Cybersecurity Compliance & Operational Resilience

Emmanuel GENESTEIX

Expert Consulting for Digital Resilience & Compliance

Table of content

① Penalties

① Banks hacking

① DORA

③ ISO 27005

③ CSSF 22806

③ ISO 27001-2

⑤ Business Continuity & Data Recovery Planning

⑥ ISO 27014

⑦ Cybersecurity Compliance Consultant

⑧ Project Management

⑨ Portfolio Management

⑩ Resume

❶ S

❷ Q

❸ S

❹ D

❺ D

❻ S

❼ S

Table of content

Penalties

- **Administrative fines**: Financial institutions may be fined up to 10 million euros or 5% of their total annual turnover, whichever is higher, in the event of a serious violation of the regulation.

- Compensation for damages: Financial institutions may be required to **compensate clients or third parties** for any damage resulting from a failure to meet the regulation’s requirements.

- **Withdrawal of authorization**: Supervisory authorities may withdraw the authorization of financial institutions that repeatedly fail to comply with the regulation’s requirements.

- **Corrective measures**: Supervisory authorities may require financial institutions to implement corrective measures to address weaknesses or failures in their operational resilience.

Banks hacking

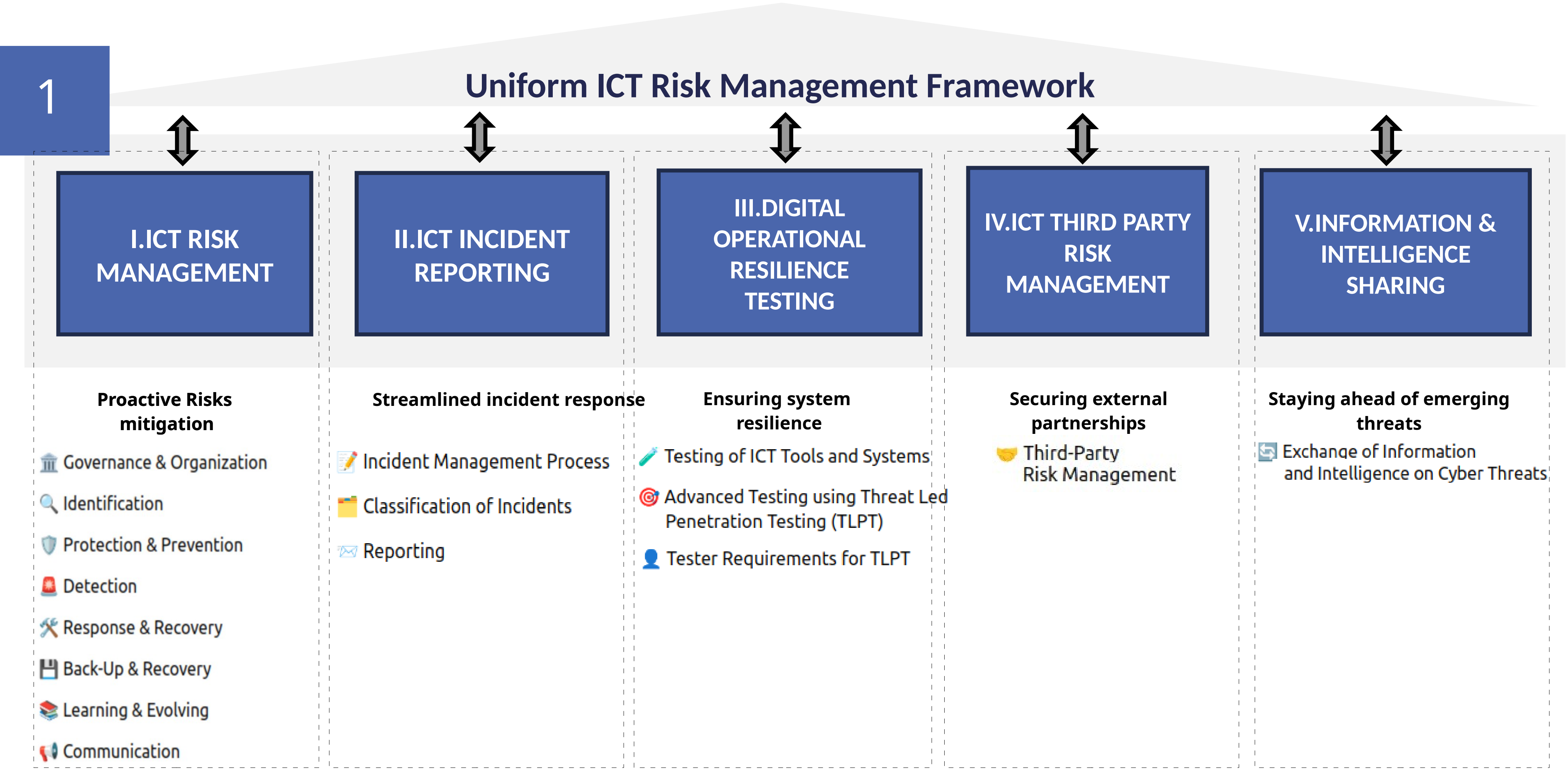
1. Revolut Data Breach (2022)

