OCEG®

DRIVING PRINCIPLED PERFORMANCE®

OCEG Red Book GRC Capability Model™ version 2.1

The continuing work of OCEG is made possible in part by the generosity of the following organizations. Please join us in thanking these leading organizations and their representatives:

2012 Sponsoring Members:

Charter Members

Leadership Council Members

OCEG Red Book
GRC Capability Model™

Achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance

Version 2.1

Principal Authors
Scott L. Mitchell, Chair
Carole Stern Switzer, Esq., President

NOTICE: THIS IS NOT LEGAL or PROFESSIONAL ADVICE

This Document, including its appendices, is provided for general information purposes only. The application of law to individual circumstances must be addressed for each unique situation. In preparing and providing this document, neither OCEG nor any of its Contributors are engaged in rendering legal, tax or any other professional advice or services. OCEG and its Contributors do not purport to identify all conceivable compliance requirements or recommended controls. It is the responsibility of each organization to understand which legal; accounting and other compliance requirements apply to its activities. Users of this document are advised to seek specific legal advice by contacting members of relevant and applicable bar associations regarding any specific legal issues. Using the document or any part herein does not create a lawyer-client relationship or any other type of professional relationship.

While OCEG and its Contributors attempt to provide accurate, complete and up to date content, errors or omissions may occur. This document is offered AS IS, WHERE IS. Neither OCEG nor any Contributor makes any representations or warranties regarding the completeness, accuracy or timeliness of the contents, and each disclaims all implied warranties (including merchantability, fitness for a particular purpose and non-infringement) and all liability for any loss, damage or claim, whether due to an error or omission or otherwise.

To the fullest extent permitted by applicable law, neither OCEG nor the Contributors (including their officers, directors, partners and employees, and their affiliates, related entities and successors and assigns) warrant or guarantee the quality, accuracy or completeness of any information on this document. Neither OCEG nor its Contributors shall be liable for any damages or costs, including any direct, consequential, incidental, indirect, punitive or special damages (including loss of profits, data, business or good will) in connection with use of this product, whether or not liability is based on breach of contract, tort, strict liability, breach of warranty, failure of essential purpose or otherwise, and even if a party is advised of the likelihood of such damages.

This document or custom report versions of this document may contain links to third party websites. Monitoring the vast information disseminated and accessible through those links is beyond our resources and neither OCEG nor any Contributors attempt to do so. This Document provides links for convenience only and nothing herein shall constitute an endorsement of the information contained in linked web sites nor guarantee its accuracy, timeliness, or fitness for a particular purpose. OCEG and its Contributors disclaim all warranties and liability for the content of any such other sources.

TABLE OF CONTENTS

RED BOOK LEADERSHIP

OCEG enjoys the expertise of an elite group of individuals and organizations who provide their invaluable wisdom and advice as we pursue serving the knowledge and resource needs of GRC and related professionals.

Please join us in thanking these leading organizations and their representatives who have contributed as leadership council organizations of OCEG during various stages of development of the GRC Capability Model (v.1 – v. 2.1), which is commonly referred to as the Red Book.

Aon
Approva
Archer Daniels Midland
Axentis
Baker Hughes
Baker Tilly Colombia
Bwise
CA, Inc
Cisco Systems
Compliance Initiatives
Corporate Integrity
Dell
Deloitte
Dow Chemical Company
Ernst & Young
EthicsPoint
Freddie Mac
Gevity HR
Global Compliance Services
Grant Thornton
Interactive Alchemy
Kalorama Partners
Kraft Foods
Levick Strategic Marketing
Littler Mendelson
McAfee
Marsh
MetricStream
Microsoft
OpenPages
Oracle
PETCO
PricewaterhouseCoopers
Qwest
Raytheon
RSA
SAI Global
SAP
SAS
Staples
Sun Microsystems
Temple-Inland
Thomson Reuters
Toyota Motor Sales, U.S.A
UHY Advisors
Unilever
U.S. Cellular
Ventura Foods
Walmart
XPLANE

Red Book 2.0 Initiative Leadership

A select group of individuals, representing cross-disciplinary, cross-industry, and trans-global perspectives, committed substantial time and expertise to shaping the OCEG GRC Capability Model™ (the Red Book). We would like to take this opportunity to thank each of our contributors. OCEG accepted the input of each of the individuals in the following roles as individual contributions, recognizing that their views and perspectives may not represent official views of the organizations with which they were affiliated at the time of their contribution.

Red Book 2.0 Steering Committee Co-Chairs

Mr. Larry Harrington, CPA, CIA

Vice President, Internal Audit, Raytheon Company

(Professional Issues Committee – IIA)

Mr. Brad Jewett

Vice President, Enterprise Risk Management, BMC Software

(Formerly during this process - Director, Enterprise Risk Management, Microsoft Corporation)

Mr. Scott Roney, Esq.,

Vice President, Compliance and Ethics, Archer Daniels Midland Company

Mr. John Steer

Partner, Allenbaugh Samini LLP

(Vice Chair US Sentencing Commission, 1999-2007)

We would like to thank the OCEG executives and staff members (present and past) who helped to make Red Book 2.1 possible, especially:

Stephane Legay

Jeanna Mitchell

We appreciate all that you do to support our members and our work.

With our thanks, Carole and Scott

Red Book 2.0 Steering Committee

Steering Committee members attended several drafting and review sessions, and individually prepared comments on each draft of the Red Book document throughout the development process. They are identified with their roles and companies as of the time of their participation.

Mr. Michael Horowitz — Partner, Cadwalader Wickersham & Taft LLP and U.S. Sentencing Commission Member

Mr. Eric Moorehead, Assistant General Counsel, United States Sentencing Commission

Mr. Richard Steinberg – CEO, Steinberg Governance Advisors, Inc. (Author, COSO Internal Control & COSO ERM and formerly corporate governance leader of PricewaterhouseCoopers)

Mr. Carlo di Florio - Partner, Advisory, PricewaterhouseCoopers

Mr. Lee Dittmar – Principal, Deloitte

Mr. Randy Nornes – Executive Vice President, Aon Corporation

Mr. Trent Gazzaway - Managing Partner of Corporate Governance, Grant Thornton LLP

Mr. Norman Comstock, CIA, CISA, CISSP, CCSA, CSOXP - Managing Director, UHY Advisors TX LLC

Mr. Gaurav Kapoor – CFO and General Manager, MetricStream

Mr. Jose Tabuena - VP Integrity and Compliance/Corporate Secretary, MedicalEdge Healthcare Group, Inc.

Mr. Mark S. Beasley - Deloitte Professor of Enterprise Risk Management and ERM Initiative Director Professor of Accounting College of Management - COSO Board Member

Mr. David B. Crawford, CIA, CCSA - Audit Manager Emeritus, System Audit Office, The University of Texas System

Mr. Ronald Berenbeim -Director of Ethics Research, The Conference Board

Mr. Earnie Broughton - Executive Director/Ethics Program Coordinator, USAA

Mr. David Koenig - Past Chairman of The Board of Directors, PRMIA

Ms. Melissa Lea - Chief Global Compliance Officer, SAP AG

Mr. Paul Liebman - Chief Compliance Counsel, Dell Corporation

Mr. Dave Ferguson - VP of Operations Compliance, Wal-Mart Stores, Inc.

Mr. Pete Fahrenthold -Managing Director Risk Management, Continental Airlines

Mr. Eugene Fredriksen – CISO, Tyco International

Mr. Abdel Krim Hamou-Lhadj, Manager, Regulatory Compliance & Quality Assurance Cognos Products – IBM

Mr. David Heller, VP Risk and Chief Ethics and Compliance Officer, Qwest Communications

Mr. Allen Stewart - Managing Director Ethics, Duke Energy

Ms. Nan Stout - Vice President, Business Ethics, Staples

Mr. Kendall Tieck - Audit Director, Business Groups,-Microsoft

Ms. Shirley Yoshida - SVP, Internal Audit, Macy's Inc.

Mr. Chet Young - Divisional VP Audit Compliance and Loss Prevention, Walgreen Co

Mr. Brian Chevlin - Deputy General Counsel, Unilever

Ms. Mary Doyle - Ethics & Compliance, Intel Corporation

Ms. Kathleen Edmond - Chief Ethics Officer, Best Buy

Mr. Rick Kulevich - Sr. Director, Ethics and Compliance, CDW

Mr. Jay Martin - VP CCO & Sr Deputy Gen Counsel, Baker Hughes

Mr. Xunlez Nunez - Ethics and Compliance Business Consultant, Baker Hughes

Ms. Haydee Olinger - VP Chief Compliance Officer, McDonalds

Mr. Paul C Palmes – President, Business Standards Architects, Inc.

Ms. Xenia Ley Parker - Senior Director, Marsh & McLennan Cos

Ms. Tian Peng, CIA - Audit Manager, China National Offshore Oil Corporation Ltd-

Ms. Deborah Penza - VP Corporate Compliance, Elan Pharmaceuticals, Inc.

Ms. Janet Sheiner, Director, Ethics & Compliance, PETCO

Ms. Faye Stallings - Vice President Audit & Ethics, El Paso Corporation

Mr. Michael Rasmussen - President, Corporate Integrity

Dr. Parveen Gupta, LL.B., Ph.D.-Professor of Accounting and Chairman Accounting - Lehigh University

Prof. Mr. Sanjay Anand - Chairperson, Sox Institute, G R C Group

Mr. Robert Chastain - General Council-VP Compliance-Chief Security Officer, Pepperweed Consulting LLC

Mr. Andrew Dahle, CPA, CIA, CISA, CFE – Partner, Advisory, PricewaterhouseCoopers LLP

Ms. Deb Davis - Executive Vice President, Great River Compliance & Advisory Services LLC

Mr. Kip Ebel, CFE - Senior Manager, Health Sciences, Fraud Investigations & Dispute Services, Ernst & Young LLP

Mr. David Gebler – President, Skout Group, LLC

Mr. Allan Goldstein - Retired Managing Director Risk Advisory, ARGUS Holdings Ltd

Mr. Steven Helwig - Director Professional Services, Compliance Spectrum

Mr. David Hess – Director, Internal Audit and Controls, Jefferson Wells International, Inc.

Ms. Sara A. Liftman - Senior Manager, AABS Advisory Services, Ernst & Young LLP

Mr. Worth MacMurray, Esq. – Principal, Compliance Initiatives

Mr. Bruce McCuaig - Director Solution Marketing, SAP Governance Risk and Compliance Solutions

Ms. Andrea McElroy - Sr. Director Compliance System Integrity, Golden Living

Mr. Robert N. Merrill, JD – Senior Manager, Fraud Investigation and Dispute Services, Ernst & Young LLP

Mr. Tom Wardell – Partner, McKenna Long & Aldridge LLP

Mr. F. Richard Ricketts, JD -Director of Finance, Workforce Development Council Snohomish County

Ms. Carole Basri - President, The Corporate Lawyering Group LLC

Task Force and Review Panel

Task Force members attended online review meetings and both Task Force and Red Book Review Panel contributors provided their focused review of the Red Book 2.0 drafts throughout the process. They are identified with their role and company as of the time of their participation.

Task Force Members

Mr. Ted Banks – Compliance & Competition Consultants, LLC (formerly Chief Counsel Global Compliance, Kraft Foods)

Mr. Dinesh O. Bareja - Program Director, CSI eSecure, Inc. (Canada)

Mr. Hadi Beski – PM, Hashem Co

Mr. Matthew Blake – Analyst, Ikobo

Mr. Wayne Brody - CCO VP Legal Affairs, Arrow Electronics, Inc

Mr. Mark Carey - Partner, Deloitte & Touche LLP

Mr. Glenn Carleton - Director National Consulting, RSM McGladrey

Mr. Nick Ciancio - Vice President Marketing, Global Compliance

Mr. Paul Cogswell – Vice President ERC, Comdata Network, Inc.

Mr. Brett Curran – Vice President GRC and Regulatory Practices, Axentis LLC

Mr. Ronald De Boer - Senior Sales Executive GRC, SAP Nederland (Netherlands)

Mr. Stephen Donovan - Chief Counsel - International Compliance, International Paper Company

Ms. Christine Doyle - SVP Senior Compliance Director, Bank of America

Mr. Rocky Dwyer, PhD, CMA – Principal, Chief Review Services, National Defence (Canada)

Ms. Catherine Finamore Henry, CIA – Ethics Officer and VP, Business Development, SmartPros Legal & Ethics, Ltd.

Mr. John Fons, Esq. – Attorney, John Fons Solo Practice

Mr. Christopher Fox – Senior Principal Manager, Governance Risk and Compliance, CA

Mr. Arnold Galit - VP Risk and Compliance, Ikobo, Inc

Mr. Jason Garelli - Head of Operational Risk and Sox Management, Och-Ziff Capital Management

Mr. Joe Grettenberger - Compliance Solutions Integration Manager, Quest Software

Mr. Eric Hespenheide - Internal Audit Services – Global Leader, Audit and Enterprise risk Services, Deloitte & Touche LLP

Mr. Eric Hong – Manager, Security Consulting, A3 Security (Republic of Korea)

Mr. Jawaid Iqbal - System Analyst, Saudi Pan Gulf (Saudi Arabia)

Mr. Dennis Irwin, CIA - Internal Audit Manager, Health Care Practice, Wipfli LLP

Mr. Bob Jacobson - Managing Director National Consulting, RSM McGladrey

Ms. Colleen Lyons, MBE, CCEP – Principal, Ethical Stability™

Mr. John MacKessy – President & CEO, Prism Risk Advisors, Inc.

Mr. Eamonn Maguire - Managing Director, PricewaterhouseCoopers LLP

Mr. Paul McGreal - Prof of Law, Southern Illinois University School of Law

Mr. Ashish Mehta - IT Manager, BP (United Arab Emerates)

Mr. Jeffrey Miller - Chief Compliance Officer, Synthes

Mr. Bruce R. Millman - Shareholder, Littler

Mr. James O'Keeffe - Consulting Manager, Sycor Americas

Mr. Brin Odell - Director - Client Services, EthicsPoint

Ms. Mary Pruitt - Associate Director Firm Compliance, Americas Office of Ethics and Compliance, Ernst & Young

Mr. Azwar Ritonga - OSS Eng, TELKOM (Indonesia)

Mr. David Mace Roberts - Vice President and Gen Counsel, Elbit Systems of America LLC

Mr. Roy Robinson - Vice President Communications Education, Archer Daniels Midland Company

Mr. Sayed Sadjady - Partner, PricewaterhouseCoopers LLP

Mr. Suvendu Samantaray - Business Consultant, Infosys Consulting

Mr. William Shenkir, Ph.D., CPA - William Stamps Farish Prof Emeritus, McIntire School of Commerce, University of Virginia

Mr. Ratan Sonti - Software Engineer, SAP

Ms. Andrea Spudich, CCEP – Principal, The Responsible Leader Group

Ms. Darla Stanley – Wal-mart Stores, Inc.

Ms. PJ Sullivan - Sr Technical Mgr-IT Compliance, Freight System, FedEx Corporation

Mr. Lou Tinto - Engagement Manager Technology Risk Management, Jefferson Wells

Ms. Patricia Towers - Senior Manager, Global Ethics & Compliance, Procter & Gamble

Ms. Juven Zeng – Consultant, Smartdot Tech

Review Panel Members

Mr. Daoud Abu-Joudom, MBA, CISA, CISM – VP, Head of IT Audit, Group Internal Audit, Arab Bank (Jordan)

Mr. John Adamsons – Coordinator, WHO

Mr. Mani Akella - Director, Technology, Consultantgurus

Ms. Julia Allen - Senior Researcher, Carnegie Mellon University

Ms. Sam Apps - Group Manager Compliance, Origin Energy Limited (Australia)

Mr. Toks Azeez - Compliance Business Consultant, Legal Department, Baker Hughes Inc

Mr. Timour Baiazitov – Head of Risk Management and Control, Severstal (Russia)

Mr. Brian Barnier – GRC, IBM Corporation

Mr. Stephen Baruch, CBCP – Disaster Preparedness, Business Continuity, Enterprise Risk Management

Mr. Bob Bassetti - Senior Manager, BearingPoint, Inc.

Mr. Indarduth Beejah – Deputy Director Internal Control, US Government (Mauritius)

Mr. Jose Antonio Rubio Blanco - Rey Juan Carlos University (Spain)

Mr. Robert Bordynuik - Sr Security Consultant, Versatile Solutions LLC (Saudi Arabia)

Mr. Bruce Buckley -General Counsel, IIR

Mr. French Caldwell - VP – Analyst, Gartner, Inc.

