The risk tent

The “risk tent” represents the shelter of structured risk management, without a reliable framework, your risk assessment collapses under pressure. Choosing the right methodology provides the support structure that keeps your organisation protected, even when conditions change.

New to risk assessment? Start with OCTAVE. It is the most accessible for organisations without dedicated risk management teams and emphasises business stakeholder involvement.

Need regulatory compliance? EBIOS aligns well with EU frameworks and ISO standards, particularly in regulated industries.

Want quantitative metrics? MEHARI provides structured scoring for risk prioritisation and board reporting.

Table of Contents

Choosing your risk map

Before assessing risk, you need a method that everyone can follow without getting lost. A good risk assessment approach clearly identifies potential impacts, evaluates how likely they are, produces consistent results, and stays reliable even when things change.

There are several established ways to do this:

- OCTAVE – a self-directed method focused on aligning risks with organisational goals. It looks beyond technology to consider how strategy, culture, and practices affect security. Best for organisations that want to involve business stakeholders directly in identifying and prioritising risks, rather than leaving it solely to IT teams.
- MEHARI – a modular European framework that integrates neatly with other management systems. It offers tools for analysing and managing risks throughout the security lifecycle. Ideal for organisations needing quantitative risk scores for board reporting or integration with existing management frameworks.
- EBIOS – a French-developed method that defines security needs and objectives before diving into technical risks, ensuring that every control serves a clear business purpose. Well-suited for regulated environments and organisations needing to demonstrate compliance with EU frameworks.

Each approach gets you to the same goal: understanding what could go wrong, how bad it could get, and how to keep climbing safely with a consistent, repeatable map.

Which methodology to choose?

Choose OCTAVE if…	Choose MEHARI if…	Choose EBIOS if…
You want business stakeholder involvement	You need quantitative risk scores	You want to start with security objectives
Your organisation values self-direction	You need to integrate with existing management systems	You work in a regulated industry (especially EU)
You focus on operational risk	You want modular, scalable assessment	You need to demonstrate compliance
You have 10-500 employees without dedicated risk teams	You need board-ready metrics and reporting	You require alignment with ISO 27001 or NIS2

Note: Each table below reflects its methodology's focus, OCTAVE emphasises threat sources and assets, MEHARI uses quantitative scoring, and EBIOS centres on security objectives. Choose the style that best fits your organisational culture and reporting needs.

OCTAVE style

Self-directed, organisational focus, identifying threats, assets, and impacts

Threat source definitions:

- Internal – employees, contractors, insiders with legitimate access
- External – attackers, competitors, malicious actors
- Environmental – natural disasters, infrastructure failures, climate events
- Accidental – human error, unintentional actions

Security area	Vulnerability	Example threats	Asset affected	Threat source	Impact	Suggested mitigating control
Hardware	Outdated firmware, default passwords	Physical tampering, malware installation	Devices	Internal/ External	Operational disruption, compromise	Automated firmware management, version control, secure configuration baselines, device hardening
Hardware	Unsecured USB ports	Malware introduction via removable media	Devices	Internal/ External	Malware infection, data theft	Disable/lock unused ports, enforce removable media policies, endpoint protection
Software	Unpatched OS or applications	Exploitation, ransomware	Systems	External	System compromise, data loss	Automated patch management, vulnerability scanning, patch testing procedures
Software	Misconfigured web apps or APIs	SQL injection, XSS, data exposure	Applications	External	Data theft, downtime	Secure coding standards, code review, penetration testing, API security testing

Security area	Vulnerability	Example threats	Asset affected	Threat source	Impact	Suggested mitigating control
Data/ Information	Unencrypted data at rest	Data theft, unauthorised access	Data	External	Confidentiality breach	Encryption at rest, key management, data classification
Data/ Information	Inadequate data classification	Mishandling of sensitive data	Data	Internal	Compliance violations, data leakage	Data classification scheme, labelling, handling procedures
Network	Open/misconfigured ports	Unauthorised access, network scanning	Network	External	Breach of perimeter	Firewall rules, network hardening, regular port scanning, change control
Network	Weak VPN/Wi-Fi credentials	Brute force, credential stuffing	Network	External	Account takeover, network compromise	Strong password policy, MFA, VPN hardening, WPA3
Cloud/SaaS	Misconfigured cloud storage	Data exposure, unauthorised access	Cloud services	Internal/ External	Data leakage	Cloud security posture management, least privilege, regular audits
Cloud/SaaS	Inadequate cloud access controls	Unauthorised resource access	Cloud services	Internal/ External	Data compromise	IAM policies, MFA, privileged access management, regular access reviews
Mobile	Lost or stolen mobile devices	Data theft, unauthorised access	Devices	External/ Accidental	Confidentiality loss	Remote wipe, encryption, device tracking, clear desk policy
Mobile	BYOD security risks	Malware, data leakage	Devices/ Systems	Internal/ External	Data compromise	BYOD policy, MDM, containerisation
Human					Account compromise,	Password policies, password managers, MFA, breach

