WEBINAR RECORDED

PECB

The Role of ISO/IEC 27001, ISO 22301, and ISO 31000 in a Unified Risk Management Framework

MAY 28 | 3:00 - 4:00 PM CEST

Noor Diab

Consulting Manager and PECB Certified Platinum Trainer

#GlobalLeadingVoices

Agenda

- Unified Risk Management Framework Overview & Importance
- ISO/IEC 27001 – Information Security Management Systems (ISMS)
- ISO 22301 – Business Continuity Management Systems (BCMS)
- ISO 31000 – Risk Management Guidelines
- How They Work Together in a Unified Risk Management Framework
- Unified Risk Management Framework – Maturity Model
- Implementation Roadmap
- Implementation Tips for Unification
- Benefits of a Unified Risk Management Framework
- Next Steps & Recommendations

PECB

Unified Risk Management Framework Overview

The Unified Risk Management Framework (URMF) integrates three leading ISO standards:

- ISO 27001: Information Security Management
- ISO 22301: Business Continuity Management
- ISO 31000: Enterprise Risk Management

Together, these standards create a holistic approach to risk that covers:

- Tactical protection of information assets
- Operational continuity during disruptions
- Strategic alignment of risk with decision-making

Why Having A Unified Risk Management Framework Matters?

Organizations today face an increasingly complex and interconnected risk environment—cyberattacks, regulatory demands, operational disruptions, and stakeholder pressure are all rising.

Siloed risk management efforts often lead to gaps, redundancies, and inefficiencies. A breach in one area can expose vulnerabilities across the entire organization.

Unifying ISO 27001, 22301, and 31000 enables organizations to manage risk proactively, build resilience, and align risk with strategic goals.

Why Having A Unified Risk Management Framework Matters?

ISO 27001 focuses on **information security**, helping safeguard confidentiality, integrity, and availability of data.

ISO 22301 ensures **business continuity**, enabling organizations to recover operations during and after disruptions.

ISO 31000 provides a **risk management framework**, guiding decision-making and aligning risks with organizational goals.

🔗 When integrated, these standards create a cohesive system that:

- Eliminates duplication
- Strengthens governance
- Improves compliance and trust
- Turns risk into a source of competitive advantage

Adopting a unified risk management framework isn't just good practice—it's strategic.

PECB

Overview: How They Relate

Standard	Focus Area	Scope
ISO/IEC 27001	Information Security Risk Management	Technical and operational IS risks
ISO 22301	Business Continuity Risk Management	Operational disruption risks
ISO 31000	Enterprise-wide Risk Management	Strategic and organizational risk

🔐 ISO/IEC 27001 – Information Security Management Systems (ISMS)

ISO/IEC 27001 provides a structured approach to securing sensitive information through:

- Establishing an Information Security Management System (ISMS)
- Conducting risk assessments and applying controls (Annex A)
- Managing threats such as cyberattacks, data breaches, and insider threats

Contribution to URMF: Forms the technical backbone by protecting the confidentiality, integrity, and availability of information across the enterprise.

Enroll in the PECB Certified ISO 27001 Training Courses

PECB

🔐 ISO/IEC 27001: Risk as a Foundation

ISO 27001 aligns with ISO 31000 by applying its **principles** to the **domain of information security**.

- Clause **6.1** of ISO 27001 requires a **risk-based approach** aligned with the organization's context.
- Risk assessment and treatment are mandatory and based on **ISO 31000-style methodology**: identify → analyze → evaluate → treat.
- Leadership, continual improvement, and controls (Annex A) support a **risk-informed ISMS**.

📎 **Connection:** ISO 27001 uses ISO 31000's risk process to build its **Information Security Risk Management** engine.

Enroll in the PECB Certified ISO 27001 Training Courses

PECB

🔐 ISO/IEC 27001: Tactical Risk Control – Information Security Management

Role in the Framework:

- Focuses on **tactical risks to information assets**
- Implements **Annex A controls** to mitigate threats to confidentiality, integrity, and availability (CIA)
- Provides a **risk assessment methodology** specific to information security
- Ensures secure access control, incident response, cryptography, supplier security, etc.

Why It Matters in a Unified Approach:

- It's the **first line of defense** against digital threats
- Strengthens trust with stakeholders, customers, and regulators
- Directly supports **business continuity planning** by protecting critical systems

Enroll in the PECB Certified ISO 27001 Training Courses

PECB

ISO 22301 – Business Continuity Management Systems (BCMS)

ISO 22301 ensures the organization can continue operations in the face of unexpected events by:

- Conducting Business Impact Analysis (BIA)
- Defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Developing and testing business continuity and disaster recovery plans

Contribution to URMF: Builds operational resilience to complement information security and strategic risk efforts.

Enroll in the PECB Certified ISO 22301 Training Courses

PECB

🔄 ISO 22301: Risk for Business Continuity

ISO 22301 relies on risk and impact analysis to ensure operational resilience.

- Clause **6.1** requires the identification of **risks and opportunities** related to business continuity.
- Clause **8.2** focuses on **risk and BIA** to prioritize continuity strategies.
- ISO 22301 aligns with ISO 31000 by ensuring risk is part of **strategic resilience planning**.

📎 **Connection:** ISO 22301 adopts ISO 31000's approach to managing **operational disruption risk**, integrated with impact analysis.