Dr. Joseph V. Carcello – Ernst & Young Professor and Director of Research - Corporate Governance Center, University of Tennessee

Mr. Anthony Chalker - Director, Protiviti

Mr. Derek Cherneski - Business Continuity & Security Analyst, Federal Communications Commission (Canada)

Mr. Mandar Chitre - Solution Architect, Infrastructure Management Services, Patni (India)

Mr. Tom Cleary (Australia)

Mr. Richard Cohan, FACHE, CHC, CCEP - Director of Integrity and Compliance and Chief Privacy Officer, Providence Health & Services

Mr. Marco Colonna (Italy)

Mr. Brian Conrey, CISA - Program Manager, Controls Integrity LLC

Ms. Laura Cote - Senior Auditor, Allergan

Mr. Doug Cotton - MD Business Ethics & Compliance Program, American Airlines

Mr. Kevin Crimmins - VP GC, Software Impressions LLC

Mr. John Cross - Lecturer, California State University Fullerton

Ms. Yo Delmar, CMC, CISM - Chief Marketing Officer, Brabeion Software Corporation

Ms. Andrea Dias – Manager, ICTS Global (Brazil)

Mr. Patrick Donovan – Chief Compliance Officer, Airbus SAS (France)

Mr. Rory Douglas - Ethics Analyst

Mr. Robert Drolet - Oracle Financials and GRC Professional, OraApps Consulting, Inc.

Mr. Tim Elliott – Senior Vice-President, Operational Risk Director, Financial Intelligence Division, Comerica Bank

Ms. Sheila Fields - Knowledge Management , HS FIDS

Ms. Cyndi Fleming - Director of IM/IT, DTSSAB (Canada)

Mr. Russ Gates – President, Dupage Consulting LLC

Mr. Leon Goldman - Chief Compliance and Privacy Officer, Beth Israel Deaconess Medical Center

Mr. Royd Graham - Corporate Controller and Senior Director of Accounting, Academy Sports + Outdoors

Mr. Luis Guadarrama - Sr Data Security Consultant (Mexico)

Mr. Richard Gudoi Gid'Agui, CIA, CGFM, CFSA, MSc. Audit(UK), MBA - Senior Lecturer / Program Coordinator Internal Auditing, School of Accountancy, Witwatersrand University (South Africa)

Mr. Miguel Gutierrez, CISA, CISM - Director Global IT Risk & Compliance, International Information Technology, Brink's Incorporated

Mr. Rodrigo Hayvard, Esq. (Chile)

Mr. Michael Helmantoler – Business Continuity, Helmantoler.net

Mr. Arnold Hill - Project Manager, Property Development Division – WPC, US General Services Administration

Mr. Peter Hillier - Principal Consultant, Hillier Security Services (Canada)

Mr. David Hoberg - Corporate Finance Manager, Voith Paper, Inc.

Mr. Matthew Hourin, - Senior Manager, Deloitte

Mr. Jörgen Jarleman - Principal, JMC Management Consulting (Sweden)

Mr. Anil Jhumkhawala – Director-Compliance, Secure Matrix I Pvt Ltd. (India)

Mr. Jim Jolley - Training and Research Manager, Office of Communication and Professional Development, Florida Department of Revenue

Mrs. Christiane Jourdain - Business Continuity Planning Project Manager, Sussex HIS, NHS (United Kingdom)

Mr. Rodriguez Julio - Chief Compliance Officer, Banco Pastor (Spain)

Mr. Daniel Karrer - E-Loan Inc (Brazil)

Ms. Marion Keraudren

Ms. Cary Klafter - VP Legal and Corporate Affairs and Corporate Secretary, Intel Corporation

Mr. Sam Koh - Technical Manager, Vasco (Singapore)

Mr. Alon Kohalny - CAE, Municipality of Kadima-Zoran (Israel)

Mr. Richard Levy - Vice President of Engineering, Mitratech Holdings, Inc.

Ms. Adlinna Liang – Director, MetLife

Mr. Peter Liria – Director, Global Ethics & Compliance, Avaya Inc.

Ms. Anna Luszpinska – Director, Prudential Regulations Department, Bank Zachodni WBK SA (Poland)

Mr. Andre Macieira – Director, ELO Group (Brazil)

Prof. Andre Macieira- Assistant Professor, Concordia University

Ms. Marjorie A. Maguire-Krupp, CPA, CIA, CFSA – President, Coastal Empire Consulting

Mr. Jorge Soeiro Marques - Chief Risk Officer, Lusitania Seguros (Portugal)

Mr. Gabe Mazzarolo - VP – Technology, Pareto (Canada)

Ms. Amelia McCarty - VP Ethics and Compliance, Cardinal Health

Mr. Tlhabano Mmusi - Compliance Trainee (Botswana)

Mr. Paul Moxey - Head of Corporate Governance and Risk Management, ACCA (Association of Chartered Certified Accountants)(UK)

Ms. Florie Munroe - Vice President for Compliance, Health Quest

Mr. Joe Nadivi - CEO, SBS (Israel)

Mr. Warren Nelson - Risk Advisor, Risk & Assurance, Inland Revenue Department (New Zealand)

Mr. Peter Parmenter – Director, Internal Controls, Biomed Realty Trust, Inc.

Ms. Alice Peterson – President, Syrus Global

Ms. Diane Pettie - Vice President General Counsel & Corporate Secretary, Legal, Canexus Limited (Canada)

Ms. Judy Pokorny – Director, Utilities Consulting, Huron Consulting

Mr. Tobin Pospisil - Chief Financial Officer, Gallatin Steel Company

Mr. Richard Poworski – ITA, SGI (Canada)

Ms. Monika Rajh Mladenov – Auditor, The Court of Audit of the Republic of Slovenia (Slovenia)

Mr. Bala Ramanan, -.Sr. Consultant, Microland Ltd (India)

Mr. Javvadi H Rao, FICWA, ACA, CMA, CFM(USA) - Head of Risk Management, Agri Business Division, ITC Ltd. (India)

Dr. Peter Reichard - Group Compliance Officer, Allianz Risk Transfer (Switzerland)

Ms. Kim Rivera - VP Associate GC, The Clorox Company

Mr. Joel Rogers – Director, Ethics & Corporate Compliance, Kaplan EduNeeringMs. Johanna Rogers - Chief Compliance Officer, SunGard

Mr. Peter Rosenzweig - Senior Manager, Advisory Services, Ernst & Young LLP

Mr. Stefano Rossi – Dott, Guidance SRL (Italy)

Ms. Mary Roth - Executive Director, RIMS (Risk and Insurance Management Society)

Mr. Paul Russo - Systems Engineer, BAE Systems

Ms. Karen Rutledge, -.Ethics & Compliance Specialist, PNM Resources, Inc.

Mr. Richard Sanzin - Company Secretary, Royal Automotive Club of Victoria (RACV) Limited (Australia)

Mr. Ram Sastry - Director - IT Audits

Mr. James Sehloff - Information Security Analyst, Holy Family Memorial

Mr. Bob Semple - PricewaterhouseCoopers LLP (Ireland)

Mr. Jerry Shafran - CEO, Compliance Assurance Corporation

Mr. Ken Shaurette - Engagement Manager, Jefferson Wells

Ms. Monica Shilling – Partner, Proskauer Rose LLP

Mr. Jay Shinde, Assistant Professor, Eastern Illinois University

Ms. Elizabeth Siemens - Senior Legal Advisor Governance, Cameco Corporation (Canada)

Mr. Samir Singh

Mr. Mark Snyderman - Chief Ethics & Compliance Officer & Assistant General Counsel, The Coca-Cola Company

Ms. Barbara Stegun Phair – Partner, Abrams Fensterman Fensterman Eisman Greenberg Formato & Einiger, LLP

Ms. C Karen Stopford - AVP Information Security, The Commerce Insurance Company, Inc.

Mr. Geoffrey Storms - Chief Internal Auditor, Cameco Corporation (Canada)

Mr. Dan Swanson - President and CEO, Dan Swanson & Associates (Canada)

Ms. Celia Szelwach - Ethics and Compliance Manager, PBS&J

Ms. Heidi Teresi - Compliance Manager, Alcatel-Lucent

Mr. Tim Tesluk - SVP, Greater China Legal & Compliance, DBS Bank (China)

Mr. Calvin Thompson - Manager, TSWCCUL (Bahamas)

Mr. Kevin Tisdel - Director of Corporate Compliance, Shaw Industries Group, Inc.

Mr. Dan Twing – COO, EMA (South Africa)

Mr. Pieter Van Hout, Ing Mba Mbci - Essent Corporation (Netherlands)

Mr. Surya Vangara – SCSL (Trinidad and Tobago)

Mr. Kishore Vekaria - Director.Secure Keys Consulting (Mauritius)

Mr. Nitish Verma - Director

Mr. Dean Wagers -SOX Compliance, The Kroger Co.

Ms. Kathy Washenberger – IPSO, Hennepin County

Mr. David Wassel - VP, Business Development, ZeroTouchWare

Mr. Ian Lawrence Webster - Governance Officer, Performance Technologies (Brazil)

Mr. Chip Weiant – Chair, American Center for Civic Character

Ms. Mary Karen Wills – Partner, Consulting, Argy Wiltse & Robinson

Ms. ChunHua Yang - Student, Southern Illinois University

Ms. Jie Yang, MBA (China)

Mr. Gunter Zimm

Introduction to Principled Performance and GRC

Today's business climate is more complex and more challenging than ever before. Even small businesses, non-profits and government agencies face issues that, historically, affected only the largest international corporations. Internal and external stakeholders demand not only high performance, but also transparency into business operations. Contemporary risks and requirements are numerous, ever-changing and fast to impact the organization. And, if that were not enough, the costs of addressing risks and requirements are spinning out of control.

In short, the status quo for many organizations is neither sustainable nor acceptable.

To address this growing web of issues, many organizations have adopted a vision toward Principled Performance – a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty (both risk and reward) and acting with integrity (honoring both mandatory commitments and voluntary promises).

Principled Performance is enabled by integrating and orchestrating areas that, in many organizations, are fragmented and siloed – areas such as governance, performance management, risk management, internal control, compliance, and audit. In some organizations, these activities are managed in more than 15 different departments with little if any cross-functional communication. In some organizations, these activities are not really managed at all – literally untouched by modern business process improvement techniques.

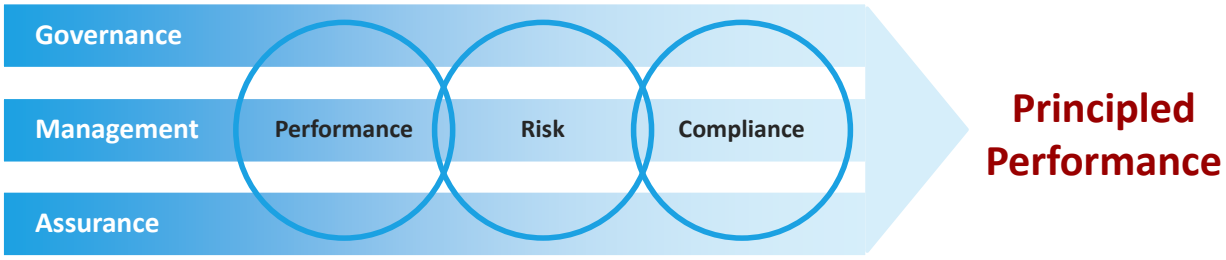


Figure 1

While there are numerous functions that contribute to Principled Performance, many organizations use the acronym GRC (governance, risk, and compliance) as a shorthand reference to the collection of activities. It is important to note that every organization engages in the underlying "GRC" activities to some degree, but many do not do so yet in an integrated way that is effective GRC which can enable Principled Performance.

As Figure 1 demonstrates, the successful attainment of Principled Performance requires a holistic view that addresses the governance, management and assurance of performance, risk and compliance; each with consideration of the other. As demonstrated by companies that have done so, this Integration delivers tangible results:

- Reported cost savings of 30% or more;
- Improved alignment of business objectives with mission, vision and values of the organization;
- Improved capital allocation to the right initiatives at the right time;
- Improved decision-making agility; and
- Top to bottom accountability for key objectives, risks, requirements and related initiatives.

In short, the modern organization must address today's business environment with modern techniques, including a mix of proactive, detective and responsive actions and controls, if it is to achieve Principled Performance. Such techniques are embedded and codified in this GRC Capability Model (also known as the OCEG Red Book).

The Anatomy of the GRC Capability Model

To realize a high-performing GRC capability, the GRC Capability Model™ — commonly called the OCEG Red Book — provides the key Components, Elements and Practices addressing management actions and controls that every organization should implement and manage. Here are definitions and a high level overview of key terms in the Red Book.

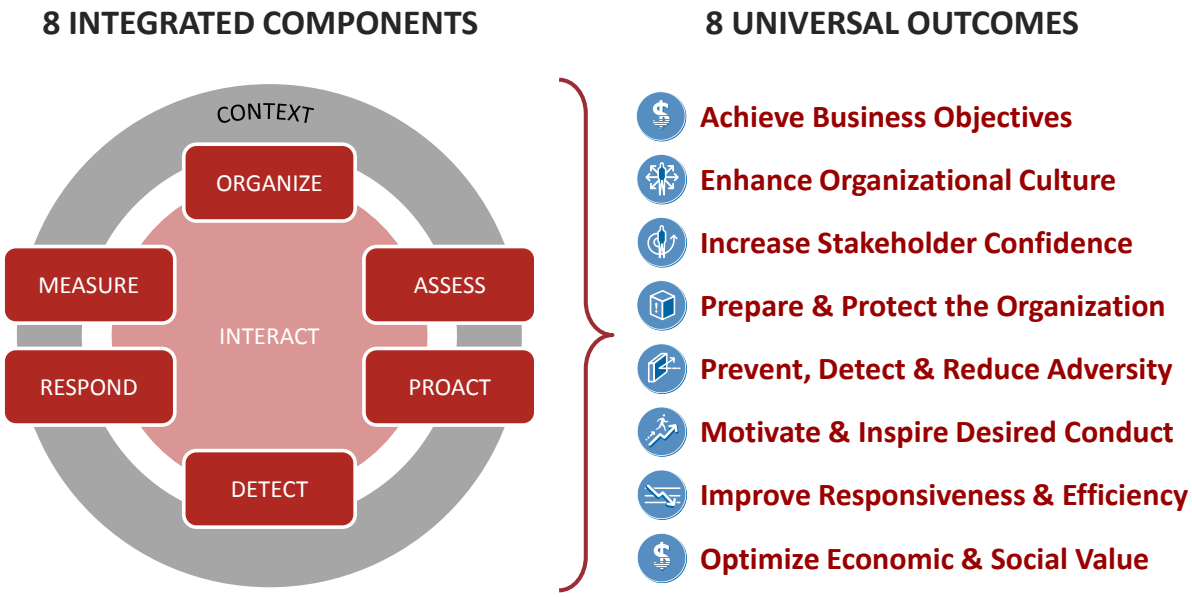


Figure 2 – GRC Capability Model Component View

Universal Outcomes

Universal Outcomes are the expected and observable results of a high-performing GRC capability.

U1. Achieve Business Objectives

Organizations exist to achieve their desired business objectives. Every *GRC capability* must contribute to attaining those business objectives.

U2. Enhance Organizational Culture

Inspire and promote a culture of performance, accountability, integrity, trust, and communication.

U3. Increase Stakeholder Confidence

Increase stakeholder confidence and trust in the organization.

U4. Prepare and Protect Organization

Prepare the organization to address risks and requirements; and protect the organization from negative consequences of adverse events, noncompliance, and unethical behavior.

U5. Prevent, Detect, and Reduce Adversity and Weaknesses

Discourage, prevent, and provide consequences for misconduct; reduce the tangible and intangible damage caused by adverse events (both those that can be controlled and those that cannot), noncompliance and unethical behavior and the likelihood of similar events happening in the future.

U6. Motivate and Inspire Desired Conduct

Provide incentives and rewards for desirable conduct, especially in the face of challenging circumstances.

U7. Improve Responsiveness and Efficiency

Continuously improve the responsiveness (timeliness and agility) and efficiency (speed and quality) of all *GRC capability* activities while improving effectiveness (ability to meet objectives and requirements).

U8. Optimize Economic & Social Value

Optimize the allocation of human and financial capital to *GRC capability* activities to maximize the value generated, benefitting the organization and the society in which it operates.

Components

Components embody integrated Elements of a high-performing GRC capability to support both universal and organizational objectives. They operate in a somewhat sequential manner; however, a user may begin to apply the Red Book at any of the Component points as a means of maturing existing capability. All Components must operate continuously to realize a high-performing GRC capability.

CONTEXT (C)
Understand the current culture and business context so that the organization can address, and proactively influence conditions to support objectives.

ORGANIZE (O)
Organize and oversee an integrated capability that enables the organization to reliably achieve objectives while addressing uncertainty and acting with integrity.

ASSESS (A)
Identify threats, opportunities and requirements; assess the level of risk, reward and conformance; and align an approach to reliably achieve objectives while addressing uncertainty and acting with integrity.

PROACT (P)
Incent desirable conditions and events; and prevent undesirable conditions and events with management actions and controls.

DETECT (D)
Detect ongoing progress toward objectives as well as actual and potential undesirable conditions and events using management actions and controls.