- What happened: In September 2022, Revolut, a fintech company with a European banking license (in Lithuania), disclosed that an unauthorized third party had gained access to a small percentage of its **customer data**.
- Impact on data: Approximately 50,000 customers worldwide were affected. Compromised information reportedly included names, addresses, emails, and partial card payment data. Full card details and PINs were not exposed.
- Consequences: Revolut notified regulators and impacted customers and implemented additional security measures. While the breach was contained, it underscored the importance of robust data protection for digital-first banking platforms.

2. DDoS Attacks on Dutch Banks (2021)

- What happened: In early 2021, Dutch banks including ING, ABN AMRO, and Rabobank experienced **distributed denial-of-service (DDoS)** attacks. These attacks significantly slowed or disrupted online and mobile banking services.
- Impact on services: Customers faced temporary difficulties accessing their accounts, making payments, and performing other online transactions. Although no sensitive data was publicly reported as stolen, the outages caused inconvenience and heightened security concerns.
- Consequences: The incidents prompted the banks to strengthen their cybersecurity defenses, improve monitoring and response capabilities, and ensure more resilient online services.

Your trusted partner in DORA compliance and Operational Resilience



1

Uniform ICT Risk Management Framework

I.ICT RISK MANAGEMENT

Proactive Risks mitigation

- 🏛️ Governance & Organization
- 🔍 Identification
- 🛡️ Protection & Prevention
- 🚨 Detection
- 🛠️ Response & Recovery
- 💾 Back-Up & Recovery
- 📚 Learning & Evolving
- 📢 Communication

II.ICT INCIDENT REPORTING

Streamlined incident response

- 📝 Incident Management Process
- 🗂️ Classification of Incidents
- 📨 Reporting

III.DIGITAL OPERATIONAL RESILIENCE TESTING

Ensuring system resilience

- 🧪 Testing of ICT Tools and Systems
- 🎯 Advanced Testing using Threat Led Penetration Testing (TLPT)
- 👤 Tester Requirements for TLPT

