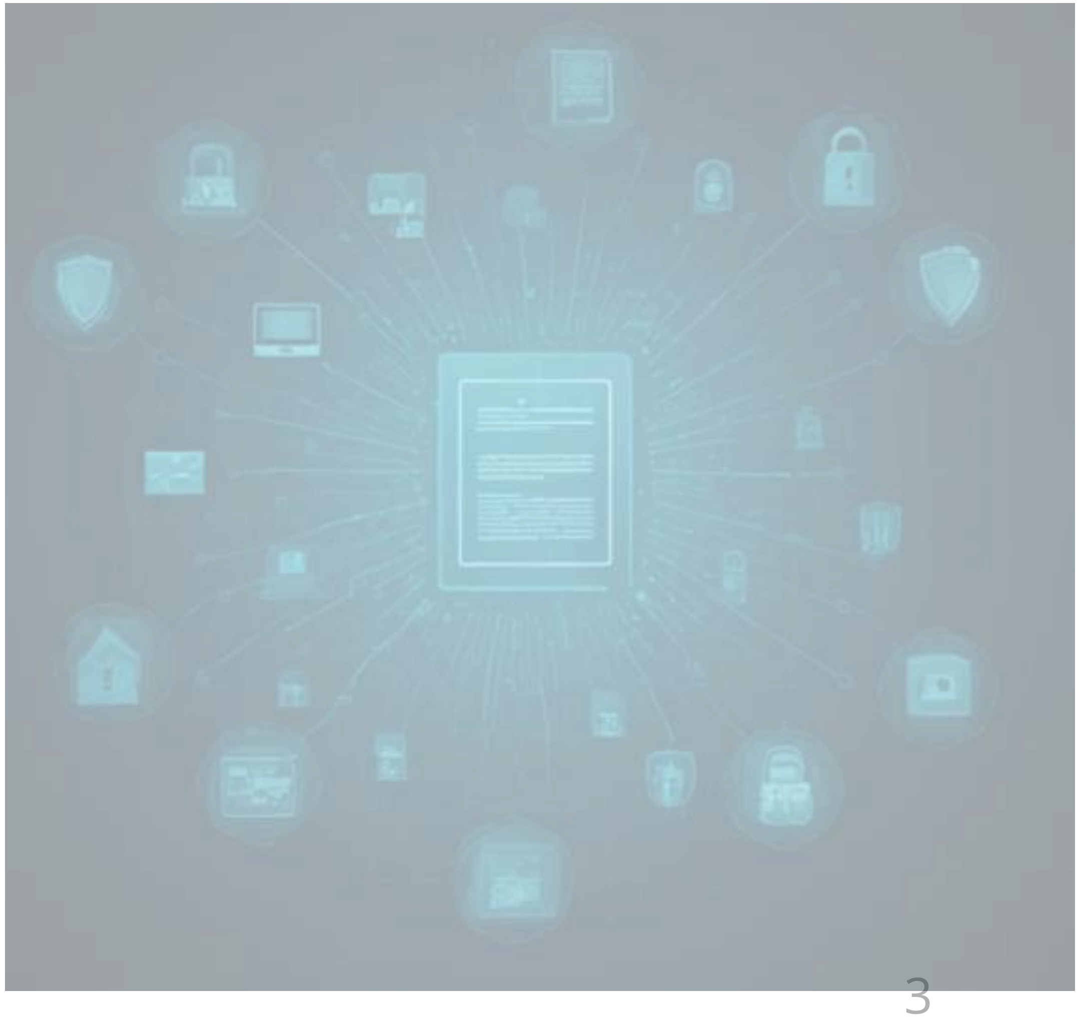
Thrive Advisory Services – CISSP certified vCISO