RESPOND (R)
Respond to desirable conditions and events with rewards; and correct undesirable conditions and events so that the organization recovers from and resolves each immediate issue and improves future performance.

MEASURE (M)
Monitor measure and modify the GRC capability on a periodic and ongoing basis to ensure it contributes to business objectives while being effective, efficient and responsive to the changing environment.

INTERACT (I)
Capture, document and manage GRC information so that it efficiently and accurately flows up, down and across the extended enterprise, and to external stakeholders.

Elements

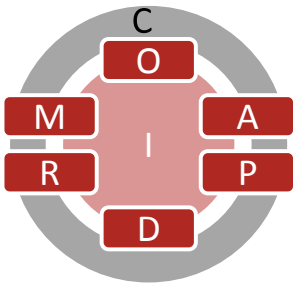
Each Element embodies a number of related Practices in a high-performing GRC capability. Each Element includes a discussion of Principles and Critical Success Factors, as well as the Practices that support success.

INTERACT
I1 – Info Management
I2 – Communication
I3 – Technology

CONTEXT
C1 – External Context
C2 – Internal Context
C3 – Culture
C4 – Objectives

ORGANIZE
O1 – Commitment
O2 – Roles
O3 – Accountability

MEASURE
M1 – Context Monitoring
M2 – Performance Monitoring
M3 – Systemic Improvement
M4 – Assurance



ASSESS
A1 – Identification
A2 – Analysis
A3 – Planning

RESPOND
R1 – Responsive Actions & Controls
R2 – Internal Investigation
R3 – 3rd Party Investigation
R4 – Crisis Response
R5 – Remediation
R6 – Rewards

PROACT
P1 – Proactive Actions & Controls
P2 – Codes of Conduct
P3 – Policies
P4 – Education
P5 – Incentives
P6 – Stakeholder Relations
P7 – Risk Financing

DETECT
D1 – Detective Actions & Controls
D2 – Notification
D3 – Inquiry

Figure 3– GRC Capability Model Elements View

Principles

The Principles behind each Element provide the "essence," at a high level, of what the Element should accomplish. The Principles reflect the consensus of the community of practice in light of its knowledge of both common requirements and practical experience across industries.

Practices

Practices are bundles of activity that address the Principles described in the Element. Practice titles are succinct to communicate the essence of the Practice and are detailed by the Sub-practices.

Sub-Practices

Sub-practices are key observable actions that, taken together, are hallmarks of an effective capability. While one organization may follow a 5-step process and another organization may follow a 20-step process to accomplish the same thing, the identified Sub-practices should be present in both. Sub-practices are generally accepted practices that help an organization effectively and efficiently address Principles and prevalent related requirements from laws and regulations. Often, external mandates are not specific regarding business practices; rather, they articulate broad Principles that an organization must address. Sub-practices help an organization address those Principles.

Actions and Controls

Throughout the Red Book there are numerous references to "actions and controls." An organization should consider the three perspectives that it must addressed when establishing actions and controls not only to ensure management of risk and compliance with requirements, but also to support performance of established organizational objectives.

- **Governance Actions & Controls** help externally direct, control and evaluate an entity, process or resource.
- **Management Actions & Controls** help internally direct, control and evaluate an entity, process or resource.
- **Assurance Actions & Controls** help objectively evaluate an entity, process or resource.

There are also three types of actions and controls, and it is essential that organizations utilize an appropriate mix of these to address performance risk and compliance within a high performing GRC capability.

- **Proactive Actions & Controls** proactively incent desirable; and prevent undesirable conditions or events.
    - Incentive Actions & Controls increase the likelihood, impact or velocity of desirable conditions or events.
    - Preventive Actions & Controls reduce the likelihood, impact or velocity of undesirable conditions or events.
- **Detective Actions & Controls** detect the actual or potential occurrence of desirable and undesirable conditions and events.
- **Responsive Actions & Controls** reward desirable; and correct undesirable conditions or events.
    - Rewarding Actions & Controls recognize the occurrence of desirable conditions or events; and increase the ongoing likelihood, impact and velocity of additional desirable conditions or events.
    - Corrective Actions & Controls clean up the mess caused by the occurrence of undesirable conditions or events; and reduce the ongoing likelihood, impact and velocity of additional undesirable conditions or events.

In short, the GRC Capability must support the governance, assurance and management of performance, risk and compliance with a mix of proactive, detective and responsive actions and controls to achieve Principled Performance. This GRC Capability Model provides the structure within which to do so.

Companion Materials

The OCEG Red Book is supported by several additional sets of materials.

- **The GRC Technology Solutions Guide**

  The Guide assists users in determining which types of technology solutions may be useful in managing each Element of the GRC Capability Model. It can help IT and business users understand at a high level the technology that is available, prioritize the needs of their organization, and start the technology selection process. The Guide defines categories of solutions and maps them to model Elements, key user roles and typical enterprise processes/functions. With an understanding of these relationships, owners of GRC processes and information technology professionals can use the Guide to better understand and enable technology support for GRC processes. The Guide is free for premium and enterprise members of OCEG, and may be purchased by others through the OCEG store at www.oceg.org .

- **The GRC Assessment Tools (Burgundy Book)**

  The GRC Assessment Tools (Burgundy Book) provide a common set of assessment procedures and a common understanding of what can be expected during an design and operating assessment of the design and operating effectiveness of a GRC Capability. These procedures align to the OCEG Red Book and can be used for self-assessment as well as independent assessment. The report from a capability assessment that is performed by a qualified third party using the agreed upon procedures set out in the Burgundy Book is acceptable as input to the OCEG Capability Certification Program. In addition to helping organizations evaluate the design and operating effectiveness of their GRC systems, the Burgundy Book can help to:

  - Reduce cost of such evaluations by eliminating the expense of creating procedures
  - Raise the overall level of maturity and quality of organizational GRC
  - Provide external judgment and recognition of sound practices.

The Burgundy Book is free for enterprise members of OCEG, and may be purchased by others through the OCEG store at www.oceg.org .

- **GRC Fundamentals**

  GRC Fundamentals is a collection of recorded courses that offer further insight into the meaning of Principled Performance and the details of a high performing GRC capability. Users can select and view sessions on their own schedules, and as needed to gain information about each Element of the OCEG Red Book. Periodic updates and additions keep the materials relevant. The series may also be used to help individuals prepare for the GRC Professional Certification (GRCP) offered by OCEG affiliate organization, GRC Certify. GRC Fundamentals may be purchased through the OCEG store at www.oceg.org. More information on the certification is available at www.grccertify.org.

- **Additional Supporting Resources**

  All of the following materials are free to OCEG premium and enterprise members and may be purchased by others through the OCEG store at www.oceg.org

  - **Measurement & Metrics Guide**
  - **Internal Audit Guide**
  - **Hotline/Helpline Handbook**
  - **GRC Illustrated Series**

OCEG Red Book

GRC Capability Model™ version 2.1

Achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance

Model Index

C CONTEXT

C

Understand the current culture and business context so that the organization can address, and proactively influence conditions to support objectives.

C1 External Context

- ***C1.1*** Analyze the External Business Context
- ***C1.2*** Analyze External Stakeholder and Influencer Needs

C2 Internal Context

- ***C2.1*** Define the Internal Context
- ***C2.2*** Determine Changes Needed to Align the Internal Context and GRC capability

C3 Culture

- ***C3.1*** Analyze Ethical Culture
- ***C3.2*** Analyze Ethical Leadership
- ***C3.3*** Analyze Risk Culture
- ***C3.4*** Analyze Board Involvement
- ***C3.5*** Analyze Governance Culture and Management Style
- ***C3.6*** Analyze Workforce Engagement

C4 Objectives

- ***C4.1*** Define Mission & Vision
- ***C4.2*** Define Values
- ***C4.3*** Define Business Objectives
- ***C4.4*** Define Risk Appetite and Decision Criteria
- ***C4.5*** Define Indicators, Targets and Tolerances
- ***C4.6*** Obtain Commitment to Mission, Vision, Values and Objectives
- ***C4.7*** Communicate Mission, Vision and Values

C1 EXTERNAL CONTEXT

C1

Understand and, when necessary, influence the external business context in which the organization operates.

Principles

01 Understanding the ever-changing external context is critical to designing a capability that is resilient to change and can evolve with it.

02 Some aspects of the external context will change despite the organization's best efforts to maintain the status quo.

03 Certain aspects of external context can, and in some cases should, be influenced by the organization.

04 The organization should recognize that there are external influencers, such as the media or community groups who can shape stakeholder opinion.

Critical Success Factors

01 Consider that sometimes aspects of the external context can be changed

02 Ensure sufficient monitoring for changes in the external context

03 Understand external stakeholder needs and requirements

04 Ensure ability to timely and appropriately respond to changes in the external context

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

C1.1 Analyze the External Business Context

C1.2 Analyze External Stakeholder and Influencer Needs

C1.1 ANALYZE THE EXTERNAL BUSINESS CONTEXT

Identify and analyze the relevant external business context factors.

Core Sub-practices

C1.1.01

- Identify factors in the external business context that can affect the organization's ability to meet its objectives , including:
  - industry forces (competitors, supply chain, labor markets, customers, etc.);
  - market forces (customer demographics, economic conditions, etc.);
  - technology forces (technological shifts and breakthroughs, etc.);
  - societal forces (community needs, media trends, etc.);
  - regulatory environment (laws, rules and regulations; enforcement trends, etc.); and
  - geopolitical forces (national politics; political stability; war and peace, etc.).

C1.1.02

- Identify reasons and opportunities to influence the external context.

C1.2 ANALYZE EXTERNAL STAKEHOLDER AND INFLUENCER NEEDS

Identify key external stakeholders, and influencers of opinion, and analyze and prioritize their needs and requirements.

Core Sub-practices

C1.2.01

- Identify key external stakeholders and influencers, including:
  - shareholders;
  - ratings agencies;
  - creditors and other underwriters;
  - customers;
  - suppliers / partners;
  - community;
  - media; and
  - government.

C1.2.02

- Analyze external stakeholder and influencer needs and perceptions for explicit or derived requirements.

C1.2.03

- Identify opportunities where the organization can affect stakeholder and influencer perceptions and requirements.

C2 INTERNAL CONTEXT

C2

Understand and, when necessary, influence the internal business context including the existing strategy, organizational structures, and all key processes and resources (people, financial, information, technology, facilities and other assets).

Principles

01 Internal context analysis should focus on key aspects that drive organizational value.

02 Design a capability that aligns with the internal context.

03 The organization should use the capability to identify and change certain aspects of the internal context to better support organizational objectives.

04 Some aspects of the internal context will change despite the organization's best efforts to maintain the status quo, thus the GRC capability must identify triggers that will require or cause it to evolve.

Critical Success Factors

01 Consider the internal context and existing operating model when designing the capability, thus designing a system that integrates with mainline operations

02 Understand how changes in the internal context require changes in the capability

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

C2.1 Define the Internal Context

C2.2 Determine Changes Needed to Align the Internal Context and GRC capability

C2.1 DEFINE THE INTERNAL CONTEXT

Identify the key structures and assets that define the Internal Context.

Core Sub-practices

C2.1.01

- Identify the organizational structure:
  - key business units,
  - key departments,
  - key job families and roles, and
  - temporary and cross functional teams.

C2.1.02

- Identify key business processes:
  - financial,
  - sales and marketing,
  - manufacturing,
  - supply,
  - distribution and fulfillment,
  - customer service,
  - research and development, and
  - employment.

C2.1.03

- Identify key human capital assets:
  - job families, positions, roles and temporary assignments that have substantial authority over key processes, information and assets,
  - contract employees and any other agents who act on behalf of the entity, and
  - key personnel including senior executives and other key employees.

C2.1.04

- Identify key technology assets:
  - networking infrastructure,
  - computer hardware / software,
  - research equipment, and
  - other operational equipment.

C2.1.05

- Identify key information assets:
  - confidential and trade secret data,
  - customer data, and
  - employee data.

C2.1.06

- Identify key physical assets:
  - buildings,
  - facilities, and
  - operational equipment.

C2.1.07

- Identify key products and services·

C2.1.08

- Identify the interrelationships between and among elements of the structure, people, processes, technology, information and physical assets to understand how the resources work together to accomplish objectives.

C2.1.09

- Identify existing strategies to achieve business objectives.

C2.1.10

- Given current state, define the risk capacity of the organization with regard to particular risk categories.

C2 INTERNAL CONTEXT

C2.2 DETERMINE CHANGES NEEDED TO ALIGN THE INTERNAL CONTEXT AND GRC CAPABILITY

Identify possible changes to the internal context that may affect design aspects of the GRC capability or ensure alignment.

Core Sub-practices

C2.2.01

- Determine what aspects of the internal context can, and should be, changed to enable the GRC capability to support organizational objectives.

C2.2.02

- Determine how the GRC capability design will align with the structure of the internal context.

C2.2.03

- Identify triggers for consideration of changes in the GRC capability, in response to changes in the internal context.

C3 CULTURE

C3

Understand the existing culture including the organizational climate and individual mindsets about governance, assurance and management of performance, risk and compliance.

Principles

01 Consider all aspects of culture including ethical culture, governance culture, risk culture and workforce culture as they stand as well as the desired future state

02 Leadership must set the tone at the top and provide consistent and repeated commitment to integrity in both words and deeds.

03 Individuals must be convinced that leadership is genuine about its commitment to values or they will not have any regard for the established values.

04 The capability can, and in some instances should, change certain aspects of the culture.

05 Some aspects of the culture will change despite the organization's best efforts to maintain the status quo, thus the GRC capability must have triggers that will tell it when to evolve to respond to cultural changes.

Critical Success Factors

01 Consider the culture of the organization as it exists before change is attempted

02 Recognize that there are often multiple "sub cultures" and different approaches to risk, communication, and value attributed to acting with integrity in different geographic or functional locations of the organization

03 Recognize that cultural change may be very difficult and requires continuous example by leadership.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

C3.1 Analyze Ethical Culture

C3.2 Analyze Ethical Leadership

C3.3 Analyze Risk Culture

C3.4 Analyze Board Involvement

C3.5 Analyze Governance Culture and Management Style

C3.6 Analyze Workforce Engagement

Key Deliverables

Plans GRC Strategic Plan

C3.1 ANALYZE ETHICAL CULTURE

Analyze the existing climate (observable, formal elements in the organization) and individual mindsets about the degree to which the workforce believes the organization expects and supports responsible behavior and integrity.

Core Sub-practices

C3.1.01

- Periodically ask a sufficient sample of employees to assess the ethical climate, including questions about:
  - perceptions about stated values/principles and organizational support for them,
  - clarity of procedures by which potential issues can be raised, discussed and reported without fear of retaliation,
  - how leaders and supervisors are demonstrating ethical fortitude and business acumen,
  - misconduct observed by employees,
  - types of misconduct observed,
  - pressure to engage in unethical conduct or perceived rewards for unethical conduct,
  - willingness of employees to report misconduct,
  - satisfaction with organizational response to reports of misconduct, and
  - when and how leaders and supervisors discuss expected behavior and integrity.

C3.1.02

- Identify how the organization discusses the following through multiple avenues of communication:
  - the importance of integrity, values and principles in decision-making,
  - the importance of asking questions and raising issues when concerns exist,
  - how to report incidents and ask questions,
  - assurance that incidents will receive a timely response,
  - assurance that reporting incidents will not result in any retaliation,
  - a commitment to anonymous reporting options, and
  - an approach to ethical decision-making.

C3.1.03

- Define ethical climate objectives, measures, targets and initiatives for inclusion in the GRC capability strategic plan.

C3.2 ANALYZE ETHICAL LEADERSHIP

Analyze whether leadership sets an appropriate "tone at the top" and models behavior in both words and deeds.

Core Sub-practices

C3.2.01

- Periodically ask a sufficient sample of workforce to understand perceptions about whether the leadership:
  - communicates ethical conduct and integrity as a priority,
  - models ethical conduct,
  - ensure internal stakeholders are properly trained about ethics and make it a priority,
  - links ethics to organizational performance metrics,
  - makes ethical decisions, and
  - talks about how ethics or integrity relate to organizational objectives, initiatives, and success.

C3.2.02

- Determine if ethical conduct and integrity is considered when evaluating, promoting and selecting leaders.

C3.2.03

- Determine if potential and newly-promoted leaders are trained about::
  - ethical decision-making,
  - how ethics tie in with organizational objectives, and
  - how to communicate the impact of ethics on organizational performance.

C3.2.04

- Compare ethical leadership objectives, measures, targets and initiatives against results achieved.

C3.3 ANALYZE RISK CULTURE

Analyze the existing climate and individual mindsets about how the workforce perceives risk, its impact on their work and the organization as a whole.

Core Sub-practices

C3.3.01

- Periodically ask a sufficient sample of the workforce to assess the risk culture, including:
  - whether leadership communicates risk appetite,
  - whether leadership models appropriate risk-taking conduct,
  - whether individuals encounter risk on the job and what types of risk, and
  - whether individuals are prepared to handle risks that they face.

