

OCEG GRC Capability Model 3.5 (Red Book)

OCEG's GRC Capability Model, the Red Book, is the open-source standard that integrates governance, risk, audit, compliance, ethics, and IT into one approach to Principled Performance.



What it is

The GRC Capability Model, known as the OCEG Red Book, is OCEG's open-source standard for integrating governance, risk management, and compliance into a single organizational capability. OCEG describes version 3.5 as the first and only open-source standard that integrates the sub-disciplines of governance, strategy, risk, audit, compliance, ethics and culture, and IT into a unified approach, with simplified, clarified, and augmented content.

OCEG is a global nonprofit founded in 2002 with more than 225,000 members in over 180 countries. It publishes the model free of charge in a general version, with a premium edition of additional tools available to its All Access Pass holders, and the model underpins OCEG's GRC Professional certification and its definition of Principled Performance, the reliable achievement of objectives while addressing uncertainty and acting with integrity.

At a glance

PUBLISHER OCEG (Open Compliance and Ethics Group)	TYPE Framework	VERSION 3.5
EFFECTIVE Version 3.5 (current edition)	DOMAIN Risk Management	FAMILY Other
REGION Global (OCEG)	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: <https://www.oceg.org/grc-capability-model-red-book/>

Why it matters

- **Unify vocabulary across disciplines** Give governance, risk, compliance, audit, and IT teams one set of terms and a common map of components and elements.
- **Define common information requirements** Standardize what the organization needs to know about objectives, obligations, risks, controls, and events so it can be captured once and reused.
- **Standardize core practices** Apply consistent practices for policies, training, controls, and monitoring rather than a different approach in every function.
- **Design or assess a GRC program** Use the elements and practices as a checklist for building a program or benchmarking an existing one.

How SmartSuite supports OCEG Red Book 3.5

GRC Capability Model Library

Hold the LEARN, ALIGN, PERFORM, and REVIEW components with their elements and practices as structured requirements linked to your program.

Ownership, Cadence, and Accountability

Assign owners to each element, set review cycles, and track maturity assessments against the model over time.

Evidence Collection and Audit Trail

Attach policies, training records, control results, and review outputs to the practices they evidence, with timestamps and reviewers.

Program Assessment and Testing

Run gap assessments against the elements and practices, document findings, and track remediation to closure.

Risk, Obligation, and Objective Alignment

Link objectives, obligations, risks, and controls so that ALIGN and PERFORM activities trace back to what the organization is trying to achieve.

Integrated GRC Reporting

Produce dashboards by component, element, and business unit that show program maturity, open gaps, and review status for leadership and the board.

Common framework mappings

ISO 31000:2018

COSO ERM 2017

COSO IC 2013

COBIT 2019

IIA Three Lines Model

USSG §8B2.1

DOJ ECCP

ISO 27001:2022

NIST CSF 2.0

ISO 42001

Official resources

OCEG: GRC Capability Model 3.5 (Red Book)

The publisher page for the model, with the free version download and the description of the LEARN, ALIGN, PERFORM, and REVIEW components.

oceg.org/grc-capability-model-red-book

OCEG: Principled Performance

OCEG's definition of Principled Performance, the reliable achievement of objectives while addressing uncertainty and acting with integrity.

oceg.org/principled-performance

About OCEG

The global nonprofit founded in 2002 that publishes the GRC Capability Model and runs the GRC Professional certification.

oceg.org/about

Frequently asked questions

What is the OCEG Red Book?

The Red Book is OCEG's GRC Capability Model, an open-source standard for integrating governance, strategy, risk, audit, compliance, ethics and culture, and IT into one organizational capability. Version 3.5 is the current edition.

What are the four components of the GRC Capability Model?

LEARN about the organization's context, culture, and key stakeholders; ALIGN strategy with objectives and actions with strategy; PERFORM actions that promote and reward desirable conduct and prevent and remediate undesirable conduct; and REVIEW the design and operating effectiveness of the strategy and actions.

What is Principled Performance?

OCEG defines Principled Performance as the reliable achievement of objectives while addressing uncertainty and acting with integrity. The Red Book exists to help organizations achieve it.

Is the Red Book free?

OCEG offers a free version of the GRC Capability Model for general download. A premium edition with additional tools and techniques is available to OCEG All Access Pass holders.

Is the Red Book a certification standard?

No. It is a capability model that organizations use to design or assess their GRC programs. OCEG uses it as the body of knowledge for its GRC Professional certification, but organizations are not certified against it.

How does the Red Book relate to ISO 31000 or COSO?

The Red Book integrates rather than replaces them. ISO 31000 and COSO ERM describe risk management, COSO describes internal control, and the Red Book shows how those and other disciplines fit into one GRC capability with shared vocabulary and information.

How does SmartSuite support the GRC Capability Model?

SmartSuite holds the components, elements, and practices as a requirement set linked to objectives, obligations, risks, controls, policies, training, incidents, and reviews. GRC teams use it to run gap assessments against the model, evidence each practice, and report program maturity to leadership.

License included / downloadable: No OCEG publishes the Red Book free of charge in a general version, with a premium edition for All Access Pass holders; the text is obtained from OCEG and is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/oceg-grc-capability-model-red-book