- ibowell@thrivenextgen.com
- https://www.linkedin.com/in/ibowell/

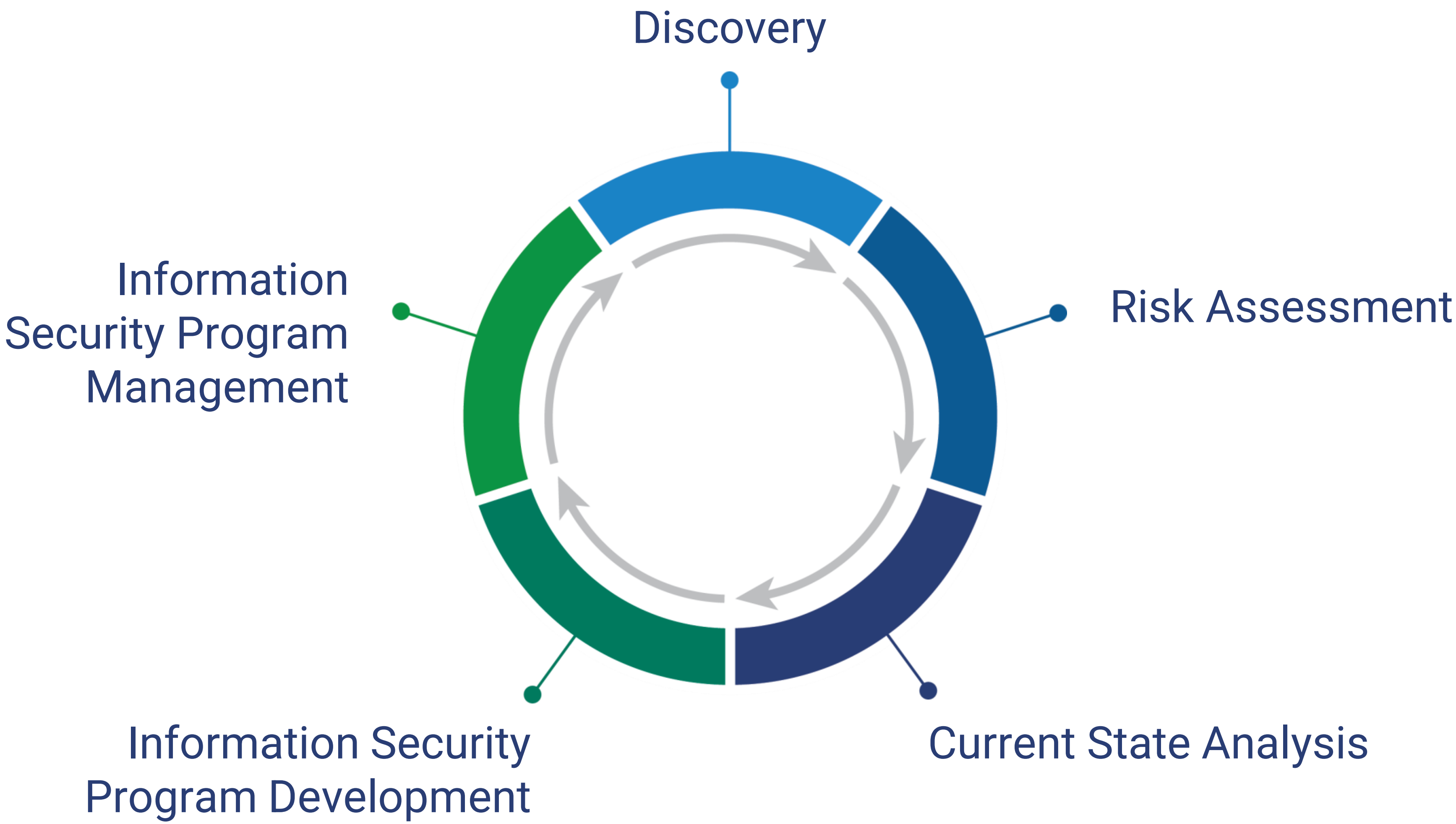
- Decades in IT leadership as VP, CTO, COO and CISO.
- Global Investment Banking, AM/HFs/FoF/PE
- Also, Microsoft and Digital Legal
- Business Oriented Secure Software, Infrastructure, Networks and more…
- London, Boston, New York, Global, Ireland, London
- BSc. CS, MBA, Dip DevOps, CISSP, PhD ?.

Agenda

- What does a CISO do ?
- Why use a Virtual CISO ?
- Current challenges
  - Detection…
    - is it working (on the latest thing)?
  - DORA, Operational Resilience,
    - FCA, other regulators
  - AI, DLP, Data classification
  - Protect and … what then?
- CIS Framework and more



CISO Process


Discovery
Risk Assessment
Current State Analysis
Information Security Program Development
Information Security Program Management

vCISO Foundation

Thrive's vCISO Offering is built around two foundational concepts:

CIS Center for Internet Security®

CISM® Certified Information Security Manager®
An ISACA® Certification

CISSP® Certified Information Systems Security Professional

1

Center for Internet Security (CIS) Framework

- "CIS Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements."

2

ISC2 Certified Information Systems Security Professional (CISSP) domains

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Center for Internet Security (CIS) Top 18 Controls (with safeguard RAG)

01 Inventory & Control of Enterprise Assets

02 Inventory & Control of Software Assets

03 Data Protection

04 Secure Configuration of Enterprise Assets & Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email & Web Browser Protections

10 Malware Defenses

11 Data Recovery

12 Network Infrastructure Management

13 Network Monitoring & Defense

14 Security Awareness & Skills Training

15 Service Provider Management

16 Applications Software Security

17 Incident Response Management

18 Penetration Testing

CISO role – first steps

- What are your organization’s most critical assets?

- What role does anyone play in safeguarding those **assets**?

- How do you develop the strategic policies and processes, and tactical details, needed to protect vital systems and secure sensitive data **and financial transactions** ?

- How can you effectively **balance** technical expertise with a business-focused approach to security planning, compliance, and risk management?

CISO role – LMF

- In a typical organisation, be it your own or your client’s, WHO would or should be responsible be setting the business’s security policy, standards and operating protocol?
- Is there an optimal model or will it differ depending on the type of company?
- Is there any correlation between involvement/responsibility and the increased likelihood of security breaches/incidents?
- What process should be in place to ensure these policies remain resilient?
- What are the key challenges for CISO’s/Risk Officers in a modern day organisation, when it comes to cyber resilience?

Think people, processes, regulation etc.

CISO role and others

- In your organization, who processes any and all security activity?

- How does your **reporting structure influence** the overall security strategy, if it’s all Software or HR, and not physical, or not by design?

- What challenges do organizations face when they lack internal IT knowledge, before they even get to security?

- How can a CISO help bridge that gap?

CISO in your organisation

- How do you drive and oversee cybersecurity initiatives to get people onboard?

- What steps have you taken to implement a robust Cybersecurity Framework in your organization?

- What disaster recovery process have you developed?

- How have you ensured effective business continuity plans are in place now that everyone **works from home** or are coming **back to the office**?

CISO in a changing world

- How do you approach secure data management strategies, for people, before AI?
- What **meaningful** data classification is in place to protect sensitive information?
- What measures do you take to supervise and ensure safe practices for user access and permissions within your organization?
- Are you confident that your organization is meeting all necessary compliance regulations?
- How do you ensure continuous alignment?

CISO and the unexpected

- How do you develop and maintain effective communication with users to minimize security vulnerabilities and promote awareness?

- When dealing with unexpected "curve balls," what situations have left you feeling uncomfortable?
- How did you address them?
- Do you know what worked elsewhere?
- Can you successfully navigate complex regulations like DORA or NIS2?
- What strategies do you use to simplify compliance without unnecessary effort?

The top five threats we are facing today.

