

OCEG® CORPORATE COMPLIANCE MATURITY MODEL™

	Level 1 Unformed	Level 2 Reactive	Level 3 Adaptive	Level 4 Proactive	Level 5 Infused
Awareness (external & internal)¹	<ul style="list-style-type: none"> Organization is unaware of the boundaries² to which it is subject and thus unable to promulgate awareness 	<ul style="list-style-type: none"> Organization is unsure of whether it knows all of its boundaries and is inconsistent in its efforts to promulgate awareness 	<ul style="list-style-type: none"> Organization believes that it is aware of its boundaries and tries to promulgate the understanding of its boundaries to process owners 	<ul style="list-style-type: none"> Organization proactively determines its boundaries and plans markets/ services in light of those boundaries and promulgates understanding of its boundaries to all people who are impacted by or part of the process of execution 	<ul style="list-style-type: none"> Organization proactively influences the scope and nature of boundaries to which it chooses to be subject and incorporates the boundaries execution into the business rules
Structure & Accountability³	<ul style="list-style-type: none"> Structure for compliance execution is diffused and isolated Structure for independent oversight does not exist Accountability not delineated 	<ul style="list-style-type: none"> Structure for compliance execution is discrete but isolated Structure for oversight exists but is not independent Accountability delineated at an operational level 	<ul style="list-style-type: none"> Structure for compliance execution is distributed and coordinated Structure for compliance oversight includes independent perspective Accountability delineated at strategic and operational levels 	<ul style="list-style-type: none"> Structure for compliance execution is distributed and aligned Structure for compliance oversight is controlled by independent perspective Accountability delineated at oversight, strategic and operational levels 	<ul style="list-style-type: none"> Structure for compliance execution is infused into organizational structure Structure for compliance oversight presents wholly independent perspective Accountability delineated at all levels (leadership/champion, oversight, strategic and operational)

¹ Degree to which the organization anticipates and influences the boundaries to which it is subject and communicates or incorporates compliance into the rules by which it runs the organization.

² Limits imposed upon the conduct of an organization and its employees either voluntarily (values, standards, internal policies) and by mandate (laws and regulations)

³ Degree to which the structure of the organization sustains and promotes accountability for compliance.

OCEG® CORPORATE COMPLIANCE MATURITY MODEL™

Culture & Consistency⁴	<ul style="list-style-type: none"> • Organization is indifferent to compliance • Stakeholders perceive hypocrisy in the organization's statements about commitment to compliance • Organization routinely finds out about non-compliance from official complaints rather than audit, inquiries or internal reporting • Discipline is inconsistently applied to employees at similar levels in the organization 	<ul style="list-style-type: none"> • Organization is concerned about fixing non-compliance • Stakeholders perceive inconsistency between the organization's statements and execution of compliance • Stakeholders usually report violations and misconduct but do not seek out preventative advice • Discipline may not be consistently applied across positions 	<ul style="list-style-type: none"> • Organization continuously monitors for compliance • Employees perceive consistency between the organization's statements and execution of compliance • Stakeholders are consistent in reporting violations and misconduct, but may not consistently seek preventive advice • Discipline is consistently applied without regard to position 	<ul style="list-style-type: none"> • Organization plans controls to sustain compliance • Employees share the organization's commitment to compliance in work processes • Stakeholders are comfortable in both seeking advice and reporting violations and misconduct • Discipline is consistently applied with those in positions of authority disciplined in a manner that communicates higher expectations 	<ul style="list-style-type: none"> • Organization incorporates compliance controls into processes as they are designed and changed • Employees share and extend the organization's commitment to compliance beyond work processes • Stakeholders are comfortable in providing appropriate advice to one another and preventing violations and misconduct as opportunities present themselves • Discipline is anticipated such that it serves as a deterrent
Processes/ Controls Automation & Integration⁵	<ul style="list-style-type: none"> • Unaware of whether compliance controls and processes contain gaps • No attempt to standardize similar processes across the organization 	<ul style="list-style-type: none"> • Aware of compliance controls and processes gaps as they appear through failures • Little, if any, attempt to standardize similar processes across the organization 	<ul style="list-style-type: none"> • Periodically test compliance controls and processes for gaps and weaknesses before they appear through failures • To the extent that processes are identified as similar, they are standardized across parts of the organization, but not the enterprise 	<ul style="list-style-type: none"> • Continuously assess compliance controls and processes gaps to prevent compliance failures • Organization affirmatively evaluates where similar processes exist and attempt to standardize across the enterprise 	<ul style="list-style-type: none"> • Proactively plan compliance controls and processes to avoid gaps and prevent compliance failures • Organization affirmatively standardizes similar processes across the enterprise

⁴ Degree to which the actions and practices of the organization are, and are perceived to be, highly committed to compliance and integrity through embedding compliance into processes and applying consistent discipline.

