Chartered Institute of Internal Auditors

08 June 2023

Risk management

Chartered Institute of Internal Auditors

Providing assurance over risk management is a core element of the role of internal auditors. Understanding risk and risk management is also central to providing risk-based assurance.

The guidance and resources on this page should be considered as a start point to your learning journey.

IPPF links | Guidance | Additional resources | Relevant position papers

Main IPPF links

Core Principles 4. Aligns with the strategies, objectives, and risks of the organization. 9. Is insightful, proactive, and future-focused. 10. Promotes organisational improvement.	Core principles
2120 Risk Management	Implementation guidance
2210 Engagement Objectives: 2210.A1	Implementation guidance
Glossary Risk | the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood Risk appetite | the level of risk that an organisation is willing to accept. Risk management | a process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's	

objectives

Guidance A-Z

Chartered IIA		
Basics of risk management (2020)	Standards for managing risk (2014)	Risk maturity assessment (2019)
Risk appetite - concept and theory (2019)	Risk appetite - the board's role (2019)	Risk appetite - the role of IA (2019)
Assessment of emerging risk (2020)	Risk identification (2021)	Reporting on risk
Quantitative Risk Appetite (2022)		
IIA Global		
Risk management process (2010)	Risk management - ISO 31000 (2010)	The role of IA in ERM (2009)
Creating maturity models (2013)	Auditing risk culture - a practical guide (IIA Australia) (2021)	Agile risk management (IIA Australia) (2021)
GRC non-financial risk | risk appetite (2023)	GRC non-financial risk | quantifying (2023)	Internal Audit and Risk Management (IIA Australia) (2023)

Additional resources

Codes of practice | Financial services, private and third sector
FRC | Guidance on Risk Management, Internal Control and Related Financial and Business Reporting
IRM | Institute of Risk Management guides and insights

Need help to find what you are looking for? ask the resources team

Risk Standards and Frameworks

ISO 31000 is widely accepted although there is no formally recognised definition or approach to risk management and enterprise risk management. The reference list below (some require a purchase) provide different options for categorising risk to help identify, assess and evaluate it.

- Institute of Risk Management/AIRMIC/Alarm - A Risk Management Standard
- COSO (2011) Embracing ERM: getting started
- COSO (2011) Developing key risk indicators
- HM Treasury Guidance Orange Book: Management of Risk - Principles and Concepts
- HSE - Principles of Sensible Risk Management
- ISO/FDIS 31000 Risk Management - Principles and guidelines
- AS/NZS ISO 31000: 2009 Risk Management

Chartered IIA Position Papers

The role of internal audit in enterprise-wide risk management