01

- Phishing Attacks
- BEC
- Funds Transfer

02

- Attack Surface

03

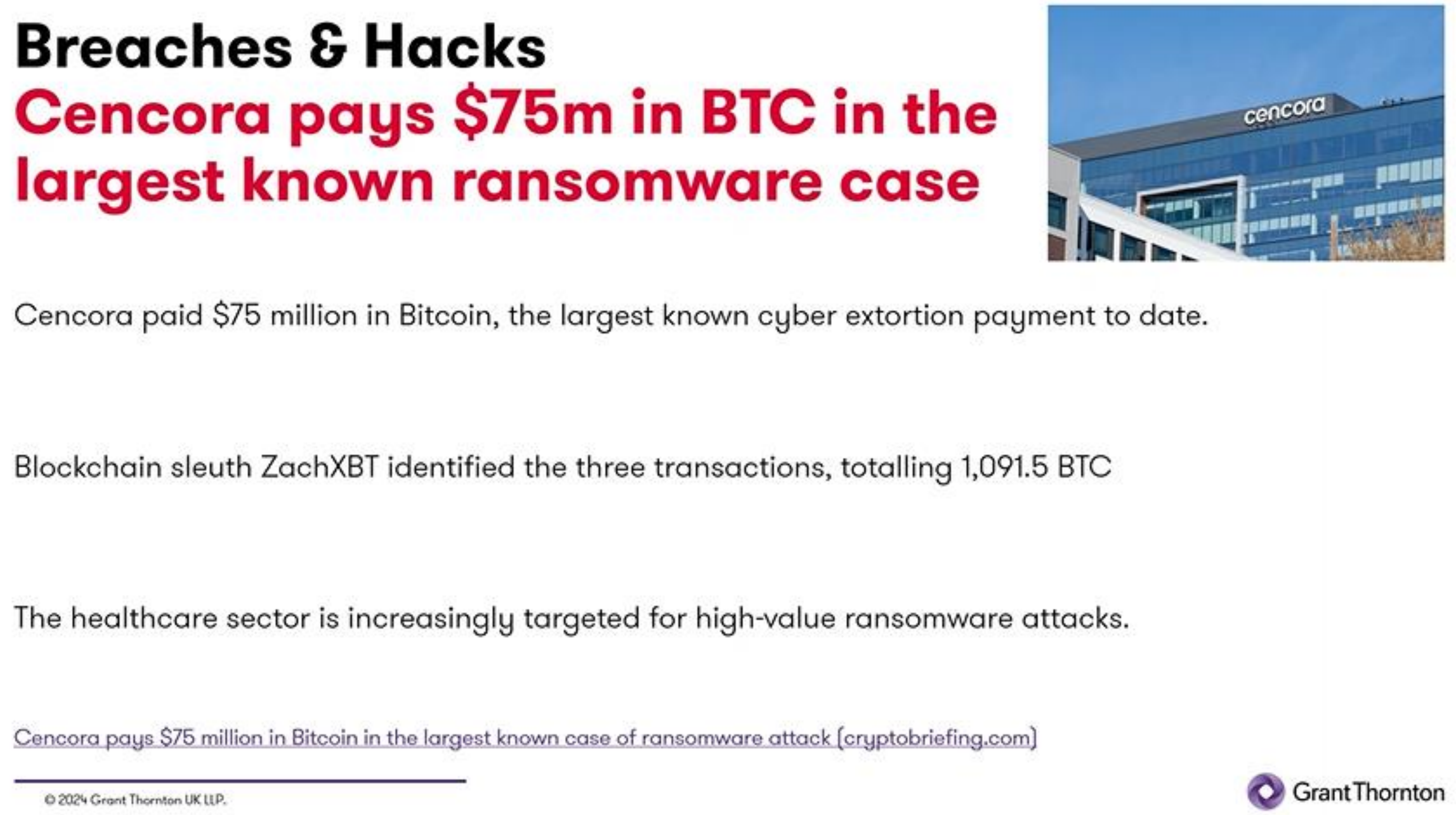
- Ransomware

04

- Insider Threats
- Leavers
- Confidential Info

05

Artificial Intelligence Exploits/Deep Fakes



Breaches & Hacks

Cencora pays $75m in BTC in the largest known ransomware case

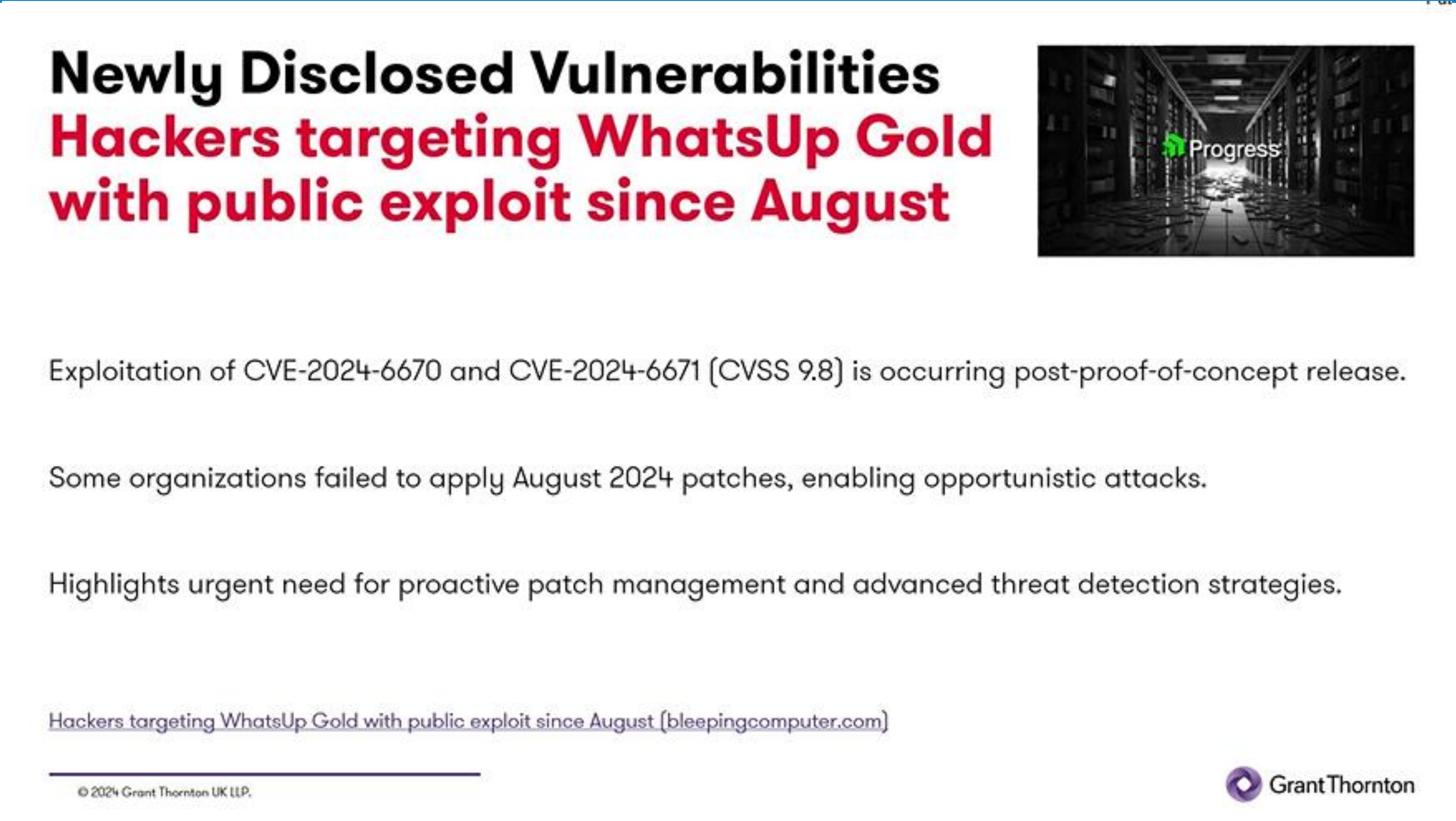
Cencora paid $75 million in Bitcoin, the largest known cyber extortion payment to date.

Blockchain sleuth ZachXBT identified the three transactions, totalling 1,091.5 BTC

The healthcare sector is increasingly targeted for high-value ransomware attacks.

Cencora pays $75 million in Bitcoin in the largest known case of ransomware attack (cryptobriefing.com)

GrantThornton



Newly Disclosed Vulnerabilities
Hackers targeting WhatsUp Gold with public exploit since August

Exploitation of CVE-2024-6670 and CVE-2024-6671 (CVSS 9.8) is occurring post-proof-of-concept release.