C3.3.02

- Define desired state of risk climate / perceptions indicators.

C3.3.03

- Define risk climate objectives, measures, targets and initiatives for inclusion in the GRC capability strategic plan.

C3.4 ANALYZE BOARD INVOLVEMENT

Analyze the degree to which the Board is involved and engaged in the organization.

Core Sub-practices

C3.4.01

- Ask the Board:
  - Do you feel comfortable raising issues?
  - Do you feel comfortable challenging management?
  - Do your suggestions get thoughtful consideration?
  - How involved are you in strategy setting and/or vetting?
  - Is the Board effective?

C3.4.02

- Ask management:
  - Is the Board effective?
  - Are Board members engaged?
  - Do they impact the business?

C3.4.03

- Analyze Board involvement:
  - passive vs. active,
  - number of meetings per year,
  - frequency of meeting without one or more officers, and
  - extent of independent resources supplied by or made available to Board members,
  - degree of cross-board involvement among board members (to what extent do board members serve on multiple boards together).

C3.5 ANALYZE GOVERNANCE CULTURE AND MANAGEMENT STYLE

Analyze the existing approach to governing, managing and enabling the workforce.

Core Sub-practices

C3.5.01

- Identify where management decision-making authority is delegated.

C3.5.02

- Determine how accountability and responsibility are assigned and enforced.

C3.5.03

- Understand how the Board is involved in managing the organization, if at all.

C3.5.04

- Understand the relative level of formality or informality of management.

C3.5.05

- Understand the philosophy around centralized or decentralized decision-making.

C3.5.06

- Understand the philosophy around enterprise, group, and individual measurement:
  - resistance to measurement;
  - prevalence of measurement;
  - preferences in types of measures (activities versus outcomes);
  - what is reported (positive, negative, both);
  - outcomes of measurement (reward focused, consequence focused, balanced).

C3.6 ANALYZE WORKFORCE ENGAGEMENT

Analyze the existing workforce culture including the degree of employee satisfaction, loyalty and engagement.

Core Sub-practices

C3.6.01

- Assess workforce views on alignment of personal values with organizational mission and values.

C3.6.02

- Ask a sample of the workforce about satisfaction with:
  - compensation,
  - responsibility,
  - career opportunities,
  - co-workers,
  - supervisors,

• senior management, and
• staff.

C3.6.03

- Ask a sample of the workforce about:
  • level of commitment to the organization,
  • engagement,
  • loyalty, and
  • willingness to recommend the employer to friends.

C3.6.04

- Ask a sample of the workforce about their perceptions of:
  • management's commitment to competence,
  • hiring policies/practices,
  • training policies/practices,
  • measurement policies/practices,
  • performance evaluation policies/practices,
  • promotion policies/practices,
  • mentoring/career path coaching,
  • compensation policies/practices, and
  • reward/discipline policies/practices.

C3.6.05

- Periodically ask management about its commitment to the workforce including views on:
  • commitment to competence,
  • hiring policies/practices,
  • training policies/practices,
  • performance evaluation policies/practices,
  • promotion policies/practices,
  • mentoring/career path coaching,
  • compensation policies/practices,
  • reward/discipline policies/practices,
  • roles/jobs and career paths, and
  • termination/retirement practices.

C4 OBJECTIVES

C4

Define and align what the organization wants to achieve; the values for which it stands; and the acceptable levels of risk.

Principles

01 Absent leadership supported clearly and regularly articulated mission, vision and values, the organization will operate on the values defined, ad hoc, by work groups or individuals according to their own beliefs and interests.

02 Values will vary for every organization -- that said, values must include adherence to legal mandates and general principles of integrity and ethical conduct.

03 Whether the organization authorizes the Board or management, with Board approval, to set objectives, the Board must oversee managment's continual efforts to meet the established objectives.

04 Align Mission, Vision, Values and Objectives

05 Ensure that both performance and risk tolerance are considered.

Critical Success Factors

01 Leadership must serve as role models and may not be allowed to act contrary to the stated values without consequence

02 Enunciate the organization's values to all stakeholders, repeatedly and from all levels of leadership

03 Address values and commitment to character ethics when setting and articulating measurable business objectives

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

C4.1 Define Mission & Vision

C4.2 Define Values

C4.3 Define Business Objectives

C4.4 Define Risk Appetite and Decision Criteria

C4.5 Define Indicators, Targets and Tolerances

C4.6 Obtain Commitment to Mission, Vision, Values and Objectives

C4.7 Communicate Mission, Vision and Values

Key Deliverables

Statements of Position Mission/ Vision/ Values Statement, Statement of Organizational Objectives

C4 OBJECTIVES

C4.1 DEFINE MISSION & VISION

Create a formal statement of the organization's mission and vision.

Core Sub-practices

C4.1.01

- Define the mission, what the organization will do.

C4.1.02

- Define the vision, what the organization will be.

C4 OBJECTIVES

C4.2 DEFINE VALUES

Create a formal statement of the core values that the organization holds and applies to its business decisions.

Core Sub-practices

C4.2.01

- Involve the Board or a designated sub-committee of the Board and appropriate internal stakeholders in the values development process.

C4.2.02

- Document the statement of values either separately or as part of another document such as a charter or code of conduct.

C4.2.03

- Make the statement of values available to internal stakeholders.

C4.2.04

- Make the statement of values available to external stakeholders.

C4.2.05

- Periodically review the statement of values to consider revisions based upon internal and external business, management, legal or cultural context changes.

C4.2.06

- Define a procedure and trigger to revisit the statement of values when merging with or acquiring a new entity.

C4.3 DEFINE BUSINESS OBJECTIVES

Define a balanced set of measurable business objectives that are congruent with mission, vision and values.

Core Sub-practices

C4.3.01

- Define business objective categories to group related types of business objectives.

C4.3.02

- Define business objectives including:
  - strategic objectives,
  - financial objectives,
  - customer objectives,
  - operational process objectives,
  - learning and growth objectives,
  - compliance objectives, and
  - reporting objectives.

C4.3.03

- Cascade business objectives to lower levels in the organization including business units, departments, teams and individuals so that more detailed, lower-level business objectives map to more high-level business objectives.

C4.3.04

- Assign accountability for achieving business objectives at each of the levels.

C4.4 DEFINE RISK APPETITE AND DECISION CRITERIA

Define the approach and criteria for making decisions about the pursuit of risk relative to reward including risk appetite, tolerance and capacity.

Core Sub-practices

C4.4.01

- For each business objective or business objective category, define a qualitative or quantitative risk tolerance - the level of related risk that the organization is unwilling to exceed to pursue objectives - taking into consideration risk capacity.

C4.4.02

- For each business objective or business objective category, define a qualitative or quantitative risk appetite - the level of related risk that the organization is willing to take while pursuing reward - taking into consideration risk tolerance and risk capacity.

C4.4.03

- Define other criteria for analyzing risk/reward and conformance related to objectives.

C4.4.04

- Define an explicit zero appetite for violating mandatory requirements.

C4.5 DEFINE INDICATORS, TARGETS AND TOLERANCES

Define a balanced set of leading and lagging indicators that help management understand if the organization is meeting its business objective targets within defined tolerances.

Core Sub-practices

C4.5.01

- Use indicators (leading and lagging) to help determine what has happened or predict what will happen.

C4.5.02

- Establish targets that represent the desired indicator value within a particular timeframe.

C4.5.03

- Determine tolerances that represent acceptable upper and lower thresholds of indicator value.

C4.6 OBTAIN COMMITMENT TO MISSION, VISION, VALUES AND OBJECTIVES

Obtain commitment from management and Board members about what the organization will achieve while living by its values.

Core Sub-practices

C4.6.01

- Obtain senior management and Board member commitment to the mission, vision, values.

C4.6.02

- Obtain senior management and Board member commitment to objectives.

C4.6.03

- Obtain senior management and Board member commitment to related risk appetites, indicators, targets and tolerances.

C4.7 COMMUNICATE MISSION, VISION AND VALUES

Communicate the mission, vision and values to internal and external stakeholders.

Core Sub-practices

C4.7.01

- Develop a template for communicating the organization's mission, vision and values, so that there is consistency in each formal communication.

C4.7.02

- Communicate the mission, vision and values of the organization to management and workforce informally and frequently, at meetings and in presentations by leadership.

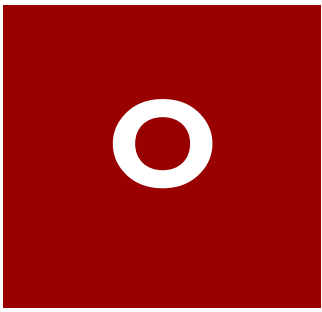
C4.7.03

- Communicate mission, vision and values to internal and external stakeholders formally through:
  • the code of conduct,
  • the entity's website,
  • reports and communications to shareholders & other stakeholders, and
  • workplace postings.

C4.7.04

- Discuss how each group's, department's, business unit's or function's outcomes support achieving the organization's mission, vision, values, and objectives.

O ORGANIZE



Organize and oversee an integrated capability that enables the organization to reliably achieve objectives while addressing uncertainty and acting with integrity.

O1 Commitment

- ***O1.1*** Define GRC capability Scope
- ***O1.2*** Define GRC capability Style and Goals
- ***O1.3*** Obtain Commitment to the GRC capability

O2 Roles

- ***O2.1*** Define and Enable GRC capability Oversight Roles and Accountability
- ***O2.2*** Define and Enable Management Roles and Accountability
- ***O2.3*** Define and Enable Leadership Roles and Accountability
- ***O2.4*** Define and Enable GRC Capability Operational Roles
- ***O2.5*** Define and Enable Assurance Roles and Accountability

O3 Accountability

- ***O3.1*** Allocate Accountability to Individuals and Committees
- ***O3.2*** Define GRC Capability Processes and Integrate with Business Processes
- ***O3.3*** Define Measurement and Evaluation Approach
- ***O3.4*** Define Organizational Change Management Approach
- ***O3.5*** Develop, Maintain and Authorize a Business Case

O1 COMMITMENT

O1

Define the goals of the GRC capability and obtain Board and management commitment.

Principles

01 The Board is responsible for establishing the purpose and goals of the GRC capability.

02 Both the Board and management must be committed to the purpose of the GRC capability, and lead by example.

03 The GRC capability is only successful if it contributes to business objectives.

Critical Success Factors

01 Establish GRC capability objectives and a charter that are aligned to the organization's enterprise objectives

02 Obtain board and key senior leadership support for the program

03 Define and describe the GRC capability as enabling the governance, management and assurance of organizational performance goals, risk management and compliance.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

O1.1 Define GRC capability Scope

O1.2 Define GRC capability Style and Goals

O1.3 Obtain Commitment to the GRC capability

Key Deliverables

Authorizations Internal Authorization, GRC capability Charter

Plans GRC Strategic Plan

01.1 DEFINE GRC CAPABILITY SCOPE

Define the scope of the GRC capability or subsystem under consideration.

Core Sub-practices

01.1.01

- Determine whether to define and implement the GRC capability enterprise-wide or whether to address it in stages by addressing portions such as:
  - broad risk area (compliance program, financial risk program, etc.), or
  - narrow risk area (internal control over financial reporting, employment compliance, fraud risk management).

01.1.02

- If using a staged approach, prioritize and coordinate development projects to ensure integration capability.

O1.2 DEFINE GRC CAPABILITY STYLE AND GOALS

Define the overall style of the GRC capability, what it will achieve, and how it relates to business objectives.

Core Sub-practices

O1.2.01

- Define the mission and vision of the GRC capability as a starting point for the GRC Strategic Plan.

O1.2.02

- Define the general approach to the GRC capability.
  - enforcing or encouraging approach.
  - directive or collaborative philosophy.

O1.2.03

- Define measurable GRC capability goals, indicators, thresholds and tolerances for inclusion in the GRC strategic plan that support the following universal objectives:
  - enhance organizational culture,
  - increase stakeholder confidence,
  - prepare and protect organization,
  - prevent, detect, and reduce adversity,
  - motivate and inspire desired conduct,
  - improve responsiveness and efficiency, and
  - optimize economic and social value.

O1.2.04

- Assign accountability for each GRC capability goal, including such in delegation of authority documents where appropriate.

O1.2.05

- Describe how GRC capability goals support business objectives.

O1.3 OBTAIN COMMITMENT TO THE GRC CAPABILITY

Obtain explicit written authorization and high-level support for the GRC capability.

Core Sub-practices

O1.3.01

- Obtain commitment and authorization from the Board.

O1.3.02

- Obtain commitment from senior management to support the GRC capability.

O2 ROLES

O2

Define, and enable through decision-making authority and resources, each role accountable for key aspects of the capability.

Principles

01 The GRC capability should be directed, designed, operated, and evaluated by a mix of the Board, management, and individuals independent of management.

02 The organization should screen individuals serving in GRC roles for prior misconduct.

03 Individuals serving in GRC roles should receive specialized training in GRC standards and guidance.

04 Leaders and champions can help to facilitate adoption and acceptance of the GRC capability.

05 Leaders and champions should be from many levels in the organization, not just senior executives.

Critical Success Factors

01 Define key roles,responsibilities and authorities

02 Groom leaders for GRC capability responsibilities

03 Assign accountability or responsibility for GRC to individuals who have requisite authority and skills

04 Ensure that assurance and management roles are segregated when appropriate.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

O2.1 Define and Enable GRC capability Oversight Roles and Accountability

O2.2 Define and Enable Management Roles and Accountability

O2.3 Define and Enable Leadership Roles and Accountability

O2.4 Define and Enable GRC Capability Operational Roles

O2.5 Define and Enable Assurance Roles and Accountability

Key Deliverables

Descriptions Role / Job Descriptions

Plans Specialized GRC Curriculum Plan

O2.1 DEFINE AND ENABLE GRC CAPABILITY OVERSIGHT ROLES AND ACCOUNTABILITY

Define oversight roles, responsibilities and accountability for each aspect of the GRC capability.

Core Sub-practices

O2.1.01

- Define critical attributes of oversight structures (e.g. the board) and personnel (e.g. board members), including:
  • independence from management,
  • objectivity in analysis,
  • integrity and ethical conduct,
  • diligence,
  • adequate competence to conduct assigned activities including generally accepted professional credentials consistent with role,
  • transparency of practices and activities, and
  • periodic additions of new oversight structure members to ensure new perspectives

O2.1.02

- Define general oversight responsibilities for:
  • directing and authorizing the purpose and expected GRC capability outcomes,
  • setting a charter for board (and other oversight structure) involvement in the system,
  • being knowledgeable about the design and operation of the system,
  • obtaining regular assurance that the system is effective, and
  • providing reasonable assurance that management's representations about the organization and the system are sound using information developed independent of management.

O2.1.03

- Define responsibility for operating aspects of the GRC capability that require board perspective and independence including:
  • vetting and guiding desired system outcomes to be congruent with business objectives,
  • establishing risk management oversight by the board or a designated committee, which includes approval and periodic review of risk management processes,
  • establishing risk appetite and tolerances and regularly reviewing risk reports to ensure conformance with such established levels,
  • independently assessing, or vetting the assessment of, and monitoring of highest priority risks,
  • requiring management to identify, assess and address risks as part of any significant change proposal,
  • requiring internal or external auditor assessment of the effectiveness and performance of risk management and compliance processes,
  • monitoring any control activities conducted by senior management,
  • monitoring senior management's override of control activities,
  • providing waiver of system requirements in defined circumstances,
  • selecting, evaluating, compensating and terminating senior management, and
  • addressing long-term issues that may exceed senior executive tenure.

O2.1.04

- Define specific GRC responsibilities of Board members and committees.

O2.1.05

- Define job descriptions and performance evaluation criteria for oversight personnel.

O2.1.06

- Check background of personnel hired or promoted into oversight roles.

O2.1.07

- Define and deliver a specialized curriculum plan for oversight personnel that includes relevant portions of OCEG GRC Fundamentals course.

O2.1.08

- Ensure that oversight personnel obtain and maintain professional credentials relevant to their GRC roles.

O2 ROLES

O2.2 DEFINE AND ENABLE MANAGEMENT ROLES AND ACCOUNTABILITY

Define management roles, responsibilities and accountability for certain aspects of the GRC capability.

Core Sub-practices

O2.2.01

- Define responsibility for operating aspects of the GRC capability that require Board perspective and independence including:
  • vetting and guiding business objectives to be congruent with desired system outcomes,
  • independently assessing, or vetting the assessment of, and monitoring highest priority risks,
  • monitoring any control activities conducted by senior management,
  • monitoring senior management's override of control activities,
  • providing waiver of system requirements in defined circumstances,
  • selecting, evaluating, compensating and terminating senior management, and
  • addressing long-term issues that may exceed senior executive tenure.

