SmartSuite

Framework / Risk Management / Other

OCEG GRC Capability Model 3.5 (Red Book)

OCEG's Red Book (GRC Capability Model 3.5) is the open-source standard integrating governance, risk, audit, compliance, ethics and IT through its LEARN, ALIGN, PERFORM and REVIEW components.



What it is

The GRC Capability Model, known as the OCEG Red Book, is the open-source standard from OCEG (Open Compliance and Ethics Group) that teaches GRC professionals how to achieve Principled Performance, which OCEG defines as the reliable achievement of objectives while addressing uncertainty and acting with integrity. OCEG, the global nonprofit that created the terms GRC and Principled Performance, released the first Red Book in 2004 and the current version 3.5 in 2023, on its 20th anniversary, to its 130,000 members and to the public. OCEG describes the model 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.

OCEG studied more than 500 organizations with a panel of more than 300 experts to document the practices in the model. The Red Book unifies vocabulary across disciplines, defines common components and elements, defines common information requirements, standardizes practices for activities such as policies and training, and identifies communication for everyone involved. It is published in three parts, GRC Concepts, GRC Capabilities and GRC Glossary, with a Tools and Techniques Appendix of 90 resources in the premium edition for All Access Pass holders; a free version is available for download from OCEG.

At a glance

PUBLISHER OCEG (Open Compliance and Ethics Group)	TYPE Framework	VERSION 3.5 (2023)
EFFECTIVE 2023	DOMAIN Risk Management	FAMILY Other
REGION Global (OCEG)	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

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

Why it matters

- **Unify vocabulary across disciplines** Give governance, risk, compliance, audit, ethics and IT teams one set of terms, with Part III, the GRC Glossary, as the alphabetical reference for untangling terminology across departments.
- **Define common components and elements** Provide the four components, LEARN, ALIGN, PERFORM and REVIEW, and their elements as the common map that any GRC program can be built from or assessed against.
- **Define common information requirements** Standardize what the organization needs to know about its context, objectives, obligations, risks and actions so the same information serves every discipline.
- **Standardize core practices** Apply consistent practices for recurring activities such as policies and training, rather than a different approach in every function.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OCEG Red Book 3.5

Capability Inventory by Component

Record the organization's GRC capabilities under LEARN, ALIGN, PERFORM and REVIEW, each with an owner, a maturity rating and the Part II elements it covers, so the program can be assessed against the model in one place.

LEARN: Context and Stakeholders

Use Enterprise Risk Management to keep the external and internal context, culture indicators and key stakeholders that inform objectives, strategy and actions, reviewed on a set cadence.

ALIGN: Objectives and Obligations

Link objectives to the values, opportunities, threats and requirements that decisions must address, and to the risks and obligations held in Enterprise Risk Management and Compliance Management.

PERFORM: Policies, Training and Controls

Use Compliance Management to centralize the policies, training records, controls and evidence through which the organization promotes desirable things, prevents and remediates undesirable things, and detects events.

REVIEW: Audits and Improvement

Use Internal Audit Management to plan reviews of the design and operating effectiveness of strategy and actions, record findings and track remediation to closure.

Shared Vocabulary and Reporting

Hold the Part III Glossary terms the program uses as a shared reference and report capability maturity, open gaps and review status by component to 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 · ISO 37301:2021

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 are the four components of the GRC Capability Model?

LEARN about the organization's context, culture and key stakeholders to inform objectives, strategy and actions; ALIGN strategy with objectives and actions with strategy, using decision-making that addresses values, opportunities, threats and requirements; PERFORM actions that promote and reward desirable things, prevent and remediate undesirable things, and detect when something happens as soon as possible; and REVIEW the design and operating effectiveness of the strategy and actions and the ongoing appropriateness of objectives. OCEG says these components have stayed true to the core framework it has taught for more than 20 years.

What is Principled Performance, and how does OCEG define GRC?

Principled Performance is the reliable achievement of objectives while addressing uncertainty and acting with integrity. OCEG defines GRC as the integrated collection of capabilities that enable an organization to achieve Principled Performance, and the Red Book teaches GRC professionals how to get there. OCEG created both terms.

 Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed in version 3.5 of the Red Book?

OCEG released version 3.5 in 2023 on its 20th anniversary, with three objectives: simplifying, clarifying and augmenting the model. Content was added, edited and removed to make the document easier to navigate, the GRC Concepts were updated, and new concepts, models and practices common in the GRC ecosystem were introduced. The four components were unchanged, and a premium edition added a Tools and Techniques Appendix with 90 resources.

Is the Red Book free, and does OCEG certify organizations against it?

OCEG offers a free version of the GRC Capability Model 3.5 for download from its website. A special premium edition, with the 90-resource Tools and Techniques Appendix, is available in English to OCEG All Access Pass holders. OCEG certifies people through its GRC Professional (GRCP) program; the public pages describe no certification of organizations against the Red Book.

How is the Red Book organized, and how should it be read?

It has three parts: Part I GRC Concepts, Part II GRC Capabilities and Part III GRC Glossary, with the Tools and Techniques Appendix in the premium edition. OCEG suggests reading the Introduction first, then GRC Concepts, consulting the Glossary for consistent vocabulary, working through GRC Capabilities to identify improvements, and finishing with Tools and Techniques. OCEG recommends pairing the model with narrower frameworks from ISO, COSO, ISACA, IIA or NIST to jump-start a program.

License included / downloadable: No OCEG publishes the GRC Capability Model 3.5 in a free version for download from its website and 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

© 2026 SmartSuite Inc. All rights reserved.