

The 6 frameworks behind leading risk programs

BY SMARTSUITE



1

ISO 31000:2018

GUIDELINE

Guidelines for managing any kind of risk in any organization, built on principles, a management framework and a process from context to treatment and review.

Voluntary

2

COSO ERM 2017

FRAMEWORK

An enterprise risk framework for boards, executives and auditors, built on five components and 20 principles that integrate risk with strategy and performance.

Voluntary

3

NIST RMF, SP 800-37 Rev. 2

FRAMEWORK

The US federal process for system security and privacy risk in seven steps, required of federal agencies under FISMA and OMB A-130 and of contractors by contract.

Mandatory



COBIT 2019

FRAMEWORK

ISACA's framework for governing enterprise IT, built on 40 governance and management objectives in five domains and used by enterprises, auditors and IT leaders.

Voluntary

5

ISO/IEC 27005:2022

GUIDANCE

Guidance on information security risk for teams running an ISO/IEC 27001 management system, applying the ISO 31000 process to the ISMS; not certifiable itself.

Voluntary

6

Basel III

STANDARD

The Basel Committee's standard on bank capital, liquidity and leverage, built on three pillars and applied to internationally active banks through national rules.

Mandatory

The 6 frameworks behind leading risk programs

SOURCES: ISO 31000:2018 · COSO ERM 2017, INTEGRATING WITH STRATEGY AND PERFORMANCE · NIST SP 800-37 REV. 2, 2018 · ISACA COBIT 2019 · ISO/IEC 27005:2022 · BCBS BASEL III, 2017

smartsuite.ai/frameworks