O2.2.02

- Define specific GRC responsibilities for management roles, including:
  • Chief Executive Officer is responsible for supporting or leading the implementation of the GRC capability,
  • Chief Financial Officer is responsible for authorizing and overseeing resource allocation and budgets, and participating in risk assessment process,
  • Chief Risk Officer is responsible for developing the risk optimization framework and aggregating and analyzing risk at the enterprise level,
  • Chief Compliance Officer is responsible for leading the compliance risk assessment process, overseeing design and implementation of a compliance program intended to prevent, detect and correct legal noncompliance,
  • Chief Ethics Officer is responsible for assessing and enhancing ethical culture through training, communication and other controls (this is often combined with the chief compliance officer), and
  • Chief Legal Officer is responsible for leading the legal risk assessment process, approving policies and controls to assure compliance with legal requirements and to ensure no creation of liability, overseeing and sometimes conducting investigations, ensuring protection of privilege where appropriate.
  • Chief People Officer is responsible for overseeing and implementing human capital incentives and controls, ethical leadership practices, incorporation of requirements into job descriptions and performance evaluations, internal

stakeholder communications, and, possibly, all education and learning initiatives.

• Chief Technology Officer is responsible for coordinating selection and application of technologies to support GRC functions.

O2.2.03

- Define job descriptions and GRC related performance evaluation criteria for management in GRC roles.

O2.2.04

- Check background of management personnel hired or promoted into substantial authority or GRC roles.

O2.2.05

- Define and deliver a specialized curriculum plan for management in GRC roles that includes relevant portions of OCEG GRC Fundamentals course.

O2.2.06

- Ensure that management obtain and maintain professional credentials relevant to their GRC responsibilities.

O2.3 DEFINE AND ENABLE LEADERSHIP ROLES AND ACCOUNTABILITY

Define individuals to serve in leadership roles to champion the GRC capability or certain aspects of the system and establish methods to ensure they possess the desired character ethics.

Core Sub-practices

O2.3.01

- Identify and select individuals at various levels of the organization to serve as leaders and champions for the GRC capability.

O2.3.02

- Define responsibilities of leaders and champions to:
  - break down barriers to change,
  - develop buy-in for the GRC capability, and
  - communicate the desired outcomes of the system and how they relate to business objectives.

O2.3.03

- Establish and communicate a defined set of essential character ethics to which executive leaders have made a commitment and require of designated leaders.

O2.3.04

- Check background of leaders and champions for any incongruence with being an ethical leader (e.g., prior misconduct) and to ensure alignment with established character ethics required of leaders.

O2.3.05

- Regularly engage in discussions with designated leaders about the values they are expected to demonstrate and set expectations about how these will be shared, pursued and monitored, as well as how lapses and trust-eroding events will be redressed.

O2.3.06

- Define and deliver a specialized curriculum for leaders that includes relevant portions of OCEG GRC Fundamentals course.

O2.4 DEFINE AND ENABLE GRC CAPABILITY OPERATIONAL ROLES

Define the roles required to deliver, operate, and execute GRC Capability practices.

Core Sub-practices

O2.4.01

- Define roles responsible for the following key GRC activities:
  - methodology, policy/procedure, standards, vocabulary development and maintenance,
  - risk and requirements identification, analysis, and optimization,
  - initiative implementation /project portfolio management,
  - stakeholder relations,
  - helpline / hotline,
  - investigation and resolution,
  - performance measurement,
  - communications, including public relations,
  - information management, and
  - technology.

O2.4.02

- Define job descriptions and performance evaluation criteria relevant to each GRC operational role.

O2.4.03

- Check background of personnel hired, transferred, or promoted into GRC operational roles.

O2.4.04

- Define and deliver a specialized curriculum plan for GRC operational roles that includes relevant portions of OCEG GRC Fundamentals course.

O2.4.05

- Monitor whether operational personnel have obtained and maintain professional credentials relevant to their GRC roles.

O2.5 DEFINE AND ENABLE ASSURANCE ROLES AND ACCOUNTABILITY

Define assurance roles, responsibilities and accountability for certain aspects of the GRC capability (e.g., chief audit executive, external auditor)

Core Sub-practices

O2.5.01

- Define critical attributes of assurance personnel, including:
  • independence from management,
  • objectivity in analysis,
  • integrity,
  • diligence,
  • adequate competence to conduct assigned activities including generally accepted professional credentials consistent with role, and
  • direct and unfettered access to the Board for senior executive responsible for independent assurance.

O2.5.02

- Define general responsibilities for assurance personnel to provide independent assurance to the Board and management that:
  • risks and requirements (external and internal) are identified, evaluated, managed, reported and monitored via effective methods,
  • they have quality information needed to make GRC capability decisions and reduce the cost of control,
  • the GRC capability is appropriately designed to address identified risks and requirements,
  • the risk management process is designed to identify, evaluate, manage, report and monitor a comprehensive set of risks to (and requirements for) the achievement of the organization's objectives within the organization's values, and
  • the GRC capability is operating as designed.

O2.5.03

- Define job descriptions and performance evaluation criteria for assurance personnel.

O2.5.04

- Check background of personnel hired or promoted into assurance roles.

O2.5.05

- Define and deliver a specialized curriculum plan for assurance personnel that includes relevant portions of OCEG GRC Fundamentals course.

O3 ACCOUNTABILITY

O3

Define an approach to embed, integrate and align the GRC capability with the business, and establish accountability for each aspect of the system.

Principles

01 The degree of integration across risk areas and with existing business processes will vary based on organizational needs.

02 When consolidating responsibilities into a single role, put in place controls to make sure the consolidation does not jeopardize any required objectivity and independence.

03 Irreconcilable conflicts of interests or legal mandates may preclude consolidating responsibilities into a single role.

Critical Success Factors

01 Develop and maintain a business case for the GRC capability with adequate resources to achieve its goals

02 Appropriately aggregate or segregate roles

03 Identify and manage potential resistance to any change that the GRC capability may imply or require

04 Establish clear reporting lines and strong inter-department knowledge sharing

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

O3.1 Allocate Accountability to Individuals and Committees

O3.2 Define GRC Capability Processes and Integrate with Business Processes

O3.3 Define Measurement and Evaluation Approach

O3.4 Define Organizational Change Management Approach

O3.5 Develop, Maintain and Authorize a Business Case

Key Deliverables

Authorizations Internal Authorization, Segregation of Duties

Plans GRC Strategic Plan

O3.1 ALLOCATE ACCOUNTABILITY TO INDIVIDUALS AND COMMITTEES

Allocate GRC roles and responsibilities to individuals and committees.

Core Sub-practices

O3.1.01

- Allocate responsibilities to individuals and committees with other primary roles, if doing so will achieve synergies and efficiencies while ensuring required objectivity and independence.

O3.1.02

- Segregate certain roles as follows:
  • roles that have an interest in uncovering misconduct and weaknesses (compliance, internal audit) from roles that have an interest in legally protecting the organization (general counsel),
  • roles that have an interest in uncovering misconduct and weaknesses (compliance, internal audit) from roles that have an interest in quarterly business performance objectives and incentives that may compromise objectivity,
  • roles that involve implementing and operating preventive and detective controls (finance, compliance) from roles that evaluate the effectiveness of those controls and structures (internal audit), and
  • roles involved in investigations of alleged misconduct and weaknesses from individuals that are alleged to have been, or have potential to have been, involved in the alleged misconduct, and from those who have direct reporting relationships with such individuals.

O3.1.03

- Design adequate reporting relationships that ensure required independence and objectivity are respected including assuring:
  • individuals charged with managing compliance risk have direct access to the Board, and
  • individuals charged with assurance have direct access to the Board.

O3.1.04

- Develop a proposed organizational structure for the GRC capability that enables objective reporting of results.

O3.1.05

- Vet the proposed structure with individuals who would serve in key roles within the GRC capability.

O3.1.06

- Finalize and document GRC capability structure including reporting lines in the GRC strategic plan.

O3.1.07

- Obtain approval of structural plan from appropriate authority.

O3.2 DEFINE GRC CAPABILITY PROCESSES AND INTEGRATE WITH BUSINESS PROCESSES

Define GRC Capability processes and synchronize with existing business processes.

Core Sub-practices

O3.2.01

- Define a GRC capability process model.

O3.2.02

- Define how and when key GRC capability processes will be conducted relative to existing business processes, including:
  • when risk assessments will occur and integrate with existing business planning activities,
  • generally how preventive, detective and corrective activities will integrate with existing business processes,
  • how GRC capability information will be used in conjunction with business information to judge performance,
  • how GRC capability information (internal and external) will integrate with existing communication channels and reporting,
  • when GRC capability monitoring will occur and synchronize it with existing performance monitoring, and
  • how technology that enables the GRC capability will leverage existing business applications and infrastructure.

O3.2.03

- Create a unified calendar for key GRC capability processes and related business processes.

O3.3 DEFINE MEASUREMENT AND EVALUATION APPROACH

Define an approach to measure and evaluate the effectiveness, efficiency, and responsiveness of the GRC capability.

Core Sub-practices

O3.3.01

- Refine desired GRC capability outcomes to ensure they are capable of measurement or evaluation.

O3.3.02

- Allocate accountability for achieving GRC capability outcomes to key personnel.

O3.3.03

- Design reports for senior management and the Board.

O3.3.04

- Define schedule for conducting ongoing and periodic evaluation of the GRC capability.

O3.3.05

- Define targets and thresholds for each measurement indicator and maturity milestones.

O3.4 DEFINE ORGANIZATIONAL CHANGE MANAGEMENT APPROACH

Define an approach to ready the organization for any changes that the GRC capability may require to people, processes, and technology.

Core Sub-practices

O3.4.01

- Identify key areas where the GRC capability may significantly affect existing business units, departments, people, stakeholder relationships, processes, and technology.

O3.4.02

- Assess the readiness of key impacted areas and the organization as a whole to integrate changes.

O3.4.03

- Define specific change management plans to address any anticipated challenges and risks.

O3.5 DEVELOP, MAINTAIN AND AUTHORIZE A BUSINESS CASE

Develop a business case for the GRC capability and obtain authorization from senior management and the Board.

Core Sub-practices

O3.5.01

- Create a strategic plan and business case that summarizes:
  - the desired outcomes of the GRC capability,
  - why it is needed and how it adds value,
  - how it will be structured,
  - how it will be resourced with people, funding and technology (and how much),
  - how it relates to business objectives and the existing operational model,
  - when system components, elements, processes, practices, and enabling technology will be implemented,
  - how performance will be measured, and
  - how assurance will be provided.

O3.5.02

- Obtain authorization from senior management and the Board.

O3.5.03

- Obtain funding for the approach.

A ASSESS

A

Identify opportunities, threats and requirements; assess the level of risk, reward and conformance; and align an approach to reliably achieve objectives while addressing uncertainty and acting with integrity.

A1 Identification

- ***A1.1*** Review Business Objectives, Processes and Resources
- ***A1.2*** Identify External Sources and Forces
- ***A1.3*** Identify Internal Sources and Forces
- ***A1.4*** Identify Opportunities & Threats
- ***A1.5*** Identify Mandatory & Voluntary Requirements
- ***A1.6*** Identify Interrelatedness & Trends
- ***A1.7*** Conduct High Level Analysis of Risk/Reward
- ***A1.8*** Conduct High Level Analysis of Requirements Impact/Conformance
- ***A1.9*** Assign Accountability to Monitor Changes

A2 Analysis

- ***A2.1*** Analyze Approach to Requirements
- ***A2.2*** Analyze Inherent Risk/Reward
- ***A2.3*** Analyze Current Approaches to Risk/Reward
- ***A2.4*** Determine Current Residual Risk/Reward
- ***A2.5*** Prioritize Threats, Opportunities and Requirements

A3 Planning

- ***A3.1*** Explore Options to Address Requirements
- ***A3.2*** Explore Options to Address Risk/Reward
- ***A3.3*** Determine Planned Residual Risk/Reward and Conformance
- ***A3.4*** Address Inherently High Risk
- ***A3.5*** Develop Key Indicators
- ***A3.6*** Develop Integrated Plan

A1 IDENTIFICATION

A1

Identify forces that may cause desirable (opportunity) or undesirable (threat) effects on the achievement of business objectives, as well as those that may compel the business to conduct itself in a particular way (requirement).

Principles

01 Given limited resources, the identification process should focus on key business objectives, processes and resources.

02 Bottom-up participation from the workforce and line managers helps to gather information about what "really happens" in the business and the threats, opportunities and requirements that the workforce and agents actually face.

03 Categorizing threats, opportunities and requirements can help to structure the identification process and ensure uniformity across the organization.

04 Threats, opportunities and requirements rarely fall into singular categories, and tend to be multi-faceted, so management should use multiple identification techniques.

Critical Success Factors

01 Identify both external and internal forces that drive threats, opportunities and requirements.

02 Designate specific personnel to monitor external and internal forces.

03 Identification must be continuous to identify changes in a timely manner.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

A1.1 Review Business Objectives, Processes and Resources

A1.2 Identify External Sources and Forces

A1.3 Identify Internal Sources and Forces

A1.4 Identify Opportunities & Threats

A1.5 Identify Mandatory & Voluntary Requirements

A1.6 Identify Interrelatedness & Trends

A1.7 Conduct High Level Analysis of Risk/Reward

A1.8 Conduct High Level Analysis of Requirements Impact/Conformance

A1.9 Assign Accountability to Monitor Changes

Key Deliverables

Matrices Prioritized Risk Matrix

A1.1 REVIEW BUSINESS OBJECTIVES, PROCESSES AND RESOURCES

Identify and review key business objectives, processes and resources that are relevant given the scope of the capability (e.g, if the scope is the entire organization, then all business objectives, processes and resources are relevant; if the scope is a single department, then some subset of business objectives, processes and resources are relevant).

Core Sub-practices

A1.1.01

- Review business objectives and determine which ones are relevant given the current scope.

A1.1.02

- Identify the key lines of business and organizational entities.

A1.1.03

- Identify key projects, programs and special initiatives.

A1.1.04

- Identify the key processes.

A1.1.05

- Identify the key resources including: people, capital, information, technology, facilities and other resources.

A1.2 IDENTIFY EXTERNAL SOURCES AND FORCES

Imagine and identify external sources and forces that may produce a requirement or cause a desirable or undesirable effect on objectives.

Core Sub-practices

A1.2.01

- Identify political sources and forces including:
  - Political changes
  - Political parties and favoritism
  - Political control of national resources or industry
  - Civil unrest

A1.2.02

- Identify economic sources and forces including:
  - Changes in macroeconomic indicators
  - Changes in disposable income and purchasing power
  - Interest rates
  - Currency fluctuation

- Economic cycles

A1.2.03

- Identify social sources and forces including:
  - Demographic change
  - Lifestyle changes
  - Global culture and subculture change
  - Changes in life expectancy
  - Changes in societal values and preferences
  - Attitudes toward work, life and leisure
  - Religious and secular beliefs

A1.2.04

- Identify technological sources and forces including:
  - Speed of change
  - Availability and cost of computing resources, information and communication
  - Improved industrial processes and materials
  - Changes in transportation and distribution

A1.2.05

- Identify legal sources and forces including:
  - Current and potential laws, rules and regulation
  - Global nuances and potential conflict in requirements
  - Trends in enforcement
  - Trends in civil and derivative litigation

A1.2.06

- Identify environmental sources and forces including flood, fire or earthquakes.

A1.2.07

- Identify external stakeholder sources and forces including:
  - customers
  - media
  - government
  - business partners
  - society

A1.2.08

- Identify competitor sources and forces including:
  - Increased competitive capabilities
  - Unethical conduct including fraud and other crime directed at the organization

A1.3 IDENTIFY INTERNAL SOURCES AND FORCES

Imagine and identify internal sources and forces that may produce a requirement or cause a desirable or undesirable effect on objectives.

Core Sub-practices

A1.3.01

- Identify business model sources and forces including:
  - Changes in mission, vision and values
  - Changes in business objectives
  - Changes in business strategies and structure

A1.3.02

- Identify human capital sources and forces including:
  - Changes in the board
  - Changes in senior management
  - Changes in the workforce

A1.3.03

- Identify internal process sources and forces including:
  - Changes in business processes
  - Ability to address demand under/over capacity
  - Ability execute according to plan
  - Dependency on outside contractors and suppliers

A1.3.04

- Identify internal technology sources and forces including:
  - Changes to IT infrastructure
  - Data integrity
  - Data and system availability
  - Capabilities to implement and support systems

A1.3.05

- Identify internal economic sources and forces including:
  - Changes in capital reserves
  - Changes in required rates of return
  - Changes in the availability of capital

A1.4 IDENTIFY OPPORTUNITIES & THREATS

Given the sources and forces, identify opportunities and threats that affect the achievement of objectives.

Opportunities are events and conditions that, on balance, contribute to reward (which is a measure of the desirable effect of uncertainty on objectives) -- while threats are events and conditions that, on balance, contribute to risk (which is a measure of the undesirable effect of uncertainty on objectives).

Core Sub-practices

A1.4.01

- Identify opportunities which are events and conditions that, on balance, contribute to reward (which is a measure of the likelihood, timing and positive impact of an event on achieving objectives).