Security area	Vulnerability	Example threats	Asset affected	Threat source	Impact	Suggested mitigating control
	Weak/reused passwords	Credential theft, account takeover	Accounts	Internal/ External	data theft	monitoring, training
Human	Phishing susceptibility	Malware execution, data theft	Accounts	External	Compromise, data breach	Awareness training, simulated phishing exercises, email filtering, reporting mechanisms
Physical/Site	Uncontrolled physical access	Theft of devices, media	Facilities	Internal/ External	Loss of devices, data	Badge access, locks, surveillance cameras, visitor controls, access logs
Physical/Site	Poor environmental controls	Fire/flood → system damage	Facilities	Environmental	System damage, downtime	HVAC, fire suppression, water detection, monitoring
Organisational	Missing or outdated policies/procedures	Compliance breaches, inconsistent practices	Organisation	Internal	Non-compliance, operational inefficiency	Policy creation, regular review, awareness, version control
Organisational	Lack of continuity/incident planning	Extended downtime, data loss	Organisation	Internal/ External	Business disruption	BCP/DR plans, testing, documented procedures, communication plans
Backup/ Recovery	Untested backup procedures	Recovery failures, data loss	Data	Internal	Data loss, downtime	Regular backup testing, documented recovery procedures, RTO/RPO
Backup/ Recovery	Insufficient backup frequency	Data loss between backups	Data	Accidental	Data gaps	Risk-based backup schedule, automated backups, monitoring

Security area	Vulnerability	Example threats	Asset affected	Threat source	Impact	Suggested mitigating control
						and alerting
Hardware	Insufficient periodic replacement schedule	Device failures, degraded security	Devices	Internal	Operational inefficiency	Equipment lifecycle management, replacement schedules, asset tracking
Software	Insecure third-party libraries	Supply chain compromise	Systems	External	Compromise, malware	Dependency management, software composition analysis, supplier security assessment
Network	Lack of network segmentation	Lateral movement	Network	Internal/ External	Breach escalation	VLANs, DMZ, zero-trust, micro-segmentation, ACLs
Cloud/SaaS	Shadow cloud services	Data leakage, compliance violations	Cloud services	Internal	Data leakage	CASB, approved service catalogue, monitoring

MEHARI style

Threat-oriented, quantitative scoring, risk treatment plan

Risk scoring guide:

- Likelihood: Low (rare) / Medium (occasional) / High (frequent or expected)
- Consequence: Low (minimal impact) / Medium (moderate impact) / High (severe impact)
- Risk Score: Combination of likelihood and consequence
    - High: Requires immediate action and senior management attention
    - Medium-High: Action needed within defined timeframe (typically 3-6 months)
    - Medium: Monitor and plan mitigation within 6-12 months
    - Low: Accept or monitor periodically

Security area	Vulnerability	Threat	Likelihood	Consequence	Risk Score	Suggested mitigating control
Hardware	Susceptible to temperature/humidity variations	Equipment malfunction, data loss	Medium	High	Medium-High	Environmental controls (HVAC, monitoring, alarms), temperature thresholds
Hardware	Lack of device hardening	Exploitation, malware installation	High	High	High	Device hardening standards, configuration baselines, regular security audits, monitoring
Software	Misconfiguration of software	System downtime, data exposure	Medium	High	Medium-High	Configuration management, change control, security baselines, automated compliance checks
Software	Misuse of software by users	Data corruption, unauthorised actions	Medium	Medium	Medium	User training, access controls, activity monitoring, approval workflows