Some organizations failed to apply August 2024 patches, enabling opportunistic attacks.

Highlights urgent need for proactive patch management and advanced threat detection strategies.

Hackers targeting WhatsUp Gold with public exploit since August (bleepingcomputer.com)

Grant Thornton

Newly Disclosed Vulnerabilities

CISA urges agencies to upgrade or remove end-of-life Ivanti appliances

CISA warns of critical vulnerability CVE-2024-8190 (CVSS 7.2) in Ivanti Cloud Services Appliance 4.6.

Urgent recommendations: upgrade to version 5.0 or remove outdated appliance.

Collaboration with FBI highlights importance of timely vulnerability remediation for security.

Ivanti Warns of Active Exploitation of Newly Patched Cloud Appliance Vulnerability (thehackernews.com)

Cyber Security News

New Android malware 'Ajina.Banker' steals financial data and bypasses 2FA via Telegram

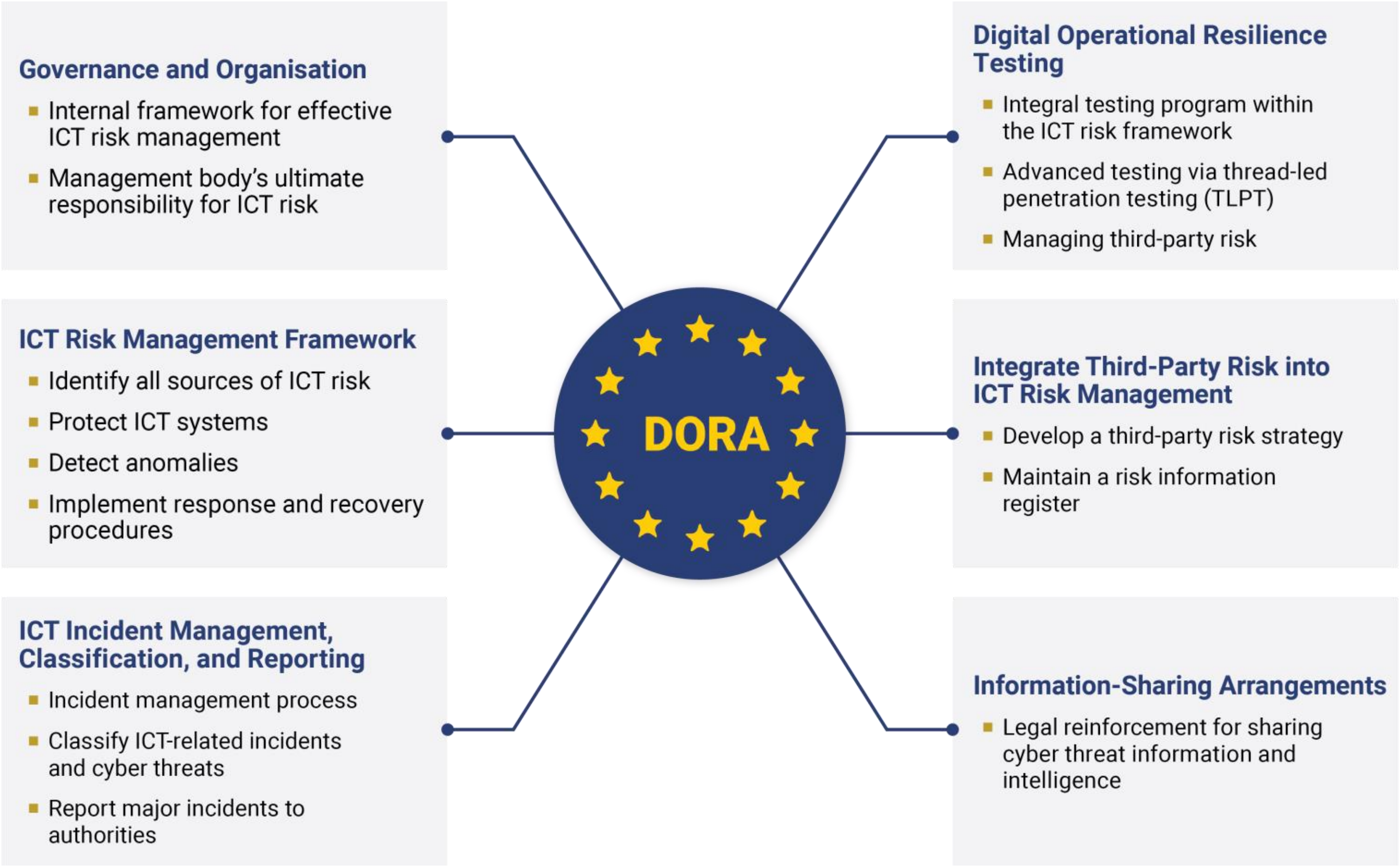
Ajina.Banker targets Central Asia, impersonating apps to steal banking credentials.