A1.4.02

- Identify threats which are events and conditions that, on balance, contribute to risk (which is a measure of the likelihood, timing and negative impact of an event on achieving objectives) including threats that impact:
  - Health and safety
  - Economics such as undesirable changes in stock and index prices, interest rates, exchange rates, commodity prices, customer or debtor payments, customer or debtor credit rating, customer or debtor liquidity
  - Business continuity such as terrorism or disaster
  - Business operations such as debarrment or restriction from specific activities
  - Reputation such as poor product quality, employee misconduct, bribery, fraud, corruption (bribery), harassment and intimidating behavior, criminal mischief, etc.

  Consider threats that result from sources and forces such as:
  - Misalignment of processes and resources
  - Unavailability of resources

A1.4.03

- To get a fulsome understanding of opportunities and threats, use various techniques that look at processes and resources from different points of view including:
  - Process mapping which lays out all key processes and identifies areas where sources and forces may give rise to opportunities/threats.
  - Resource mapping which lays out all key resources (financial, people, technology, facilities, information, etc.) and identifies how sources and forces may give rise to opportunities/threats.
  - Event inventories are detailed listings of events and conditions common to organizations in an industry, geography or using a particular operating model.

A1.5 IDENTIFY MANDATORY & VOLUNTARY REQUIREMENTS

Given sources and forces, identify mandatory and voluntary requirements that must be addressed.

Core Sub-practices

A1.5.01

- Identify key legal compliance areas that apply to the organization, such as:
  - employment,
  - information management, privacy and security,
  - environmental, health and safety,
  - foreign corrupt practices,
  - antitrust,
  - government contracting, and
  - regulated industry requirements.

A1.5.02

- Identify explicit and derived legal requirements that apply to the organization, including those contained in:
  - laws, rules and regulations,
  - administrative rulings,
  - judicial rulings,
  - contracts, and
  - settlement or consent orders and integrity agreements.

A1.5.03

- Identify other explicit and derived external requirements potentially applicable to the organization, including those contained in:
  - safe harbor standards,
  - international, national and industry standards,
  - trade association commitments,
  - stock exchange listing commitments,
  - prosecution, enforcement, penalty and sentencing guidelines,
  - customary practices in the industry, and
  - customary practices in the geography and national culture.

A1.5.04

- Identify explicit and derived internal requirements set forth in:
  - mission, vision, values,
  - code of conduct,
  - policies, and
  - established procedures.

A1.6 IDENTIFY INTERRELATEDNESS & TRENDS

Identify how opportunities, threats and requirements relate to one another and how they have been trending both internally and externally with industry peers.

Core Sub-practices

A1.6.01

- Identify how the likelihood and impact of each event has trended in the organization.

A1.6.02

- Identify how the likelihood and impact of each event has trended in peers and the industry.

A1.6.03

- Identify how likelihood, timing and impact change when repeated or correlated events occur.

A1.7 CONDUCT HIGH LEVEL ANALYSIS OF RISK/REWARD

Conduct a high-level analysis of inherent, current and planned residual risk/reward so that the most relevant items are prioritized in future, more detailed analysis.

Core Sub-practices

A1.7.01

- Risk is a measure of the likelihood, timing and negative impact of an event on the achievement of objectives.

A1.7.02

- Reward is a measure of the likelihood, timing and positive impact of an event on the achievement of objectives.

A1.7.03

- Both risk and reward must be considered together as they offset one another.

A1.8 CONDUCT HIGH LEVEL ANALYSIS OF REQUIREMENTS IMPACT/CONFORMANCE

Conduct a high-level analysis of inherent, current and planned level of conformance with requirements, including rough economic analysis, so that the most relevant items are prioritized in future, more detailed analysis.

Core Sub-practices

A1.8.01

- Conformance is a measure of the degree to which a requirement has been fulfilled often expressed in absolute terms (yes/no).

A1.8.02

- Rough economic analysis helps to understand the significants of mandatory and voluntary requirements.

A1.9 ASSIGN ACCOUNTABILITY TO MONITOR CHANGES

Assign accountability for monitoring the underlying sources that may lead to events and conditions that positively or negatively effect objectives.

Core Sub-practices

A1.9.01

- Assign responsibility to monitor and identify changes to internal factors that affect risks, including:
  - mergers and acquisitions,
  - new product development,
  - expansion into new markets,
  - new contracts or voluntary commitments,
  - key personnel or management changes, and
  - business process changes.

A1.9.02

- Assign responsibility to monitor and identify changes to external factors that affect risks, including:
  - macroeconomic events and cycles,
  - new laws, rules, regulations,
  - shifts in regulatory climate,
  - natural or health hazards,
  - political events and changes,
  - shifts in societal attitudes and perceptions, and
  - shifts in stakeholder attitudes, perceptions and expectations.

A2 ANALYSIS

A2

Analyze current and planned approach to addressing opportunities, threats and requirements so that the inherent, actual, and planned residual levels of risk, reward and conformance are acceptable.

Principles

01 Use top-down analysis and input from senior executives to scope risk analysis activities, but rely on bottom-up information from individuals "on the ground" to ensure that operational reality drives risk analysis.

02 Use risk criteria (risk capacity, risk tolerance, and risk appetite) to determine if current residual risk is acceptable or unacceptable.

03 Document risk analysis so others can use it for other purposes such as audit and assurance activities.

04 Analyze inherent risk and risk criteria so that management can rationalize current and future resource allocation based on the underlying level of risk, and so that risks are not over-managed or under-managed.

Critical Success Factors

01 Use consistent methodologies to analyze and categorize risks across silos

02 Not using both top-down and bottom-up risk analysis techniques

03 Not using both quantitative and qualitative risk analysis techniques

04 Not analyzing both the inherent and current residual risk

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

A2.1 Analyze Approach to Requirements

A2.2 Analyze Inherent Risk/Reward

A2.3 Analyze Current Approaches to Risk/Reward

A2.4 Determine Current Residual Risk/Reward

A2.5 Prioritize Threats, Opportunities and Requirements

Key Deliverables

Matrices Prioritized Risk Matrix

A2.1 ANALYZE APPROACH TO REQUIREMENTS

Analyze the current and planned actions and controls to address requirements including costs.

Core Sub-practices

A2.1.01

- Identify actions and controls in place to address requirements and determine if they meet planned levels of conformance.

A2.2 ANALYZE INHERENT RISK/REWARD

Analyze the effects of threats and opportunities without consideration of current actions or controls.

Core Sub-practices

A2.2.01

- Analyze the likelihood that a risk will materialize including identification of likely:
  • single vs. multiple events, and
  • short-term vs. long-term events.

A2.2.02

- Analyze likely speed of onset and momentum once the risk occurs.

A2.2.03

- Analyze inherent relationship with other risks.

A2.2.04

- Use history of the organization and peers (based on industry, geography, business activities, and workforce scale and footprint) to analyze vulnerability considering likelihood and impact.

A2.2.05

- Pay special attention to inherently high risks as these risks, no matter how well they are addressed with actions and controls, may devestate an organization. Special care should be taken to ensure that related actions and controls are

A2.2.06

- Augment the prioritized risk matrix with a synopsis of the inherent risk analysis.

A2.3 ANALYZE CURRENT APPROACHES TO RISK/REWARD

Identify the presence and effectiveness of current actions and controls that are in place to address the effect of threats and opportunities.

Core Sub-practices

A2.3.01

- Identify and evaluate current actions that either:
  - ACCEPT the risk at the current residual level,
  - AVOID the risk and cease activities (or change requirements) that give rise to the risk,
  - SHARE the impact or optimization of the risk with other entities, including use of risk financing, or
  - SHIFT the risk to another business partner (via joint ventures or risk financing structures),
  - REDUCE likelihood of the risk by implementing incentives, controls and other activities that prevent or reduce the probability that undesirable activities occur, or
  - REDUCE impact by more quickly detecting and responding to undesirable activity, or otherwise preventing risks from accelerating into high impact levels.

A2.3.02

- Identify and evaluate current actions to address risk including use of:
  - incentives for desired conduct,
  - preventive, detective and corrective controls to address undesired conduct or events,
  - issue identification and management ,
  - monitoring activities,
  - policies and procedures,
  - education and awareness programs, and
  - risk financing.

A2.3.03

- Identify and evaluate who, or what department, is accountable for managing each action:
  - mainline business functions, departments and staff,
  - risk management, ethics and compliance departments and staff,
  - assurance departments and staff, and
  - oversight (Board).

A2.3.04

- Identify any gaps and unnecessary overlaps.

A2.3.05

- Augment the prioritized risk matrix with a synopsis of the current approach to address risk.

A2.4 DETERMINE CURRENT RESIDUAL RISK/REWARD

Determine the current level of risk/reward remaining given the presence and effectiveness of current actions and controls.

Core Sub-practices

A2.4.01

- Analyze the effect of current approaches on the likelihood, timing and impact of each risk or category of risk.

A2.4.02

- Determine the cost to maintain current approaches.

A2.4.03

- Determine current level of residual risk.

A2.4.04

- Augment prioritized risk matrix with analysis of the current residual risk.

A2.5 PRIORITIZE THREATS, OPPORTUNITIES AND REQUIREMENTS

Prioritize and categorize threats, opportunities and requirements to determine approach and resource allocation.

Core Sub-practices

A2.5.01

- Determine areas where requirements are not addressed or fail to meet stated levels of conformance.

A2.5.02

- Identify risks that call for high prioritization for improved or additional action or control, including:
  - when current residual risk is unacceptable based on the organization's risk appetite,
  - when current residual risk is unacceptable and immediate action is required,
  - when current actions and controls are ineffective, inconsistently effective, or inefficient,
  - when an inherently high risk requires actions and controls that must be constantly monitored, and
  - when risks require crisis response plans such as workplace violence, natural disasters, and significant reputational issues.

A2.5.03

- Ensure that inherently high risks are specifically addressed since any breakdown in actions or controls to address these risks may result in significant impact on the organization.

A2.5.04

- Augment the priority risk matrix with the prioritization analysis.

A3 PLANNING

A3

Evaluate and implement strategies, tactics, projects and other actions so that the levels of planned residual risk, reward and conformance are acceptable.

Principles

01 Inherently high risk should be prioritized along with unacceptable residual risks.

02 A layered approach may result in a more efficient use of resources and more effective risk optimization.

03 Where appropriate, integrate the management of performance, risk and compliance and embed these within existing, mainline business processes.

Critical Success Factors

01 Monitor inherently high risks, regardless of the current residual risk level, so that the organization will not be exposed to catastrophic impact

02 Assign specific accountability for implementing actions and controls to ensure follow-through

03 Obtain authorization and funding for the integrated plan to ensure that it can and will be implemented

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

A3.1 Explore Options to Address Requirements

A3.2 Explore Options to Address Risk/Reward

A3.3 Determine Planned Residual Risk/Reward and Conformance

A3.4 Address Inherently High Risk

A3.5 Develop Key Indicators

A3.6 Develop Integrated Plan

Key Deliverables

Matrices Prioritized Risk Matrix

Plans Integrated Plan

A3 PLANNING

A3.1 EXPLORE OPTIONS TO ADDRESS REQUIREMENTS

When current level of conformance is not acceptable, or when existing actions and controls are not optimal, explore additional actions and controls to address requirements.

Core Sub-practices

A3.1.01

- Design actions and controls to address gaps and unnecessary overlap in the way that requirements are addressed.

A3.1.02

- Analyze the costs/benefits of proposed actions and controls.

A3 PLANNING

A3.2 EXPLORE OPTIONS TO ADDRESS RISK/REWARD

When the current residual risk is unacceptable or when current approach can be improved, explore alternative actions and controls to address risk/reward.

Core Sub-practices

A3.2.01

- Evaluate and select actions and controls including decisions to accept, avoid, share, shift, or reduce.

A3.2.02

- Evaluate and select actions and controls including those that prevent, detect and respond to undesirable events and conditions.

A3.2.03

- Design a layered approach to avoid "single response bias" in optimizing key risks.

A3.2.04

- Identify areas where optimizing tactics and activities can address more than one risk.

A3.2.05

- Design optimizing activities so that they generate information that can be used for monitoring.

A3.2.06

- If the primary risk optimization option for a particular risk will take some time to implement, define interim risk optimization options including consideration of delaying the action that presents the risk.

A3.2.07

- Estimate the cost associated with planned risk optimization activities and determine if the cost is appropriate given the prioritization of the risk and the level of risk optimization achieved.

A3.3 DETERMINE PLANNED RESIDUAL RISK/REWARD AND CONFORMANCE

Determine the level of risk/reward and conformance that will remain after planned actions and controls are established and operating effectively.

Core Sub-practices

A3.3.01

- Assess the planned residual risk anticipated when the proposed options are put in place.

A3.3.02

- If planned residual risk is not acceptable, reconsider options.

A3.3.03

- If planned residual risk is acceptable, implement the selected options.

A3.3.04

- Analyze the costs and benefits of planned activities.

A3.4 ADDRESS INHERENTLY HIGH RISK

Identify current and planned actions and controls that specifically address inherently high risk and that, should they cease to perform effectively, will expose the organization to unacceptable levels of risk.

Core Sub-practices

A3.4.01

- Identify optimizing activities that currently are in place or are planned to address inherently high risks.

A3.4.02

- Design additional monitoring activities to ensure that these optimizing activities continue to be effective and operate according to plan.

A3.4.03

- Augment the prioritized risk matrix with the planned risk optimization activities and planned residual risk analysis.

A3.4.04

- Include these risks and optimizing activities in assurance plans.

A3.5 DEVELOP KEY INDICATORS

Develop key indicators that inform management about the level of performance, risk and conformance.

Core Sub-practices

A3.5.01

- Identify performance indicators for each objective.

A3.5.02

- Identify conformance indicators for each requirement.

A3.5.03

- Identify risk indicators for each key risk, or category of key risk.

A3.5.04

- Identify thresholds for each indicator that trigger:
  - escalation / reporting,
  - corrective action, or
  - reevaluation of approaches.

A3.5.05

- Assign accountability to periodically, or continuously, monitor each established indicator.

A3.5.06

- Design management reports and dashboards to inform appropriate personnel about indicator values and changes.

A3.6 DEVELOP INTEGRATED PLAN

Develop a plan to govern, assure and manage the approach to addressing performance, risk and compliance.

Core Sub-practices

A3.6.01

- Identify opportunities to consolidate activities into fewer actions.

A3.6.02

- Identify opportunities to embed risk management activities into business processes.

A3.6.03

- Identify opportunities to leverage existing programs, projects, processes, and resources (people, budgets, and technology) before creating new structures.

A3.6.04

- Define initiatives that address related risk optimizing activities in a coordinated fashion.

A3.6.05

- Establish a timeline to implement each initiative.

A3.6.06

- Assign accountability for each initiative and for monitoring events that may require changes to initiatives.

A3.6.07

- Obtain approval for each initiative.

P PROACT

P

Proactively incent desirable conditions and events; and prevent undesirable conditions and events with management actions and controls.

P1 Proactive Actions & Controls

- ***P1.1*** Establish Proactive Management Actions and Controls
- ***P1.2*** Establish Preventive Process Controls
- ***P1.3*** Establish Preventive Human Capital Controls
- ***P1.4*** Establish Preventive Technology Controls
- ***P1.5*** Establish Preventive Physical Controls

P2 Codes of Conduct

- ***P2.1*** Develop the Code of Conduct
- ***P2.2*** Implement and Manage the Code of Conduct
- ***P2.3*** Develop and Implement Ethical Decision-Making Guidelines

P3 Policies

- ***P3.1*** Establish Policy Structure
- ***P3.2*** Develop Policies
- ***P3.3*** Implement and Manage Policies

P4 Education

- ***P4.1*** Define an Awareness and Education Plan
- ***P4.2*** Define a Curriculum Plan
- ***P4.3*** Develop or Acquire Content
- ***P4.4*** Implement Education
- ***P4.5*** Provide Helpline
- ***P4.6*** Provide Integrated Support

P5 Incentives

- ***P5.1*** Hire and Promote Based on Conduct Expectations
- ***P5.2*** Develop Compensation and Remuneration that Consider Conduct Expectations
- ***P5.3*** Develop Rewards Programs

P6 Stakeholder Relations

- ***P6.1*** Understand Stakeholders
- ***P6.2*** Develop Stakeholder Relations Plans
- ***P6.3*** Identify and Track Activity by Requirement Issuing Authorities
- ***P6.4*** Comment on Planned or Proposed Items
- ***P6.5*** Propose Mandates, Standards or Guidance

P7 Risk Financing

- ***P7.1*** Assess Risk Financing Need and Options
- ***P7.2*** Set Risk Financing Objectives
- ***P7.3*** Design Risk Financing Strategy
- ***P7.4*** Implement Risk Financing Strategy

P1 PROACTIVE ACTIONS & CONTROLS

P1

Establish management actions and controls to incent desirable conditions and events; and prevent undesirable conditions and events.