IV.ICT THIRD PARTY RISK MANAGEMENT

Securing external partnerships

- 🤝 Third-Party Risk Management

V.INFORMATION & INTELLIGENCE SHARING

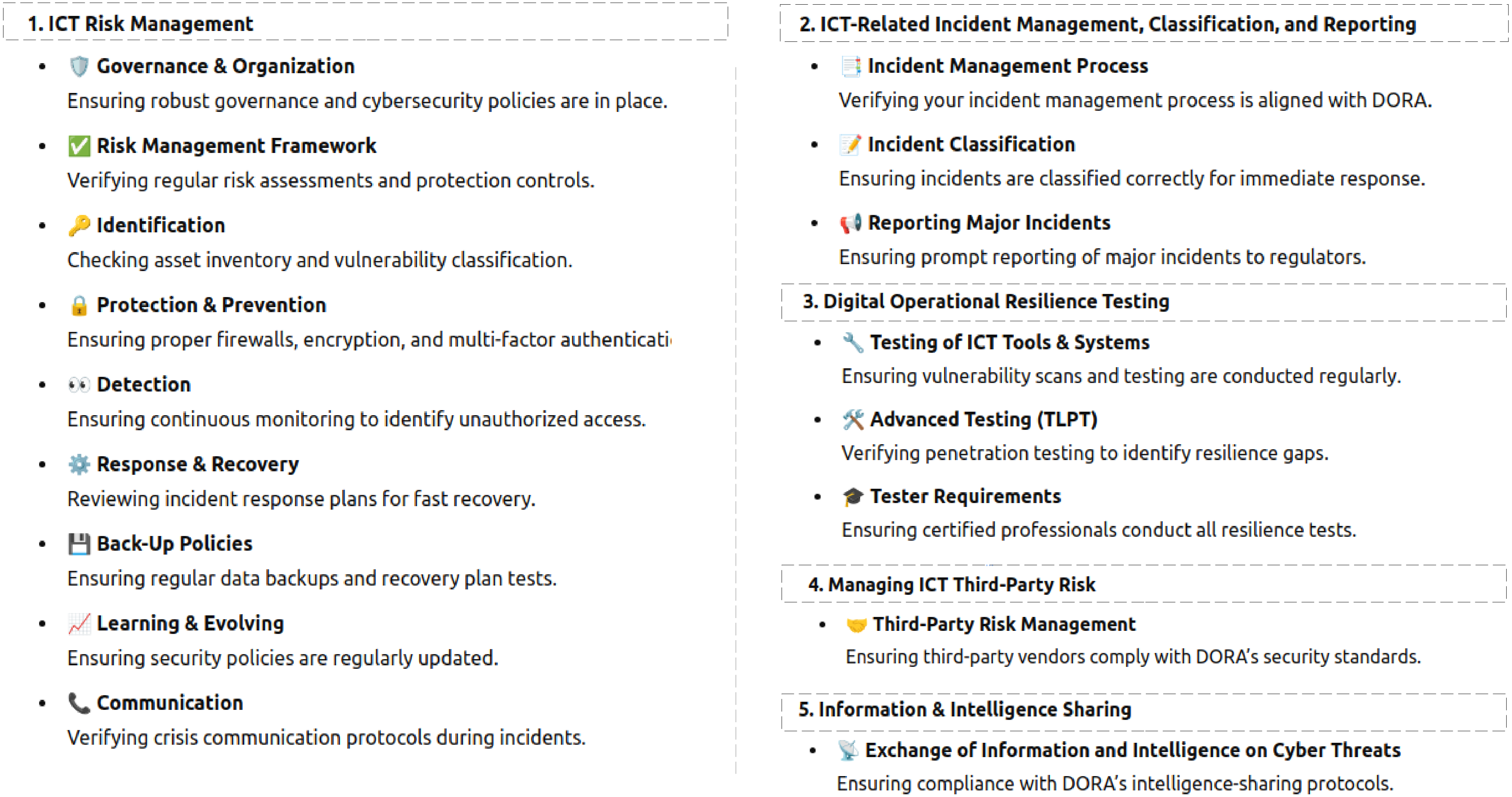
Staying ahead of emerging threats

- 🔄 Exchange of Information and Intelligence on Cyber Threats

Your partner implementing DORA to ensure operational resilience

DORA regulation: Building resilient digital operations

1



1. ICT Risk Management

- 🛡️ **Governance & Organization**
  Ensuring robust governance and cybersecurity policies are in place.
- ✅ **Risk Management Framework**
  Verifying regular risk assessments and protection controls.
- 🔑 **Identification**
  Checking asset inventory and vulnerability classification.
- 🔒 **Protection & Prevention**
  Ensuring proper firewalls, encryption, and multi-factor authenticati
- 👀 **Detection**
  Ensuring continuous monitoring to identify unauthorized access.
- ⚙️ **Response & Recovery**
  Reviewing incident response plans for fast recovery.
- 💾 **Back-Up Policies**
  Ensuring regular data backups and recovery plan tests.
- 📈 **Learning & Evolving**
  Ensuring security policies are regularly updated.
- 📞 **Communication**
  Verifying crisis communication protocols during incidents.

2. ICT-Related Incident Management, Classification, and Reporting

- 📑 **Incident Management Process**
  Verifying your incident management process is aligned with DORA.
- 📝 **Incident Classification**
  Ensuring incidents are classified correctly for immediate response.
- 📢 **Reporting Major Incidents**
  Ensuring prompt reporting of major incidents to regulators.

3. Digital Operational Resilience Testing

- 🔧 **Testing of ICT Tools & Systems**
  Ensuring vulnerability scans and testing are conducted regularly.
- 🛠️ **Advanced Testing (TLPT)**
  Verifying penetration testing to identify resilience gaps.
- 🎓 **Tester Requirements**
  Ensuring certified professionals conduct all resilience tests.

4. Managing ICT Third-Party Risk

- 🤝 **Third-Party Risk Management**
  Ensuring third-party vendors comply with DORA's security standards.