Utilizes social engineering via Telegram for distributing malicious links and offers.

Employs an affiliate model; professionals should advocate for cautious app practices.

New Android Malware Ajina.Banker Steals 2FA Codes, Spreads via Telegram (hackread.com)

What is the EU's DORA?



Governance and Organisation

- Internal framework for effective ICT risk management
- Management body's ultimate responsibility for ICT risk

ICT Risk Management Framework

- Identify all sources of ICT risk
- Protect ICT systems
- Detect anomalies
- Implement response and recovery procedures

ICT Incident Management, Classification, and Reporting

- Incident management process
- Classify ICT-related incidents and cyber threats
- Report major incidents to authorities

Digital Operational Resilience Testing

- Integral testing program within the ICT risk framework
- Advanced testing via thread-led penetration testing (TLPT)
- Managing third-party risk

Integrate Third-Party Risk into ICT Risk Management

- Develop a third-party risk strategy
- Maintain a risk information register

Information-Sharing Arrangements

- Legal reinforcement for sharing cyber threat information and intelligence

The Digital Operational Resilience Act (DORA), which entered into force on 16 January 2023 and will apply from 17 January 2025, aims to enhance the digital **operational resilience** of entities across the EU financial sector - https://www.eba.europa.eu/

vCISO Four Pillars in summary

1

Information Security Program Management

Develop and maintain an Information Security Program that complements their business strategy and risk tolerance.

2

Trusted Advisor – Coaching and Counsel

Helping reach balanced conclusions that drive reasonable Information Security decisions and measures.

Providing clarity and focus to see through the complexities and contradictions of today's Information Security and threat landscape.

3

Governance and Compliance Oversight

Ensuring Information Security Programs will meet their regulatory, audit and compliance obligations.

4

A Flexible Approach

"What keeps you up at night?" Customized solutions and recommendations for special Information Security challenges and concerns.

Did we cover everything?
Anything else on your mind?

THRIVE℠

Thank you for your time

thrivenextgen.com / 0 203 535 7800

Protect
and Serve
vCISO

Additional vCISO Focus Areas

- Gap Analysis. Current State -> Future State execution.
- Security Framework. Discuss, Refine and Improve, Develop and Publish
- Incident Response. Develop
- **Perform Table-Top Exercise for senior LOB management – make it relevant.**
- Ongoing Penetration Testing.
- Custom Requests.
  Discuss and address ad hoc security concerns and projects as they come up.