Principles

01 Consider how actions and controls can prevent or incent conduct, events and conditions throughout the extended enterprise.

02 Consider the need for actions and controls that not only serve the management perspective, but also governance and assurance perspectives.

03 Use actions and controls to address performance, risk and compliance management.

04 Use a range of proactive action and control types taking into consideration the need for layering without unnecessary overlap.

05 Identify actions and controls that can serve more than one purpose.

Critical Success Factors

01 Identify or track out-of-date, inaccurate, conflicting and inconsistent actions and controls

02 Ensure that actions and controls neither "under-control" nor "over-control" risks

03 Field test actions and controls to identify weaknesses

04 Identify the ways that a preventive action or control can be violated, circumvented or manipulated

05 Apply controls consistently and make any exceptions clear to those subject to the controls

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P1.1 Establish Proactive Management Actions and Controls

P1.2 Establish Preventive Process Controls

P1.3 Establish Preventive Human Capital Controls

P1.4 Establish Preventive Technology Controls

P1.5 Establish Preventive Physical Controls

Key Deliverables

Authorizations	External Authorizations, Segregation of Duties
Descriptions	Role / Job Descriptions, GRC Technology Data Model Descriptions
Matrices	Policies and Related Procedures Matrix, Prioritized Risk Matrix, Risk / Control Matrix
Plans	Integrated Plan
Reports	Findings and Recommendations Report

P1.1 ESTABLISH PROACTIVE MANAGEMENT ACTIONS AND CONTROLS

Establish proactive management actions and controls that incent desirable, and prevent undesirable, events and conditions.

Core Sub-practices

P1.1.01

- Establish management actions that prevent undesirable events including policies, processes, organizational structures, technology and other actions.

P1.1.02

- Establish management actions that incent desirable events including policies, processes, organizational structures, technology and other actions.

P1.1.03

- Establish controls that ensure management actions are effectively designed and operating.

P1.2 ESTABLISH PREVENTIVE PROCESS CONTROLS

Establish preventive process control activities and procedures to reduce the likelihood and/or impact of adverse events, noncompliance and misconduct.

Core Sub-practices

P1.2.01

- Establish preventive process control activities that are required under mandates or voluntary commitments including:
  - Approvals
  - Authorizations
  - Pre-Submission Reviews
  - Quality Reviews

P1.2.02

- For each preventive process control activity:
  - Define who will perform the activity
  - Define when and how often the activity will be performed
  - Identify individuals with appropriate authority to modify or override preventive process control activities

P1.2.03

- For each preventive process control activity, establish appropriate awareness, education, and support for responsible personnel.

P1.2.04

- Determine the need to assess or certify responsible personnel to ensure that they are able to perform preventive process control activities.

P1.2.05

- Establish a method to periodically assess the effectiveness of each preventive process control activity.

P1.2.06

- For each procedure, define a testing approach and related monitoring activities to ensure that the procedure is operating effectively within defined tolerances.

P1.2.07

- Define procedures and accountability for exceptions to preventive process control activities.

P1.2.08

- Determine which preventive process control activities should be established throughout the extended enterprise.

P1.2.09

- Establish procedures to manage changes to preventive process control activities including:
  - Notifying help desk of any change to a procedure
  - Updating related awareness and education module
  - Updating related skill assessments and certifications
  - Maintaining revision history

P1.2.10

- Update the prioritized risk matrix to reflect:
  - implemented preventive process controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

P1.3 ESTABLISH PREVENTIVE HUMAN CAPITAL CONTROLS

Establish preventive human capital controls to reduce the likelihood and/or impact of adverse events, noncompliance and misconduct.

Core Sub-practices

P1.3.01

- Define job/role descriptions for all key roles.

P1.3.02

- Define which duties should be segregated to prevent conflicts of interest.

P1.3.03

- Confirm that individuals understand that a particular responsibility is segregated from another.

P1.3.04

- Incorporate GRC expectations into appropriate job/role descriptions as determined during assignment of accountability for GRC responsibilities.

P1.3.05

- Define a methodology to check the backgrounds of employees, executives and personnel being hired or promoted into positions

of substantial authority and to evaluate their past conduct, including:

- determinations of any history of violations of the law or unethical conduct,
- how recently any violations or instances of unethical conduct have occurred,
- how any violations or conduct are related to the area of concern for the proposed position of authority,
- any patterns of violations or unethical conduct,
- any conflicts of interest, and
- compatibility of personal values with organizational values.

P1.3.06

- Obtain approval from legal counsel (employment) regarding the background check methodology and criteria.

P1.3.07

- Conduct background checks for individuals hired, promoted, or transferred into roles with substantial authority and document result of background checks for candidates in employment file.

P1.3.08

- Document consent to background check by each candidate.

P1.3.09

- Consistently use interviewing checklists that probe for indicators of behavior consistent with entity values/principles, as well as ethical and unethical behavior and decision-making.

P1.3.10

- Augment or revise the prioritized risk matrix and risk optimization plan to reflect:
  - implemented human capital controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

P1.4 ESTABLISH PREVENTIVE TECHNOLOGY CONTROLS

Establish preventive technology controls to reduce the likelihood and/or impact of adverse events, noncompliance and misconduct.

Core Sub-practices

P1.4.01

- Create a common vocabulary to describe the types of technology controls.

P1.4.02

- Establish preventive technology controls including:
  - Application access controls which limit access to systems, applications and information repositories
  - Physical access controls which limit access to physical technology components such as networks, servers and workstations
  - Configuration controls which prevent or restrict changes to hardware, system and application configurations
  - Master data controls which prevent or restrict changes to information stored in data sources

P1.4.03

- Update the prioritized risk matrix and risk optimization plan to reflect:
  - implemented preventive technology controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

P1.5 ESTABLISH PREVENTIVE PHYSICAL CONTROLS

Establish preventive physical controls to reduce the likelihood and/or impact of adverse events, noncompliance and misconduct.

Core Sub-practices

P1.5.01

- Establish preventive physical controls to meet mandated requirements.

P1.5.02

- Establish preventive physical controls to protect human health and safety.

P1.5.03

- Establish preventive physical controls to protect environmental conditions.

P1.5.04

- Establish preventive physical controls to protect key physical assets including facilities and equipment.

P1.5.05

- Establish preventive physical controls to protect key information assets, including security of laptops, jump drives and other sata storage devices used by employees.

P1.5.06

- Update the prioritized risk matrix and risk optimization plan to reflect:
  - implemented preventive physical controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

P2 CODES OF CONDUCT

P2

Implement a code or codes of conduct for the Board, the workforce and the extended enterprise.

Principles

01 The code should satisfy all legal requirements to have a code for specific positions or purposes but this is not enough; the entire workforce benefits from a code of conduct.

02 Using the code development process to mold champions and secure commitment and buy-in can help to drive its acceptance and strengthen the overall GRC capability.

03 There is an opportunity to include decision guidelines so people can act responsibly and with integrity when the code, policies or applicable law are not specific.

04 Expecting internal stakeholders and the extended enterprise to performing according to the code is only reasonable if the Board and senior management have committed to live by and model the code.

Critical Success Factors

01 Draft the code in language (both type and level) appropriate to its audience

02 Document receipt and understanding of the code

03 Not adapting the code for local culture, norms, and needs

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P2.1 Develop the Code of Conduct

P2.2 Implement and Manage the Code of Conduct

P2.3 Develop and Implement Ethical Decision-Making Guidelines

Key Deliverables

Reports	Findings and Recommendations Report
Statements of Position	Code of Conduct, Ethical Decisions Guidelines

P2.1 DEVELOP THE CODE OF CONDUCT

Work with appropriate stakeholders to develop a code of conduct that addresses the organizational mission, vision, values, key policies and expected business conduct.

Core Sub-practices

P2.1.01

- Define a repeatable methodology for developing the code of conduct.

P2.1.02

- Develop the code of conduct with the participation of stakeholders representing various levels of authority within the organization.

P2.1.03

- Develop all codes of conduct required by legal or other mandates or one code that addresses all such requirements.

P2.1.04

- Identify stakeholders (including those whose behavior may affect the entity's integrity) who are target recipients of the code of conduct.

P2.1.05

- Establish procedures for globalization and localization of the code of conduct that consider local issues while preserving management's intended message.

P2.1.06

- Correlate the code of conduct to sources of requirements, principles, and values.

P2.1.07

- If there is more than one code of conduct, ensure consistency of language and intent between like content.

P2.1.08

- Have appropriate experts review the code of conduct and implementation approach for compliance with mandates.

P2.1.09

- Have relevant policy owners approve code of conduct and implementation approach to confirm adherence to principles.

P2.1.10

- Prioritize the subjects addressed in the code of conduct based on risk analysis.

P2.1.11

- Include an endorsing statement from the Board and senior management.

P2.1.12

- Address the goals and philosophy of the code of conduct and how they align with the overall mission, vision, and values of the organization.

P2.1.13

- At a minimum, provide for the code of conduct to address:
    - compliance with all applicable laws and regulations,

- zero tolerance for corruption and other serious issues,
- conflicts of interest,
- proper use of organizational property, information and opportunities,
- fair treatment in business dealings,
- transparency, timeliness and accuracy of public disclosures and regulatory reporting,
- prompt internal reporting of violations,
- accountability for adherence to the code provisions,
- substance abuse,
- political contributions and activities,
- the importance of ethical values and principles in decision making,
- the importance of asking questions and raising issues when concerns exist,
- how to report misconduct,
- how to report incidents and ask questions, and
- a guarantee of non-retaliation for reporting incidents.

P2.1.14

- Define a procedure to waive and depart from the code of conduct.

P2 CODES OF CONDUCT

P2.2 IMPLEMENT AND MANAGE THE CODE OF CONDUCT

Distribute and manage a code of conduct to ensure that all relevant stakeholders receive the code of conduct, certify that they will follow it that the practices and principles are honored, observed, and enforced, and that it continues to be relevant.

Core Sub-practices

P2.2.01

- Develop a launch plan to distribute the code of conduct.

P2.2.02

- Before implementing the code of conduct, train help desk personnel and others who are designated to answer questions about the content of the code of conduct.

P2.2.03

- Distribute the code of conduct to all targeted stakeholders.

P2.2.04

- Confirm that targeted stakeholders received the code of conduct.

P2.2.05

- Design and deliver training and communication for continual reinforcement of the code of conduct.

P2.2.06

- Ensure that the code of conduct is disclosed to the public and available to external stakeholders (e.g., post on the internet).

P2.2.07

- Disclose, report or file the code of conduct as required by legal mandates.

P2.2.08

- Periodically re-evaluate and define events that trigger re-evaluation of the code of conduct, including changes in laws, operating conditions and policies.

P2.2.09

- Define a methodology for the periodic review and modification of the code of conduct, including identification of specific personnel to monitor legal factors and internal factors that may necessitate modifications.

P2.2.10

- Include code of conduct related criteria in standard individual performance evaluation criteria.

P2.2.11

- Determine scope of code of conduct application in extended enterprise.

P2.2.12

- Be prepared to produce evidence of knowledge or awareness, support and understanding of the code of conduct.

P2.2.13

- Ensure that critical stakeholders understand the code of conduct (via some form of assessment, certification, communication, and/or training).

P2.2.14

- Make adherence to the code of conduct, or to a similar code, a condition of doing business for key suppliers and other partners.

P2.3 DEVELOP AND IMPLEMENT ETHICAL DECISION-MAKING GUIDELINES

Work with appropriate stakeholders to develop and implement guidelines on how to choose a course of action consistent with the organization's mission, vision, values, key policies and expected business conduct when the circumstances are not explicitly covered by the code of conduct, policies, or procedures.

Core Sub-practices

P2.3.01

- Develop the ethical decision guidelines with participation of stakeholders representing various levels of authority within the organization.

P2.3.02

- Develop the ethical decision guidelines with participation of stakeholders representing a variety of the cultures (sub-cultures) that exist across the organization.

P2.3.03

- Identify the ethical and cultural factors to be considered in reaching a decision about a course of conduct, including:
  - congruence with the organization's mission, vision and values;
  - compliance with the organization's requirements;
  - consideration of all relevant viewpoints;
  - completeness of all facts needed to reach a decision;
  - consistency with prior organization behavior and anticipated future decisions under analogous circumstances;
  - comfort with others broadly knowing which individual made the decision;
  - consideration of likely implications to and reactions of stakeholders, influencers or the public; and
  - criticism is anticipated and preempted through clear and cogent explanation.

P2.3.04

- Include an endorsing statement from the Board and senior management.

P2.3.05

- Make the ethical decision guidelines accessible to the workforce and the extended enterprise together with any supplemental resources and information on how to engage someone for further guidance.

P2.3.06

- Provide awareness and education on how to obtain, apply and secure additional guidance in connection with the ethical decision guidelines simultaneously and consistent with communications and education on code(s) of conduct, policies, and procedures.

P2.3.07

- Establish procedures for globalization and localization of the ethical decision-making guidelines that consider local issues and language needs while preserving management's intended decision factors.

P3 POLICIES

P3

Implement policies and associated procedures to address opportunities, threats and requirements.

Principles

01 The policy development process can mold champions and secure buy-in.

02 Policies can both prohibit certain conduct and promote desired behavior.

03 Ethical decision guidelines help people decide what to do in the absence of an explicit policy or procedure.

04 Having evidence that formal policies are communicated and enforced protects the organization when violations occur.

Critical Success Factors

01 Formalize and document policies to ensure that they are known and accessible to their applicable audience (i.e., do not establish "secret policies" that are only uncovered once violated)

02 Establish a plan to implement policies, so they do not just "sit on the shelf"

03 Synchronize all copies with authoritative "master" policies

04 Ensure that policies neither "under-control" nor "over-control" risks

05 Communicate and train the workforce about about new, current, and revised policies

06 Periodically review and revise policies on a schedule so that unplanned atrophy does not occur

07 Audit compliance with policies

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P3.1 Establish Policy Structure

P3.2 Develop Policies

P3.3 Implement and Manage Policies

Key Deliverables

Matrices Policies and Related Procedures Matrix

P3.1 ESTABLISH POLICY STRUCTURE

Establish an organizing structure for identifying and creating policies that support the GRC capability.

Core Sub-practices

P3.1.01

- Develop a list of policies required by applicable mandates, standards, and voluntary commitments.

P3.1.02

- Develop a list of desired policies based on internal decisions.

P3.1.03

- Develop a list of existing policies.

P3.1.04

- Determine redundancies and overlaps in existing policies.

P3.1.05

- Conduct gap analysis against existing policies.

P3.1.06

- Establish methodology to update policy needs analysis.

P3.2 DEVELOP POLICIES

Develop a mix of preventative and directive policies to address requirements, risks, and other program objectives.

Core Sub-practices

P3.2.01
- Ensure that only individuals with appropriate authority issue and modify policies.

P3.2.02
- Define the objective of each policy.

P3.2.03
- Define the target audience for each policy.

P3.2.04
- Have appropriate experts approve policies that must satisfy mandates.

P3.2.05
- Understand business model elements that are affected by each policy.

P3.2.06
- Define when to review, revisit, modify, or expire each policy.

P3.2.07
- Define resources needed for roll-out/implementation/enforcement of each policy.

P3.2.08
- Determine which policies to impose through extended enterprise or to require partners to address directly.

P3.2.09
- Translate or localize policies when determined to be necessary.

P3.2.10
- Map or identify interrelated or dependent policies so that management may understand how changing one may affect another.

P3.2.11
- Design templates for various types of policies.

P3.3 IMPLEMENT AND MANAGE POLICIES

Implement, communicate, and manage policies to ensure that they operate and continue to be relevant.

Core Sub-practices

P3.3.01

- Determine how to make each policy available to each target audience.

P3.3.02

- Determine whether training or testing of target audience is required for each policy.

P3.3.03

- Deliver policies to target audiences.

P3.3.04

- Confirm and document target audience receipt of policies.

P3.3.05

- Define what awareness, education, and support practices should be in place for each policy and each target audience.

P3.3.06

- Define methods for assessing knowledge of the existence and understanding of each policy by target audiences.

P3.3.07

- Define procedure to notify help desk of any additions, modifications, or expiration of policies.

P3.3.08

- Establish a method to assess periodically the effectiveness of each policy in meeting the requirement or objective it is meant to address.

P4 EDUCATION

P4

Educate the Board, management, the workforce and the extended enterprise about expected conduct, and increase the skills and motivation needed to help the organization address threats, opportunities and requirements.

Principles

01 Awareness, education and ongoing support enables individuals to:
- know what is expected,
- reduce the likelihood of errors and criminal behavior, and
- be comfortable about reporting misconduct or GRC capability flaws.

02 A strong education program is not a one-time effort; it requires repeated, consistent messaging in language that the target audiences understand.

03 Qualified professionals should design and deliver education.

04 The ability to seek guidance, including anonymous requests for guidance, prior to or at decision-making time, is critical in an effective GRC capability.

05 Questions can be a source of information that will enable GRC capability improvements or identification of inappropriate conduct.