Security area	Vulnerability	Threat	Likelihood	Consequence	Risk Score	Suggested mitigating control
Data/ Information	Poor data retention practices	Compliance violations, data exposure	Medium	High	Medium-High	Retention policies, automated deletion, archive procedures
Data/ Information	Inadequate data backup	Data loss, business disruption	Medium	High	Medium-High	Regular backups, backup testing, offsite storage, recovery procedures
Network	Insufficient monitoring	Undetected intrusions	High	High	High	SIEM, alerting, log review, anomaly detection, SOC
Network	Proof of sending/receiving messages lacking	Message tampering, spoofing	Medium	Medium	Medium	Digital signatures, non-repudiation mechanisms, secure protocols (S/MIME, TLS)
Cloud/SaaS	Misconfigured cloud storage	Data exposure, unauthorised access	High	High	High	Cloud security posture management, least privilege, regular audits
Mobile	Inadequate mobile device management	Unpatched devices, policy violations	Medium	Medium	Medium	MDM solution, automated patching, compliance monitoring, device inventory
Human	Excessive privileges	Insider misuse, sabotage	Medium	High	Medium-High	Role-based access, least privilege, periodic reviews, approval workflows
Human	Absence of key personnel	Delayed response, unmonitored systems	Medium	Medium	Medium	Cross-training, shift coverage, succession planning, documented procedures
Physical/Site	Inadequate visitor management	Tailgating, unauthorised access	Medium	Medium	Medium	Visitor logs, escorts, badge system, policy enforcement, reception

Security area	Vulnerability	Threat	Likelihood	Consequence	Risk Score	Suggested mitigating control
Physical/Site	Insecure storage of backups	Data theft, destruction	Medium	High	Medium-High	Offsite encrypted backups, secure storage, access controls
Organisational	Poor vendor management	Third-party compromise	Medium	High	Medium-High	Vendor risk assessments, security requirements in contracts, monitoring
Organisational	Weak audit and monitoring	Undetected insider activity	Medium	Medium	Medium	Centralised logging, audit trail reviews, automated alerting, periodic audits
Backup/ Recovery	Lack of backup verification	Corrupted or incomplete backups	Medium	High	Medium-High	Automated verification, integrity checks, regular restoration tests
Backup/ Recovery	Untested backup procedures	Recovery failures, data loss	Medium	High	Medium-High	Regular backup testing, documented recovery procedures, RTO/RPO
Hardware	End-of-life devices still in use	No patches, unsupported security	Medium	High	Medium-High	Retirement plan, replacement schedule, asset lifecycle policy
Network	Insecure network architecture	Lateral movement, MITM attacks	Medium	High	Medium-High	Network design review, defence in depth, segmentation, secure routing protocols
Network	Unprotected network connections	Eavesdropping, data interception	Medium	High	Medium-High	Encrypted protocols (TLS 1.3+), VPN, secure Wi-Fi (WPA3), certificate validation
Cloud/SaaS	Shadow cloud services	Data leakage, compliance violations	Medium	High	Medium-High	CASB, approved service catalogue, monitoring

Security area	Vulnerability	Threat	Likelihood	Consequence	Risk Score	Suggested mitigating control
Mobile	BYOD security risks	Malware, data leakage	Medium	Medium	Medium	BYOD policy, MDM, containerisation
Human	Shadow IT usage	Use of unapproved software/services	Medium	Medium	Medium	IT asset inventory, approval processes, monitoring, user education

EBIOS style

Risk expressed in terms of security objectives and threat scenarios

Security objectives:

- Confidentiality: Protecting information from unauthorised disclosure
- Integrity: Ensuring information accuracy and preventing unauthorised modification
- Availability: Ensuring systems and data are accessible when needed
- Traceability: Maintaining audit trails for accountability
- Authenticity: Verifying identity and origin of information
- Non-repudiation: Preventing denial of actions taken
- Compliance: Adherence to legal, regulatory, and policy requirements

Security area	Vulnerability	Security objective affected	Threat scenario	Likelihood	Severity	Countermeasures
Hardware	Poor cable management	Availability	Accidental disconnection	Medium	Medium	Structured cabling, cable covers, access restriction, physical inspections
Software	Legacy or unsupported software	Integrity	System compromise, incompatibility	Medium	Medium	Software upgrade plan, vendor support agreements, migration roadmap
Data/ Information	Unencrypted data at rest	Confidentiality	Data theft	Medium	High	Encryption at rest, key management, data classification
Network	Misconfigured load balancers/proxies	Availability	Traffic interception, service disruption	Medium	High	Configuration review, security hardening, access control, health monitoring