⁵ Degree to which processes and controls for compliance are integrated, standardized, and automated to avoid control gaps and compliance failures.

OCEG® CORPORATE COMPLIANCE MATURITY MODEL™

Processes/ Controls Automation & Integration⁶ (cont'd)	<ul style="list-style-type: none"> • Compliance processes operate without regard to organizational business processes • Heavily, if not exclusively, rely on manual compliance processes and controls 	<ul style="list-style-type: none"> • Compliance controls and processes are distinct from and inconsistent with organizational business processes • Environment has an ad hoc mix of manual and automated compliance processes and controls 	<ul style="list-style-type: none"> • Compliance controls and processes are distinct from but consistent with organizational business processes • Compliance processes and controls are tactically automated but not strategically automated 	<ul style="list-style-type: none"> • Compliance controls are distinct from and coordinated with compliance and organizational business processes • Compliance processes and controls are automated without regard to flexibility and adaptability 	<ul style="list-style-type: none"> • Compliance processes are indistinct from and infused into organizational business processes • Compliance processes and controls are optimized through automation to be flexible and adaptable
Measurement⁷	<ul style="list-style-type: none"> • Metrics and measurement methods at enterprise, division, group and individual levels are not established 	<ul style="list-style-type: none"> • Metrics are established at some of the levels (enterprise, division, group and individual) but not all levels • Measurement methods are not consistent at each level 	<ul style="list-style-type: none"> • Metrics are established at each of the levels (enterprise, division, group and individual) but not aligned • Measurement methods are consistent at each level but not integrated across levels 	<ul style="list-style-type: none"> • Metrics are established at each of the levels (enterprise, division, group and individual), aligned across levels but not integrated with performance metrics • Measurement methods are consistent at each level and integrated across levels 	<ul style="list-style-type: none"> • Metrics are established at each of the levels (enterprise, division, group and individual), aligned across levels and integrated with performance metrics • Measurement methods are consistent at each level, integrated across levels, and consistent with performance metric methods

⁶ Degree to which processes and controls for compliance are integrated, standardized, and automated to avoid control gaps and compliance failures.

⁷ Degree to which metrics and measurements designed to enable and sustain compliance are established and consistently measured. Degree to which such metrics are susceptible of integrated/aggregated reporting and incorporated into performance measures.

OCEG® CORPORATE COMPLIANCE MATURITY MODEL™

Technology⁸	<ul style="list-style-type: none"> • Few if any IT resources are allocated to GRC. • Ad hoc approach to technology • Little if any technology in place • Information is not available let alone shared • New requirements are not easily addressed • Success is not measured 	<p>See some of the interdependencies between governance, risk and compliance; but do not provide a common platform for GRC.</p> <ul style="list-style-type: none"> • Tactical, siloed approach to technology • Silos have systems in place w/o integration • Information is not shared between silos • New requirements within a silo are addressed without considering other areas • Measurement is difficult 	<p>See the need to integrate GRC systems to provide better information and results; a common GRC platform and approach is in place.</p> <ul style="list-style-type: none"> • Unified approach to GRC • Silos have some integration but are broken down • Information is shared across the enterprise • New requirements are rapidly addressed by a common platform • GRC benefits are measured 	<p>Align and leverage the GRC platform to realize not only GRC benefits; but also general business benefits such as growth, profitability and asset utilization.</p> <ul style="list-style-type: none"> • Strategic approach to aligning GRC with the overall business • Silos are nonexistent • Technology is consolidated wherever possible • Business benefits are measured 	<p>Have language and set of metrics to continuously improve the platform year over year.</p> <ul style="list-style-type: none"> • Strategic approach to optimize the GRC platform • GRC technology and non-GRC technology are almost indistinguishable • GRC is “baked into” all business systems • Business benefits are measured and improved year over year
-------------------------------	--	---	---	--	--

⁸ Degree to which an integrated technology platform is adopted, extensible to a variety of compliance risk areas, and optimized across the organization.