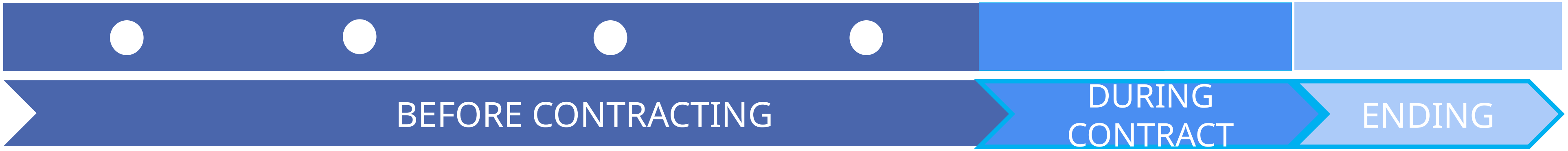
5. Information & Intelligence Sharing

- 📡 **Exchange of Information and Intelligence on Cyber Threats**
  Ensuring compliance with DORA's intelligence-sharing protocols.

Your specialist implementing CSSF regulation 22-806

I will help you fortify your organization's cybersecurity defenses addressing third-party risk management, mitigating operational risks, and enhancing overall resilience.

1



CRITICAL FUNCTIONS

Classify outsourced functions (e.g., payroll, IT hosting) as critical or non-critical based on business impact.

RISK ASSESSMENT & DUE DILIGENCE

Assess provider location, political risks, data protection, and perform due diligence before outsourcing.

OUTSOURCING PROCESS

Maintain an outsourcing register, evaluate risks and conflicts, and notify authorities for critical functions.

OUTSOURCING AGREEMENT

Define rights, obligations, audit rights, data confidentiality, and termination clauses in written agreements.

MONITORING

Continuously monitor provider performance, especially for critical functions, using KPIs and audits.

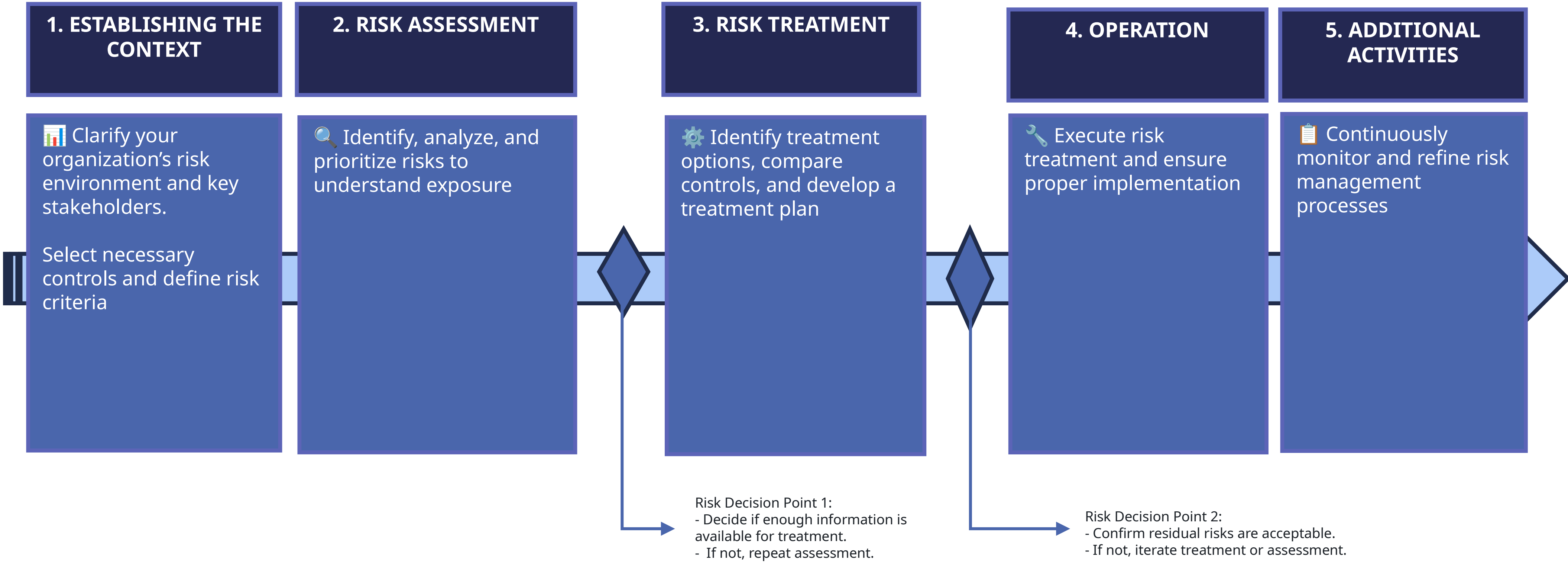
EXIT PLAN

Prepare exit strategies for provider failure, contract termination, or degraded service quality.