🔄 ISO 22301: Operational Risk Management – Business Continuity

Role in the Framework:

- Focuses on **continuity risks** from operational disruptions (e.g., natural disasters, supply chain issues, cyberattacks)
- Defines **RTO (Recovery Time Objective)** and **RPO (Recovery Point Objective)**
- Requires a **Business Impact Analysis (BIA)** to prioritize recovery strategies
- Tests and improves continuity plans through **exercises and audits**

Why It Matters in a Unified Approach:

- Ensures that security breaches (ISO 27001 events) don’t cripple operations
- Builds resilience at the process and people levels
- Helps prove **organizational readiness** to regulators and clients

Enroll in the PECB Certified ISO 22301 Training Courses

PECB

ISO 31000 – Risk Management Guidelines

ISO 31000 outlines principles and guidelines for managing all types of risks across the organization:

- Embeds risk-based thinking into decision-making processes.
- Establishes a framework for identifying, analyzing, evaluating, and treating risks.
- Promotes leadership accountability and cross-functional governance.

Contribution to URMF: Provides the strategic foundation, aligning risk management with organizational objectives and governance structures.

ISO 31000: The Strategic Risk Framework

ISO 31000 provides the **overarching principles and framework** for managing all types of risk, regardless of context or industry. It is:

- **Guideline-based** (not certifiable)
- Focused on integrating risk into **governance, strategy, and decision-making**
- Applicable to **enterprise risk**, including financial, reputational, operational, and strategic risks

✅ **Key Elements:**

- Risk identification, analysis, and evaluation
- Risk appetite and tolerance
- Integration with leadership and culture

Enroll in the PECB Certified ISO 31000 Training Courses

PECB

ISO 31000: Strategic Risk Alignment – Enterprise Risk Management (ERM)

Role in the Framework:

- Provides a **unifying philosophy and structure** for managing all types of risk
- Encourages **integration into governance, planning, and decision-making**
- Defines principles like:
  - Value creation and protection
  - Tailored to the organization
  - Dynamic and responsive
- Applies to all departments: operations, finance, IT, HR, etc.

Why It Matters in a Unified Approach:

- Serves as the **strategic core**: risk is not a checklist—it's a mindset
- Bridges the gap between technical (27001) and operational (22301) controls
- Helps prioritize resources based on **risk appetite and tolerance**

How They Work Together in a Unified Risk Management Framework

Function	ISO 27001	ISO 22301	ISO 31000
Focus	InfoSec threats	Operational disruptions	Strategic/business risk
Key Tool	ISMS	BCMS	Risk framework
Primary Outcome	Protected data	Business continuity	Informed decision-making
Key Document	SOA, Risk Treatment Plan	BIA, BCP, DR Plan	Risk Register, Policy

Unified Risk Management Framework – Maturity Model

Maturity Level	Characteristics	Focus Area
1. Initial (Ad Hoc)	- Siloed risk practices - No formal integration of standards - Reactive risk response	Awareness of risk standards (ISO 27001/22301/31000) but no structure
2. Developing	- Some documentation of ISMS or BCMS - Basic risk assessments in place	Start aligning ISO 27001 and ISO 22301 at department or process level
3. Defined	- Documented and repeatable risk management processes - Clear roles & responsibilities	Begin cross-referencing ISO standards; apply ISO 31000 for strategic alignment
4. Integrated	- Enterprise-wide governance - Unified risk register - Shared risk treatment plans	Embed unified risk principles in operations, compliance, and IT
5. Optimized	- Real-time risk insights - Continual improvement - Risk is seen as a strategic enabler	Continuous learning, automation, and resilience planning at the core of decision-making

Implementation Roadmap

Phase 1: Initiate and Align

- Identify stakeholders and assign risk owners.
- Conduct a gap analysis across ISO 27001, 22301, and 31000.
- Define scope, objectives, and success metrics.

Phase 2: Design the Framework

- Develop integrated policies and controls.
- Align risk assessment and treatment processes.
- Create unified governance structures.

Implementation Roadmap

Phase 3: Implement and Train

- Deploy risk controls and business continuity strategies.
- Train teams across all levels.
- Integrate monitoring tools and reporting systems.

Phase 4: Monitor and Optimize

- Track KPIs and incidents.
- Review and refine framework annually.
- Benchmark against best practices.

🛠️ Implementation Tips for Unification

- **Conduct a crosswalk analysis** to align controls between ISO 27001 Annex A, ISO 22301 clauses, and ISO 31000 guidelines.
- **Establish a central risk function** that oversees InfoSec, BCMS, and ERM activities.
- **Use a unified risk register** with categories like strategic, operational, information, and continuity risk.
- **Integrate monitoring and reporting** dashboards for real-time visibility across systems.
- **Train cross-functional teams** on the unified framework—not just their area of expertise.

✓ Benefits of a Unified Risk Management Framework

- **Eliminates duplication**: No need for separate risk assessments across departments
- **Centralizes governance**: One risk committee, one reporting structure
- **Improves response time**: When events occur, communication and escalation paths are predefined
- **Reduces audit fatigue**: One coherent system that satisfies multiple standards
- **Builds risk culture**: Every employee knows their role in protecting and sustaining the organization

Next Steps & Recommendations

- Conduct a GRC Gap Assessment to evaluate current posture.
- Establish a cross-functional risk steering committee.
- Define a 12-month roadmap for integrating ISO standards.
- Secure executive sponsorship and align with strategic planning cycles.

Enroll in PECB Certified Training Courses

PECB

Upskill your career with PECB Skills

15-minute courses on:

- AI
- Cybersecurity
- Data Protection
- Auditing
- Information Security

Earn CPDs for each competency and Get Certified

PECB Skills

Q&A

THANK YOU

ndiab@aacmena.com

https://www.linkedin.com/in/noor-diab-mba-97aa6831/

Enroll in PECB Certified Training Courses