Organizational / Financial Justification

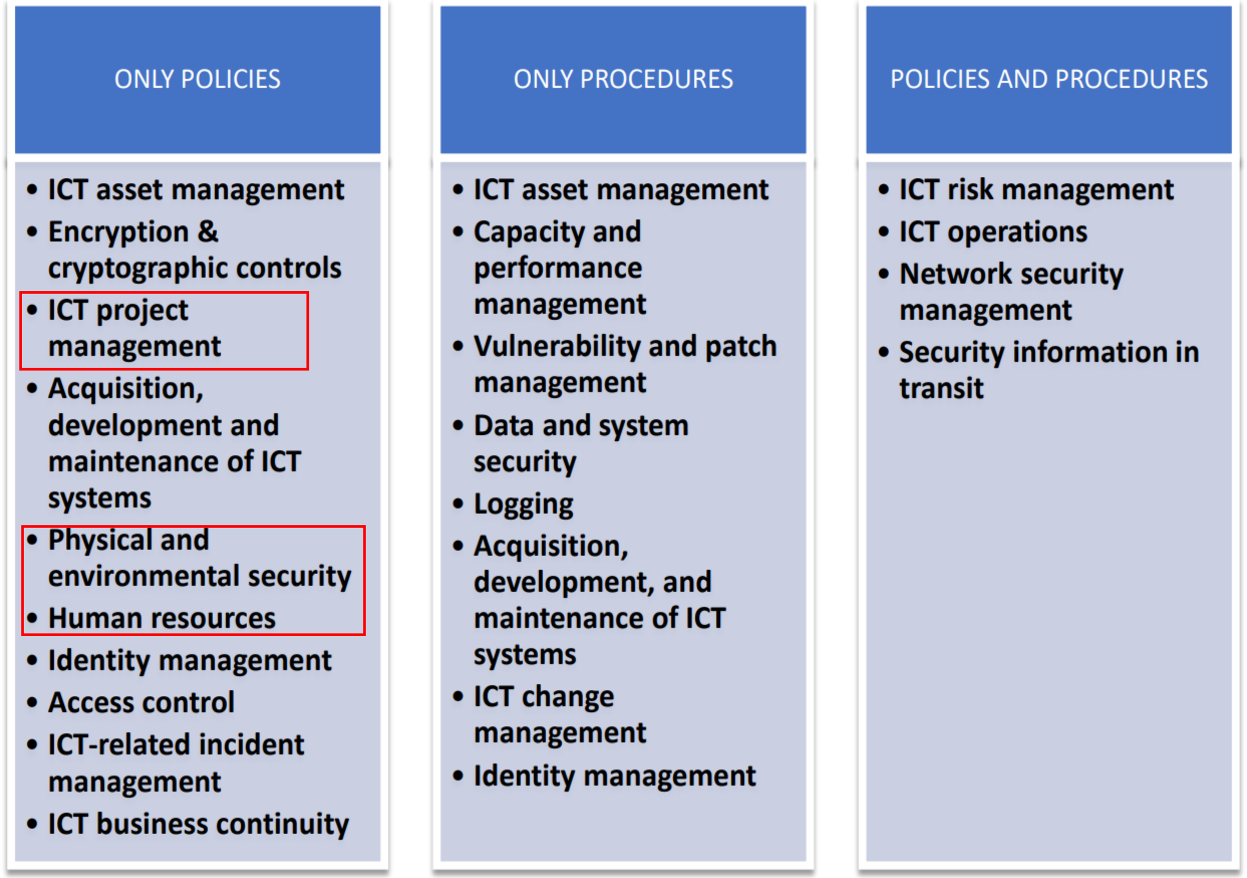
- The majority of Thrive customers are unable to utilize a full-time CISO
- On demand expertise – as little (or as much) as you need
- Full-time CISOs are difficult to attract and retain
- Full-time CISO average tenure less than 24 months
- High Demand = High Costs
- On average, a vCISO solution costs one-third to one-half what a full-time CISO commands
- Results focused. An objective, external advisor unencumbered by internal pressure and politics
- Team based model with peer review. Broader focus on your information Security challenges

Cybersecurity Frameworks

- Common Security Frameworks
  - Center for Internet Security (CIS)
  - International Standards Organization (ISO 27001) – See DORA
  - National Institute of Standards and Technology (NIST Cybersecurity Framework)
  - NIS and NIS2

- Industry Specific Frameworks
  - Health Information Trust Alliance (HITRUST)
  - **Payment Card Industry Data Security Standard (PCI DSS)**
  - Control Objectives for Information and Related Technologies (COBIT)

DORA – Policies and Procedures



ONLY POLICIES

- ICT asset management
- Encryption & cryptographic controls
- ICT project management
- Acquisition, development and maintenance of ICT systems
- Physical and environmental security
- Human resources
- Identity management
- Access control
- ICT-related incident management
- ICT business continuity

ONLY PROCEDURES

- ICT asset management
- Capacity and performance management
- Vulnerability and patch management
- Data and system security
- Logging
- Acquisition, development, and maintenance of ICT systems
- ICT change management
- Identity management

POLICIES AND PROCEDURES

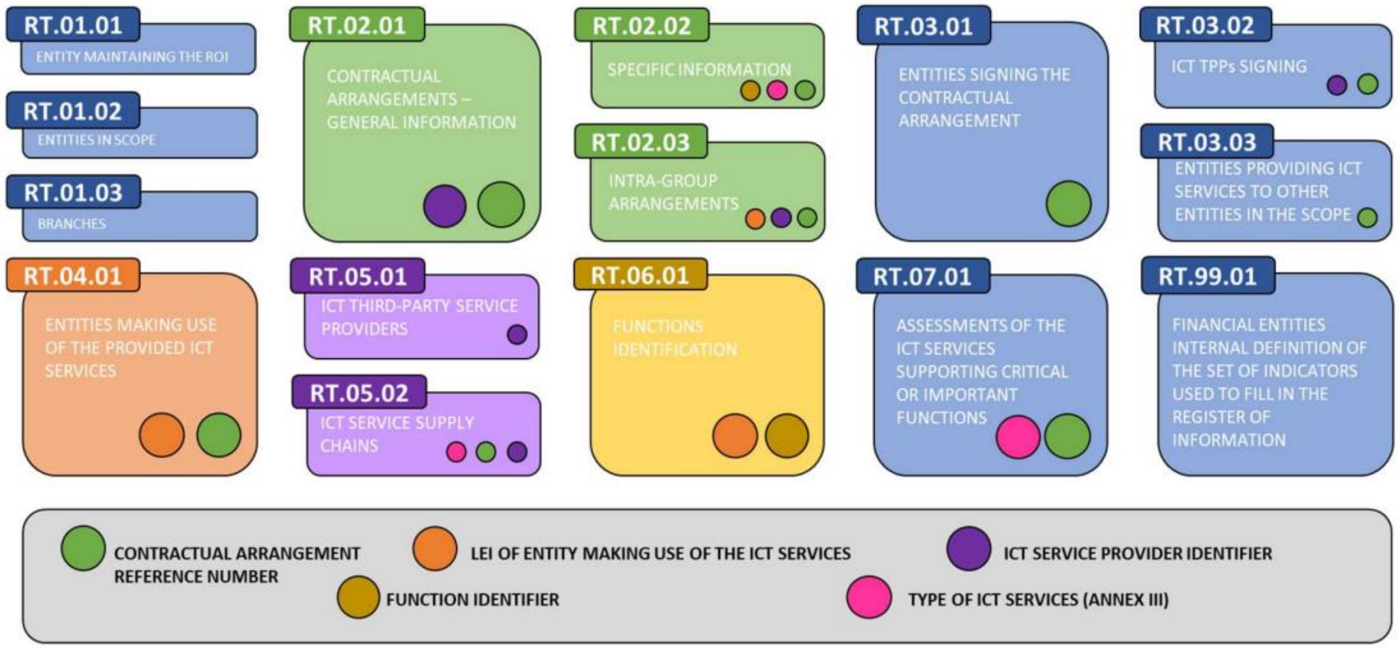
- ICT risk management
- ICT operations
- Network security management
- Security information in transit