Helping you achieve ISO 27005 Risk Management Compliance

ISO 27005 Risk Management Framework for Information Systems & Organizations

1



1. ESTABLISHING THE CONTEXT

📊 Clarify your organization’s risk environment and key stakeholders.

Select necessary controls and define risk criteria

2. RISK ASSESSMENT

🔍 Identify, analyze, and prioritize risks to understand exposure

3. RISK TREATMENT

⚙️ Identify treatment options, compare controls, and develop a treatment plan

4. OPERATION

🔧 Execute risk treatment and ensure proper implementation

5. ADDITIONAL ACTIVITIES

📋 Continuously monitor and refine risk management processes

Risk Decision Point 1:
- Decide if enough information is available for treatment.
- If not, repeat assessment.

Risk Decision Point 2:
- Confirm residual risks are acceptable.
- If not, iterate treatment or assessment.

Your ISO 27001/27002 specialist for resilient information security

ISO 27001:27002 Information security management standards

1

A.5 SECURITY POLICY

Policy

- Establish and review your information security policy for organizational consistency.

A.6 INFORMATION SECURITY ORG.

Organization

- Ensure strong management commitment and coordination for security.

A.7 ASSET MANAGEMENT

Assets

- Track and classify assets for better risk management.

A.8 HR SECURITY

👥 People

- Establish roles, responsibilities, and security awareness for all staff
- Define assets return policies.

A.9 PHYSICAL & ENVIRONMENT AL

🔒 Security

- Ensure secure access and disposal for physical assets.

A.10 OPERATIONS MANAGEMENT

⚙️ Operations

- Implement and monitor operational procedures for security compliance.
- Monitor Third party services
- Data back-up

A.11 ACCESS CONTROL

🔑 Access

- Ensure strict access control policies and authentication mechanisms: access policy, pivilege management, password policy

A.12 SYSTEM DEVELOPMENT

💻 Development

- Integrate security measures throughout system development: security requirements, cryptography, vulnerability management.

A.13 INCIDENT MANAGEMENT

🚨 Incident

- Develop incident reporting and evidence collection processes.

A.14 BUSINESS CONTINUITY

🔄 Continuity

- Ensure business continuity plans and ongoing testing.

A15. ENSURE LEGAL & SECURITY COMPLIANCE

⚖️ Legal

- Ensure compliance with data protection and privacy regulations.

Your Guide to BCMS and Disaster Recovery Planning

1

- **ISO 22301:2019** BCMS Framework
- **ISO 22317:2015** BIA - Business Impact Analysis
- **ISO 22313:2020** BCMS Guidelines
- **ISO 27001:2013** Information Security Continuity

1. ANALYZE BUSINESS CONTEXT

- Conduct BIA,
- Define BCMS scope,
- Align with legal & regulatory requirements

2. SECURE LEADERSHIP COMMITMENT

- Engage senior management and secure buy-in.
- Establish and communicate a continuity policy.
- Gain support for necessary resources.

3. EVALUATE & MITIGATE RISKS

- Identify and assess risks to business operations.
- Select strategies to treat risks (avoid, reduce, transfer, accept).
- Prioritize mitigation efforts based on impact.

4.DEVELOP CONTINUITY STRATEGIES

- Design detailed continuity & recovery strategies.
- Identify critical resource needs (staff, infrastructure, tools).
- Document response and recovery plans.

5. IMPLEMENT & EXECUTE PLANS

- Set up response structures and teams.
- Establish effective communication protocols.
- Execute response plans during incidents.

6. TEST, MONITOR & IMPROVE

- Test plans through simulations and exercises.
- Evaluate BCMS performance and identify gaps.
- Implement continuous improvements.