Security area	Vulnerability	Security objective affected	Threat scenario	Likelihood	Severity	Countermeasures
Cloud/SaaS	Inadequate cloud access controls	Confidentiality	Unauthorised resource access	Medium	High	IAM policies, MFA, privileged access management, regular access reviews
Mobile	Lost/stolen mobile devices	Confidentiality	Data theft	Medium	High	Remote wipe, encryption, device tracking, clear desk policy
Human	Inadequate security awareness	Compliance	Security incidents	Medium	Medium	Regular training, role-specific education, testing, security champions programme
Physical/Site	Inadequate power protection	Availability	Outages, device damage	Medium	High	UPS, surge protection, backup generators, monitoring
Physical/Site	Improper disposal of equipment/media	Confidentiality	Data recovery from discarded items	Medium	High	Secure disposal procedures, data wiping, physical destruction, certificates of destruction
Organisational	Inadequate staff training	Compliance	Mistakes, security incidents	Medium	Medium	Comprehensive awareness programmes, role-based training, testing, continuous learning
Backup/ Recovery	Insufficient backup frequency	Availability	Data loss between backups	Medium	High	Risk-based backup schedule, automated backups, monitoring and alerting
Backup/ Recovery	Untested backup procedures	Availability	Recovery failures	Medium	High	Regular backup testing, documented recovery procedures, RTO/RPO
Hardware	Insufficient periodic replacement schedule	Availability	Device failures	Medium	Medium	Equipment lifecycle management, replacement schedules, asset tracking

Security area	Vulnerability	Security objective affected	Threat scenario	Likelihood	Severity	Countermeasures
Software	Insecure third-party libraries	Integrity	Supply chain compromise	Medium	High	Dependency management, software composition analysis, supplier security assessment
Network	Lack of network segmentation	Integrity	Lateral movement	Medium	High	VLANs, DMZ, zero-trust, micro-segmentation, ACLs
Network	Weak VPN/Wi-Fi credentials	Confidentiality, Authenticity	Credential theft	Medium	High	Strong password policy, MFA, VPN hardening, WPA3
Cloud/SaaS	Misconfigured cloud storage	Confidentiality	Data exposure	Medium	High	Cloud security posture management, least privilege, regular audits
Mobile	Inadequate mobile device management	Integrity	Policy violations	Medium	Medium	MDM solution, automated patching, compliance monitoring, device inventory
Human	Weak/reused passwords	Confidentiality, Authenticity	Account takeover	Medium	High	Password policies, password managers, MFA, breach monitoring, training
Human	Phishing susceptibility	Confidentiality	Malware execution, data theft	Medium	High	Awareness training, simulated phishing exercises, email filtering, reporting mechanisms
Physical/Site	Uncontrolled physical access	Confidentiality	Theft of devices/media	Medium	High	Badge access, locks, surveillance cameras, visitor controls, access logs
Organisational	Lack of incident response capability	Availability, Traceability	Poor incident handling	Medium	High	Incident response plan, response team, playbooks, training and exercises

Security area	Vulnerability	Security objective affected	Threat scenario	Likelihood	Severity	Countermeasures
Organisational	Incomplete recordkeeping	Compliance, Traceability	Legal/regulatory risk	Medium	Medium	Standardised records management, retention policies, regular audits, backup procedures

Tools/Templates

Note: Tool availability and maintenance status verified as of November 2025. Check project websites for current status.

Methodology	Tool / Template	Platform / Format	What it supports	Best suited for	Status
OCTAVE / OCTAVE-inspired	OpenISMS (GitHub)	Web / open source	Governance + risk module inspired by OCTAVE Allegro	Small to medium orgs (10-500 employees) wanting free tool aligned with OCTAVE workflow	Active
MEHARI	MEHARI-Expert (Excel)	Excel workbook (legacy format)	MEHARI 2010 risk assessment + mapping to ISO 27001/27002	Small/medium organisations comfortable with Excel, note this is a 2010 version	Legacy
EBIOS / RM + MEHARI	Oligo Risk Manager	Web / cloud or on-premises	Supports EBIOS RM, MEHARI, ISO 27001; scenario modelling, control mapping	Medium/large organisations needing flexible methodology + tooling	Active
EBIOS / EBIOS RM	EBIOS-RM (SourceForge Access/ACCDB)	Microsoft Access (legacy format)	Full EBIOS RM workflows, import/export, scenario modelling	Organisations comfortable with Access database format, wanting full method support without licensing	Active
EBIOS / EBIOS RM	Agile Risk Manager	Web / client-server	Full EBIOS RM method, guided workflows, report and repository features	Medium to large orgs wanting method-aligned collaborative tooling	Active
EBIOS / EBIOS RM	Fence (Airbus Protect)	Web / on-premises	EBIOS RM implementation and compliance mapping	Enterprises or security teams needing scalable EBIOS RM tooling	Active
	eramba		GRC platform configurable for various methods	Small to medium orgs wanting unified GRC tool with method flexibility	Active