DORA Title II: Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

DORA – Register of Information of ICT TPPs

Illustration 1: Structure of the Register of Information



RT.01.01 ENTITY MAINTAINING THE ROI

RT.01.02 ENTITIES IN SCOPE

RT.01.03 BRANCHES

RT.02.01 CONTRACTUAL ARRANGEMENTS – GENERAL INFORMATION

RT.02.02 SPECIFIC INFORMATION

RT.02.03 INTRA-GROUP ARRANGEMENTS

RT.03.01 ENTITIES SIGNING THE CONTRACTUAL ARRANGEMENT

RT.03.02 ICT TPPs SIGNING

RT.03.03 ENTITIES PROVIDING ICT SERVICES TO OTHER ENTITIES IN THE SCOPE

RT.04.01 ENTITIES MAKING USE OF THE PROVIDED ICT SERVICES

RT.05.01 ICT THIRD-PARTY SERVICE PROVIDERS

RT.05.02 ICT SERVICE SUPPLY CHAINS

RT.06.01 FUNCTIONS IDENTIFICATION

RT.07.01 ASSESSMENTS OF THE ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

RT.99.01 FINANCIAL ENTITIES INTERNAL DEFINITION OF THE SET OF INDICATORS USED TO FILL IN THE REGISTER OF INFORMATION

CONTRACTUAL ARRANGEMENT REFERENCE NUMBER

LEI OF ENTITY MAKING USE OF THE ICT SERVICES

ICT SERVICE PROVIDER IDENTIFIER

FUNCTION IDENTIFIER

TYPE OF ICT SERVICES (ANNEX III)

Each box represents one template of the Register of information.

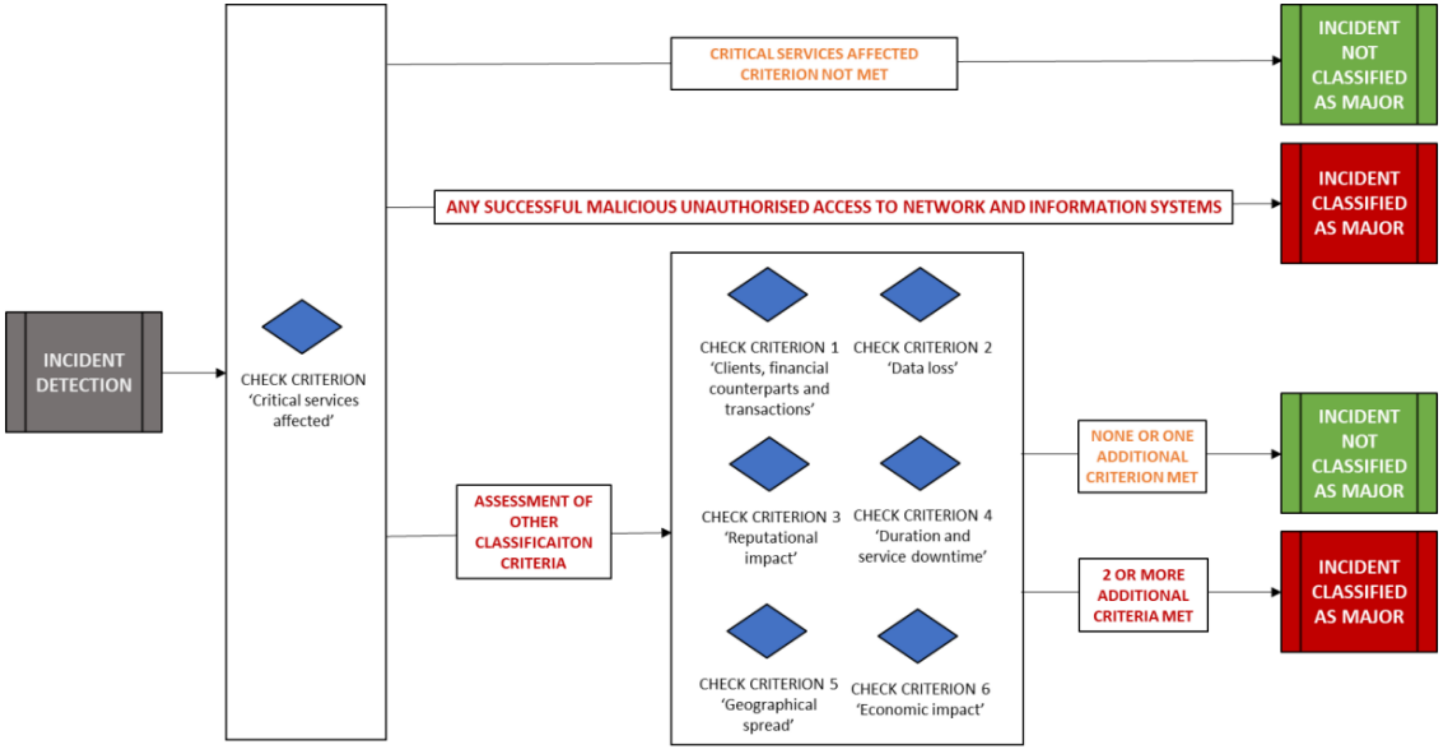
All FEs are required to maintain and update a register of information (ROI) in relation to all contractual arrangements on the use of ICT services provided by ICT Third-Party Service Providers (ICT TPPs).