Monitoring Risk Management Metrics with ISO/IEC 27014:2016

1

Monitoring these metrics ensures alignment with ISO 27014:2016, strengthens ISMS processes and enhances overall security resilience

Processes to monitor:

🛠️ ISMS processes Implementation
🚨 Incident Management
🛡️ Vulnerability Management
🖥️ Configuration Management
🗣️ Security awareness and training
🔒 Access control, firewall, and event logging
🔍 Audit
🧮 Risk assessment process
♻️ Risk treatment process
🤝 Third-party risk management

Key metrics examples to monitor ISMS processes

PROCESS	KPI	DESCRIPTION	✅ TARGET
🚨 Incident Management	Mean Time to Detect/Resolve	Average time to detect & resolve security incidents.	Detect < 24 hours, Resolve < 72 hours
🛡️ Vulnerability Management	Percentage of vulnerabilities remediated within SLA	Rate of of remediation completion within SLA.	> 95% remediation rate
🖥️ Configuration Management	Percentage of systems compliant with baseline configuration standards	Adherence to approved configuration baselines.	> 95% compliance

My offer in cybersecurity compliance

I will help you fortify your organization's cybersecurity defenses, ensuring compliance with regulations, mitigating risks and enhancing resilience.

2

CATEGORY	DETAILS
KEY ACHIEVEMENTS	▪ Conducted comprehensive Risk Assessments under the DORA framework ▪ Led internal and external audits in compliance with ISO standards ▪ Designed and implemented BCP/DRP plans to ensure operational resilience ▪ Developed and executed risk mitigation plans for critical systems ▪ Drafted and enforced IT Policies aligned with industry best practices ▪ Delivered cybersecurity awareness training to enhance organizational security culture ▪ Successfully improved compliance posture by aligning with CSSF Regulation 22-806 and ISO standards
REGULATIONS	DORA, ISO 27001 – 27002, ISO 27005, ISO 22301:2019, ISO 27001:2013, ISO 22317:2015 ISO 22313:2020, CSSF Regulation 22-806
TRAININGS	CISM, COMPTIA Network +, COMPTIA Security +
DELIVERABLES	• Audit Reports with actionable recommendations • Risk Management Plans including prioritized mitigation actions • BCP/DRP Plans ensuring resilience and continuity • Cybersecurity Awareness Training Materials tailored to organizational needs • Compliance Checklists for regulatory alignment
KPIS	• Compliance Rate: Alignment with DORA and ISO standards (%)
VALUE ADDED	▪ Enhanced organizational compliance with DORA and CSSF regulations ▪ Reduced cybersecurity risks through effective mitigation strategies ▪ Improved operational resilience via robust BCP/DRP plans ▪ Increased staff cybersecurity awareness, reducing the likelihood of human error ▪ Strengthened organizational reputation with clients and regulators through proactive risk and compliance management

My offer in Project Management

I will help you deliver projects on time, within budget and aligned with your strategic goals by leveraging agility, collaboration, and effective risk management.

2

CATEGORY	DETAILS
KEY ACHIEVEMENTS	▪ DORA Risk Assessments, ▪ Transition to ServiceNow ITSM ▪ Hardening of network Architecture design - Defense in Depth ▪ BCP/DRP initiatives ▪ Salesforce data migration
CERTIFICATIONS	Prince2 Practitioner, PM² Certified, Scrum Alliance Certified, SAFe Scaled Agile Certified, Change Management Practitioner
PROCESS EXPERTISE	Full project lifecycle: Initiation, Planning, Execution, Monitoring, Closure. Optimizing Scope, Risks, Quality, Budget, and Timeline
DELIVERABLES	Business Plans, Project Charters, Risk/Change Management Plans, SOPs, Gap Analysis, Service Level Agreements, Technical Specifications, Target Architecture
KPIS	Schedule/Cost Variance, Risk Resolution, On-time Delivery (%), Stakeholder Satisfaction (%), Project Success Rate (%), Resource Utilization Efficiency (%)
VALUE ADDED	▪ Facilitate effective meetings, ensuring clear communication and stakeholder collaboration. ▪ Resolve challenges through proactive problem-solving and creative solutions. ▪ Manage risks by anticipating, assessing, and mitigating potential disruptions. ▪ Optimize project delivery with critical path planning and milestone prioritization. ▪ Enhance visibility through dashboards, providing clear KPIs and actionable insights.

My offer in Portfolio Management

I will help you optimize portfolio performance, prioritize projects, and allocate resources efficiently, ensuring alignment with your strategic goals through agility, collaboration, and effective risk and value management.