Methodology	Tool / Template	Platform / Format	What it supports	Best suited for	Status
General / GRC		Web application (open-source)			
General / GRC	CISO Assistant (Open source)	Web / SaaS / code	Supports EBIOS RM among other frameworks, mapping, compliance & tasks	Organisations wanting risk + compliance in one tool stack	Active

Risk treatment options

When managing information security risks, selecting an appropriate treatment strategy is critical. ISO/IEC 27005 identifies four primary approaches: avoidance, modification, retention, and sharing. Each option can be applied depending on the nature of the risk, the affected assets, and organisational priorities.

Applying risk treatment: Once you've mapped risks using your chosen methodology, apply the appropriate treatment strategy. Most mitigating controls in the tables above represent risk *modification* (mitigation). If a control is too costly or complex, consider risk *retention* (acceptance) or *sharing* (transfer) instead. Risk *avoidance* means choosing not to engage in the risky activity at all.

Risk avoidance

Eliminating a risk by choosing not to engage in the activity that generates it.

Example: Mobile device security

An organisation identifies that employee-owned devices (BYOD) introduce a high risk of malware or data leakage. Instead of attempting complex technical controls, the organisation may decide not to allow BYOD at all, avoiding the risk entirely. In practice, this means requiring staff to use company-issued devices with pre-configured security controls and mobile device management, ensuring consistent security posture across all endpoints.

Example: Cloud/SaaS data storage

A team considers storing highly sensitive customer records in a low-cost, public cloud environment. Given the risk of accidental exposure or misconfiguration, the organisation may choose to avoid using that cloud provider and instead use an on-premises solution with tighter access controls. This eliminates dependency on third-party security whilst accepting the operational overhead of self-hosting.

Risk modification (mitigation)

Reducing the likelihood or impact of a risk through controls or process changes.

Example: Network access

Open or misconfigured network ports may allow unauthorised access. The organisation implements firewalls, network segmentation, and intrusion detection systems, reducing both the likelihood of successful attacks and the potential impact of any breach by limiting lateral movement.

Example: Software vulnerabilities

Legacy software may be exploitable. The organisation adopts a patching schedule, automated updates, and secure configuration baselines, mitigating the risk of exploitation. Critical systems receive priority patching within 48 hours, whilst lower-priority systems follow monthly maintenance windows.

Risk retention

Accepting a risk, usually after informed assessment, because the cost of mitigation may outweigh the potential impact.

Example: Minor operational disruptions

Periodic short-term network outages may temporarily interrupt internal communications but do not significantly affect critical services. The organisation chooses to retain this risk, accepting minor downtime as tolerable given the cost of implementing fully redundant network infrastructure would exceed the business impact of occasional brief outages.

Example: Low-value hardware loss

Small peripheral devices (e.g., inexpensive mice or keyboards) may be lost or stolen occasionally. Due to the low value and minimal operational impact, the organisation accepts this risk rather than investing in asset tracking systems, RFID tags, or security cables for every peripheral device.

Risk sharing

Spreading the consequences of risk with other parties, internally or externally.

Example: Cloud storage services

Sensitive backups are stored in a third-party cloud with strong SLA guarantees and insurance for data loss. The organisation shares the risk with the provider and the insurance company, reducing its direct exposure. The contract specifies liability limits, recovery time objectives, and compensation for service failures.

Example: Vendor dependencies

A key software supplier maintains critical systems. The organisation implements contracts specifying liability, service levels, and disaster recovery obligations, sharing responsibility for availability and security. Escrow agreements ensure access to source code if the vendor ceases operations, further mitigating dependency risk.