The registers of information should include only financial entities licenced and operating in the EU

Microsoft Word - JC 2023 85_Final report on draft ITS on Register of Information.docx (europa.eu)

DORA – Incident Classification

Figure 1: Approach for classifying major incidents under DORA

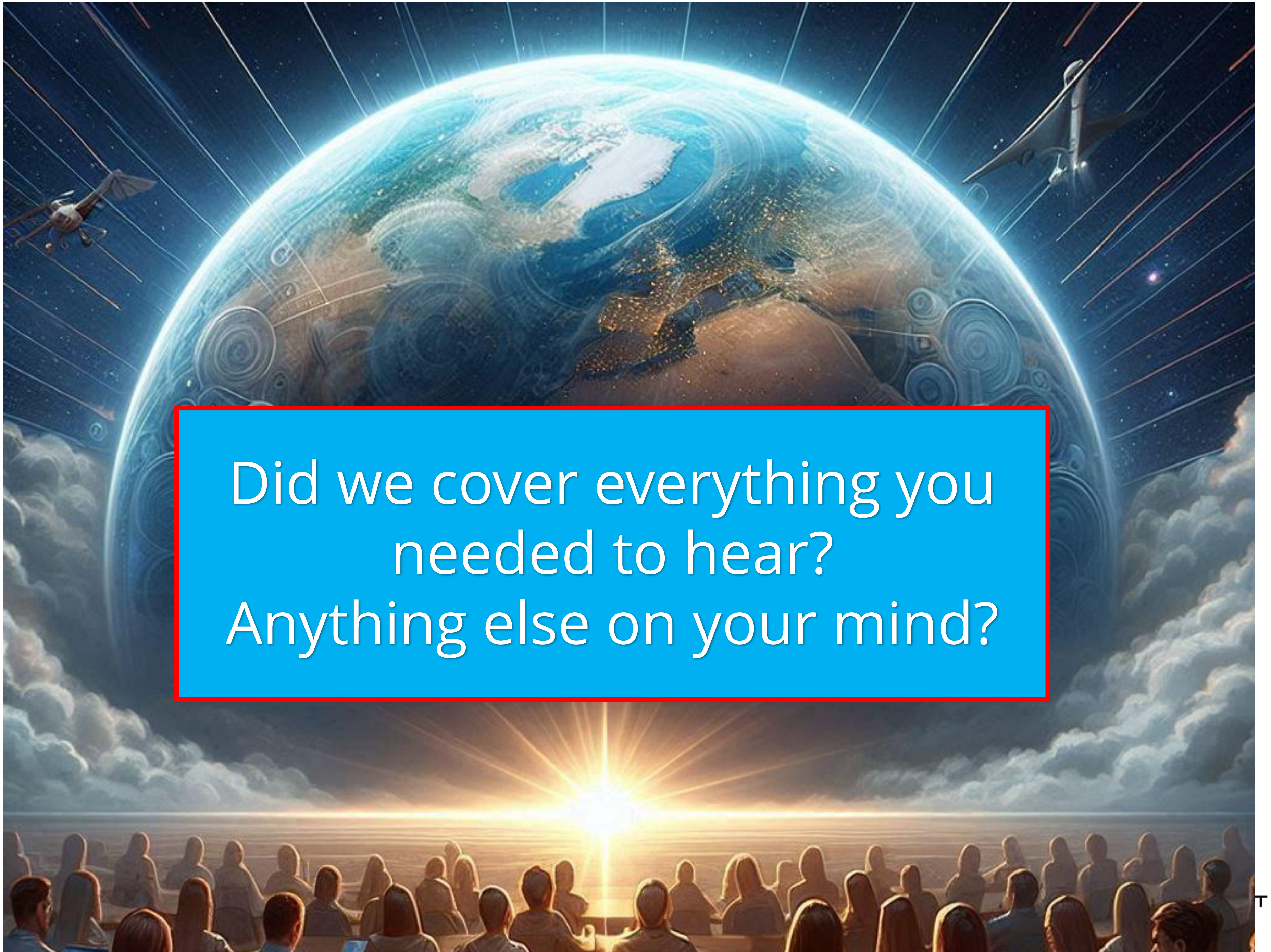

INCIDENT DETECTION
CHECK CRITERION 'Critical services affected'
CRITICAL SERVICES AFFECTED CRITERION NOT MET
INCIDENT NOT CLASSIFIED AS MAJOR
ANY SUCCESSFUL MALICIOUS UNAUTHORISED ACCESS TO NETWORK AND INFORMATION SYSTEMS
INCIDENT CLASSIFIED AS MAJOR
ASSESSMENT OF OTHER CLASSIFICAITON CRITERIA
CHECK CRITERION 1 'Clients, financial counterparts and transactions'
CHECK CRITERION 2 'Data loss'
CHECK CRITERION 3 'Reputational impact'
CHECK CRITERION 4 'Duration and service downtime'
CHECK CRITERION 5 'Geographical spread'
CHECK CRITERION 6 'Economic impact'
NONE OR ONE ADDITIONAL CRITERION MET
INCIDENT NOT CLASSIFIED AS MAJOR
2 OR MORE ADDITIONAL CRITERIA MET
INCIDENT CLASSIFIED AS MAJOR

DORA introduces consistent requirements for FEs on management, classification and reporting of ICT-related incidents.

JC 2023 83 - Final Report on draft RTS on classification of major incidents and significant cyber threats.pdf (europa.eu)

Why Virtual CISO?

- Need for a proactive approach to cybersecurity
- Board level and executive concern
  - Partner requirement
  - Audit requirement
  - Regulatory requirement
  - Cyber Insurance requirement
- Awareness of the cybersecurity landscape
  - Read something
  - Saw a news story
  - Knew someone who knew someone who had suffered a compromise



Did we cover everything you needed to hear?
Anything else on your mind?

THRIVE℠

Thank you for your time

thrivenextgen.com / 0203 535 7800