2

CATEGORY	DETAILS
KEY ACHIEVEMENTS	▪ Successfully grew the portfolio budget from €600K in Year 1 to €1.8M in Year 3, securing C-Suite approval for increased funding through strong value demonstration.
CERTIFICATIONS	SAFe Scaled Agile Certified
PROCESS EXPERTISE	▪ Portfolio Management Framework Definition ▪ Portfolio Composition (selection, prioritization, and approval) ▪ Portfolio Delivery (monitoring, controlling, and managing value) ▪ Stakeholder Engagement and Communication ▪ Portfolio Governance and Decision-Making
DELIVERABLES	Portfolio Manual, Portfolio Analysis Report, Stakeholder Matrix, Portfolio Logs (risks, issues, decisions), Communication Plan, Portfolio Dashboards and Reports
KPIS	Portfolio Value Realization (CPI, SPI, EAC), Resource Utilization Efficiency (%), On-time Delivery (%), Portfolio Success Rate (%), Stakeholder Satisfaction (%), Portfolio Financial Metrics (ROI, Cost-Benefit Ratio)
VALUE ADDED	▪ Facilitate portfolio meetings, ensuring clear communication and alignment with stakeholders ▪ Resolve challenges through proactive risk management and issue resolution

Resume

Emmanuel GENESTEIX

3

PROFESSIONAL BACKGROUND

- Over 20 years in IT, specializing in cybersecurity.
- Roles in consulting, audit and cybersecurity project/portfolio management.

FRAMEWORK EXPERTISE

- DORA
- ISO 27001-27002, 27005
- ISO 22301:2019, ISO 27001:2013, ISO 22317:2015, ISO 22313:2020
- CSSF 22-806,
- NIS2 etc

DIPLOMAS/CERTIFICATIONS/TRAININGS

- Diploma: MBA, computer science
- Certifications: SAFe, Scrum, PM2, PM2 Agile Prince2 Practitioner
- Cybersecurity trainings::
  Certified Information Security Manager (CISM)
  CompTIA Security+
  CompTIA Network+

KEY EXPERIENCE AREAS

- Cybersecurity Compliance Consulting
- Project Management
- Portfolio Management

Next Steps

4

- ❑ I suggest we have 30 mn call or meeting at your premises
- ❑ My email: emmanuelgenesteix@yahoo.fr
- ❑ Telephone: +352.661.78.08.07

Your ISO 27001/27002 specialist for resilient information security

ISO 27001:27002 Information security management standards

1

A.5 SECURITY POLICY

- A.5.1.1 Security Policy Document,
- A.5.1.2 Policy Review

A.6 INFORMATION SECURITY ORG.

- A.6.1.1 Management Commitment,
- A.6.1.2 Security Coordination
- A.6.2.1 External Risks Identification,
- A.6.2.2 Security in Client/Tier Agreements

A.7 ASSET MANAGEMENT

- A.7.1.1 Asset Inventory,
- A.7.1.2 Asset Ownership,
- A.7.2.1 Classification Guidelines

A.8 HR SECURITY

- A.8.1.1 Roles & Responsibilities,
- A.8.2.2 Security Awareness Training,
- A.8.3.2 Asset Return

A.9 PHYSICAL & ENVIRONMENTAL

- A.9.1.1 Security Perimeter,
- A.9.1.2 Physical Entry Controls,
- A.9.2.6 Secure Disposal

A.10 OPERATIONS MANAGEMENT

- A.10.1.1 Operational Procedures,
- A.10.2.2 Monitoring Third-Party Services,
- A.10.5.1 Data Backup

A.11 ACCESS CONTROL

- A.11.1.1 Access Policy,
- A.11.2.2 Privilege Management, A.11.3.1 Password Policy

A.12 SYSTEM DEVELOPMENT

- A.12.1.1 Security Requirements, A.12.3.1 Cryptographic Controls,
- A.12.6.1 Technical Vulnerability Management

A.13 INCIDENT MANAGEMENT

- A.13.1.1 Incident Reporting,
- A.13.2.2 Lessons Learned,
- A.13.2.3 Evidence Collection

A.14 BUSINESS CONTINUITY

- A.14.1.3 Continuity Plans,
- A.14.1.5 Testing & Maintenance

A15. AVOID BREACHES OF LAWS, CONTRACTUAL OBLIGATIONS & SECURITY REQUIREMENTS.

- A.15.1.4 Data Protection & Privacy, A.15.3.2 Audit Tools Protection