Critical Success Factors

01 Match the rigor of the messaging or education structure to the nature of the risk or significance of the underlying objective

02 Keep content current, fresh and relevant

03 Establish curriculum that is tied to knowledge requirements of specific roles

04 Provide access to education and other supporting information at the right "points of need"

05 Offer multiple paths to ask questions and obtain guidance, allowing for anonymity when appropriate

06 Obtain evidence of completion and understanding of curriculum

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P4.1 Define an Awareness and Education Plan

P4.2 Define a Curriculum Plan

P4.3 Develop or Acquire Content

P4.4 Implement Education

P4.5 Provide Helpline

P4.6 Provide Integrated Support

Key Deliverables

Descriptions	Helpline FAQ Descriptions
Matrices	Prioritized Risk Matrix
Plans	Awareness and Education Plan, Integrated Plan
Reports	Findings and Recommendations Report

P4.1 DEFINE AN AWARENESS AND EDUCATION PLAN

Develop a plan to inform and educate the Board, management, the workforce and the extended enterprise about their GRC responsibilities and expected conduct.

Core Sub-practices

P4.1.01

- Define a plan to make each target population generally aware of the GRC capability and their responsibilities and expected conduct and as part of the plan:
  • consider scope of awareness required in extended enterprise,
  • consider the existing level of skill when designing plan,
  • categorize content – general awareness versus specific, in-depth training,
  • ensure people only get training relevant to their function/position, and
  • ensure the approach to education considers cultural differences, generational differences, and learning style differences in the target populations.

P4.1.02

- Develop materials describing the primary elements of the GRC capability including the underlying mission, vision, and values of the organization.

P4.1.03

- Determine which target audiences require more specific education about particular aspects of the GRC capability or about specific policies and procedures.

P4.2 DEFINE A CURRICULUM PLAN

Develop a job specific curriculum and appropriate training program for the Board, senior management, the workforce and the extended enterprise to fulfill their GRC responsibilities.

Core Sub-practices

P4.2.01

- Identify legally required education courses including:
  - who must be trained,
  - what the content must cover,
  - how much time must be devoted to the course and how it will be measured, and
  - what methods may be used.

P4.2.02

- For each course that contains legal and/or policy content, map the objective to specific legal and/or policy requirements.

P4.2.03

- Define the competence required of specific roles and positions.

P4.2.04

- Map the series of required and desired courses for each role and position.

P4.2.05

- Conduct a needs assessment that identifies high risk and mandatory training needs, and develop a training plan for each job or job family that details:
  - learning objectives,
  - training modules,
  - target duration of training module,
  - timeline for conducting training,
  - timeline and method(s) for assessing knowledge and/or skill, and
  - frequency for each course, including any "refresh" courses.

P4.2.06

- Define the timeframe for training newly hired, promoted, or transferred individuals for their new roles.

P4.2.07

- For each learning object, select appropriate training mode, media, and synchronicity based on:
  - current skill level of the target audience,
  - target skill level of the target audience,
  - total population size and geographic distribution of the audience, and
  - existing resources and technical capability to deliver training.

P4.3 DEVELOP OR ACQUIRE CONTENT

Develop or acquire content that does not exist in the curriculum or education plan and modify any content that needs updating in current learning objects.

Core Sub-practices

P4.3.01

- Inventory all standardized awareness messages, capturing critical information on each and compare to desired communications in awareness and education plan.

P4.3.02

- Inventory all live, online, and self-paced courses and related training vendors, capturing critical information on each and compare to desired courses in master curriculum.

P4.3.03

- Prepare content development plan to fill gaps in inventory.

P4.3.04

- Use qualified individuals to develop training modules including, as appropriate, learning professionals and subject matter experts with relevant training and experience.

P4.3.05

- Tailor content to an understanding of the target audience's general ability and readiness to learn.

P4.4 IMPLEMENT EDUCATION

Implement and manage the education program to ensure that each target audience achieves learning objectives and can transfer knowledge and skills to their jobs.

Core Sub-practices

P4.4.01

- Integrate GRC training into existing job training wherever possible.

P4.4.02

- Use appropriate technology to develop, deliver, and measure education and awareness.

P4.4.03

- Prepare helpdesk to support questions regarding training access and content.

P4.4.04

- Distribute communications and deliver courses in accordance with plan to target audiences.

P4.4.05

- Deliver training to potential and newly promoted leaders about:
  - responsible decision making,
  - how integrity and responsible business conduct tie in with organizational objectives, and
  - how to communicate about integrity and its impact on organizational performance.

P4.4.06

- Deliver training for all employees about responsible decision-making.

P4.4.07

- Confirm that training was delivered/attended and completed.

P4.4.08

- Assess knowledge, competency, and skills when required and for training that addresses significant risks.

P4.4.09

- Measure training progress against training plan.

P4.4.10

- Augment or revise the prioritized risk matrix and risk optimization plan to reflect:
  - implemented awareness and education initiatives,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

P4.5 PROVIDE HELPLINE

Establish ways for the workforce and other stakeholders to seek guidance about future conduct and ask general questions about GRC responsibilities, including the option for anonymity in locations where that is required or allowed.

Core Sub-practices

P4.5.01

- Define the helpline approach and policy, including the preference for posing questions to a supervisor (or other internal route) first or to the helpline first (this may differ based on type of issue).

P4.5.02

- Define whether helpline (for questions) and hotline (for reporting concerns) are combined or separate.

P4.5.03

- Determine whether a caller must or may remain anonymous or be assured of confidentiality, which in some circumstances may create an atmosphere of greater trust and openness.

P4.5.04

- Establish a process to determine if a question is driven by observations of (or belief that there has been) noncompliance or undesirable conduct, including:
  • if concerns or allegations about noncompliance or misconduct are expressed either directly or after probing about the reason for a question, determine if the allegations or concerns are specific and credible enough to act on,
  • obtain as much information as possible to assist in the process of categorizing the issue within established investigation tiers, and
  • after gaining basic information, redirect to hotline process if an issue has been identified that constitutes a report.

P4.5.05

- Provide helpline personnel with a list of frequently asked questions and answers.

P4.5.06

- Staff the helpline with personnel who are well trained to respond to, or seek assistance to answer, a variety of anticipated inquiries related to the GRC capability and requirements.

P4.5.07

- Establish a method to log questions and responses, indicating final resolution.

P4.6 PROVIDE INTEGRATED SUPPORT

Establish ways for the workforce to get questions about GRC requirements answered within their usual work environment.

Core Sub-practices

P4.6.01

- Ensure that supervisors and GRC capability personnel embedded in the business can answer questions about authority, responsibilities, and issues related to compliance, ethics, and undertaking risks.

P4.6.02

- Inform employees about who is available within their work location to answer questions about authority, responsibilities, and issues related to compliance, ethics and undertaking risks.

P4.6.03

- Develop and make available "self help" materials that employees and other agents can use to answer questions without requiring human interaction.

P4.6.04

- Provide self-service resources (electronic or otherwise) to help individuals answer their questions.

P5 INCENTIVES

P5

Implement incentives that motivate desirable conduct.

Principles

01 Incentive actions and controls are an important balance to preventive actions and controls.

02 Initial hiring requirements that reflect the values of the organization can be one of the most important incentives.

03 Using the observable and measured application of values to business conduct in compensation, recognition and promotion will signal their importance to the workforce and extended enterprise.

Critical Success Factors

01 Consider the full range of incentives including the way that employees are hired, compensated, recognized, educated, and promoted.

02 Analyze incentives to ensure that they incent desired conduct and do not lead to counterproductive behavior.

03 Be consistent when providing rewards and avoid favoritism.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P5.1 Hire and Promote Based on Conduct Expectations

P5.2 Develop Compensation and Remuneration that Consider Conduct Expectations

P5.3 Develop Rewards Programs

Key Deliverables

Matrices Prioritized Risk Matrix

Plans Integrated Plan

Reports Findings and Recommendations Report

P5.1 HIRE AND PROMOTE BASED ON CONDUCT EXPECTATIONS

Consider articulate desirable conduct when defining jobs, career paths and performance review criteria of employees and business partners - and use these same criteria for promoting individuals.

Core Sub-practices

P5.1.01

- Build ethical considerations into:
  - job descriptions,
  - hiring decisions,
  - employee performance evaluation,
  - promotion decisions,
  - compensation and bonus decisions,
  - termination criteria, and
  - disciplinary actions.

P5.1.02

- Conduct performance evaluations for key jobs/roles with GRC related duties.

P5.1.03

- Include GRC related criteria in performance evaluations including:
  - understanding of values,
  - incidents of ethical or alleged unethical conduct, and
  - compliance responsibilities related to the position.

P5.1.04

- Consider ethical conduct as a positive factor (and unethical conduct as a negative factor) when evaluating and promoting employees and when selecting leaders.

P5.1.05

- Define a promotion process that considers an individual's support for and achievement of GRC objectives.

P5.2 DEVELOP COMPENSATION AND REMUNERATION THAT CONSIDER CONDUCT EXPECTATIONS

Design compensation plans and bonus structures for employees and business partners that align with desired conduct and do not reward undesirable conduct.

Core Sub-practices

P5.2.01

- Develop compensation and bonus structures that include consideration and reward for compliance and ethical conduct in any role.

P5.2.02

- Avoid compensation or bonus incentives that encourage misconduct in any role.

P5.2.03

- Analyze compensation and bonus plans for jobs/roles that relate to revenue generation or financial roles/responsibilities, confirming that they do not induce noncompliant or unethical behavior.

P5.2.04

- Analyze compensation and bonus plans for key roles including roles with substantial authority confirming that they do not induce noncompliant or unethical behavior.

P5.2.05

- Analyze discretionary budgets or allowances for all roles, confirming that they do not induce noncompliant or unethical behavior.

P5.3 DEVELOP REWARDS PROGRAMS

Establish a reward program for all employees, business partners and other stakeholders that recognizes individuals and organizational units for exhibiting desired conduct.

Core Sub-practices

P5.3.01

- Develop awards and other incentives to reward model conduct and leadership.

P5.3.02

- Develop incentives that encourage reporting of misconduct or GRC capability flaws.

P5.3.03

- Develop awards and other incentives to recognize organizational units and extended enterprise partners for exemplary management of the GRC capability or group conduct.

P5.3.04

- Develop awards and other incentives for suggestions that improve the GRC capability.

P5.3.05

- Develop awards and other incentives for contributions by individuals or organizational or extended enterprise units that result in reduced compliance failures, enforcement actions or other external challenges to the organization.

P5.3.06

- Augment and/or revise the prioritized risk matrix and, as needed, the risk optimization plan, to reflect:
  - implemented human capital incentives,
  - resulting current residual risk analysis, and
  - performance against planned residual risk analysis.

P5.3.07

- Reward by at least acknowledging members of the workforce for the successful completion of on the job training and self-initiated continuous learning and improvement.

P6 STAKEHOLDER RELATIONS

P6

Interact with stakeholders to shape expectations, affect requirements, and influence perspectives that impact the organization.

Principles

01 Key stakeholders in a business organization include creditors, customers, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources.

02 Stakeholding is usually self-legitimizing (those who judge themselves to be stakeholders are stakeholder); however, not all stakeholders are equal and different considerations can be granted to different stakeholders.

03 Stakeholder requirements can often be shaped when they understand the implications to individual businesses, the industry, the economy and the community at large.

04 Developing key champions in stakeholder groups can help to build trust and confidence.

05 Involvement in developing mandates and standards offers the opportunity to show where integrated or aligned approaches can reduce the burden of compliance and generate more reliable, useful information.

Critical Success Factors

01 Identify individuals with proper skills to serve as the "face of the organization"

02 Identify the key individuals with power and/or influence within each stakeholder group and understand what motivates them (individually and collectively)

03 Communicate early, often and sufficiently with stakeholders before they develop requirements that apply to the organization

04 Provide full information, both good and bad, relevant to stakeholder views of the organization and decisions about requirements

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P6.1 Understand Stakeholders

P6.2 Develop Stakeholder Relations Plans

P6.3 Identify and Track Activity by Requirement Issuing Authorities

P6.4 Comment on Planned or Proposed Items

P6.5 Propose Mandates, Standards or Guidance

Key Deliverables

Plans Communication and Reporting Plan

Reports Filings

P6.1 UNDERSTAND STAKEHOLDERS

Research and analyze the organizations and key individuals involved within various stakeholder constituencies in order to understand their concerns and how best to relate to them.

Core Sub-practices

P6.1.01

- Develop an inventory of key stakeholder organizations and categorize by type, including:
  - government oversight and regulatory agencies,
  - investors,
  - insurers and underwriters,
  - ratings agencies and exchanges,
  - suppliers, extended enterprise partners,
  - customers,
  - communities of operations, and
  - employees, agents, unions.

P6.1.02

- Assemble and review available information about each key stakeholder organization including:
  - mission, vision and values,
  - any statements or documents about relationship with your organization,
  - key individuals important to the relationship, and
  - any information about ethical conduct or noncompliance issues or concerns.

P6.1.03

- Assign ownership for responsibility to keep information about each key stakeholder group current and to inform stakeholder relations executives of any relevant changes.

P6.2 DEVELOP STAKEHOLDER RELATIONS PLANS

Develop stakeholder relations plans, including communications plans, for each stakeholder constituency.

Core Sub-practices

P6.2.01

- Identify circumstances and processes where communications to each stakeholder type may be required.

P6.2.02

- Develop a high-level communication plan that aligns with existing entity channels of communication and which may be adapted to specific circumstances and requirements.

P6.2.03

- Define communication/message interdependencies and how each fits into the overall landscape of other entity communications/messages.

P6.2.04

- Determine which role(s) may authorize initiating communications with each stakeholder type or stakeholder group.

P6.2.05

- Determine who establishes and approves the content and design of communications for each stakeholder type or individual stakeholder groups.

P6.2.06

- Determine who delivers, responds to, and interacts with (i.e., the "face of the organization") each stakeholder type or individual stakeholder groups.

P6.2.07

- Identify other participants in any process where stakeholder relations are important, including likely coalitions and their expected positions that may influence stakeholder views and be prepared to respond.

P6.3 IDENTIFY AND TRACK ACTIVITY BY REQUIREMENT ISSUING AUTHORITIES

Determine which government agencies, standards organizations, and other entities that issue mandates, standards or guidance have significant effect on the organization's GRC requirements and track their activities.

Core Sub-practices

P6.3.01

- Document the issuing authorities of key mandates, standards, and guidelines.

P6.3.02

- Learn each authority's internal procedures for developing mandates, standards, and guidance.

P6.3.03

- Establish procedures to identify when an authority is planning to propose rules, standards, and guidance before publication.

P6.3.04

- Establish procedures to track and review proposed rules, standards, and guidance.

P6.3.05

- Build relationships of trust and respect with key personnel within issuing authorities by creating a reputation for providing valuable assistance and reliable, truthful information.

P6.4 COMMENT ON PLANNED OR PROPOSED ITEMS

Actively participate in the development of mandates, standards, and guidance through various comment pathways.

Core Sub-practices

P6.4.01

- Meet with issuing authorities to understand and discuss planned items and provide organization viewpoint.

P6.4.02

- Provide the issuing authority any relevant data or information that the organization has or may assemble, that enables the authority to make a well-reasoned decision.

P6.4.03

- Participate where appropriate in hearings and provide testimony regarding formal or planned proposals.

P6.4.04

- Provide issuing authority explanatory documents, proposed language or amendments to language, and alternative drafts.

P6.4.05

- Prepare formal written comments on proposed items made available for public comment, which include data and other information that enables the authority to make well-reasoned review and changes to the proposal if appropriate.

P6.4.06

- Provide data and other information to the issuing authority that counters arguments raised by those with different views and interests than the organization.

P6.4.07

- Form formal or informal coalitions with entities that share the organization's viewpoint.

P6.5 PROPOSE MANDATES, STANDARDS OR GUIDANCE

Actively propose development of mandates, standards, and guidance to issuing authorities.

Core Sub-practices

P6.5.01

- Meet with issuing authorities to discuss the need for and benefit of proposed items in terms that meet the interests of the authority.

P6.5.02

- Develop and make available to the issuing authority any relevant data or information that the organization has or may assemble, that enables the authority to make a well-reasoned decision about developing the desired item.

P7 RISK FINANCING

P7

Develop or acquire risk-sharing and financing instruments, including insurance, indemnifications, reserves, captives, and legal entities for appropriately reducing or removing the potential impact of threats.

Principles

01 Risk financing helps to address the impact, usually the financial impact, of adverse events and conditions after they occur.

02 Finance risks simultaneously with consideration of other actions and controls that reduce the likelihood that the adverse event or condition will occur.

03 External risk financing is most helpful for adverse events and conditions with low likelihood and high impact that, should they materialize, would require financial resources beyond the organization's means.

Critical Success Factors

01 Appropriately weigh cost versus benefit of risk financing instruments (e.g., do not over-insure).

02 Ensure that all risk financing obligations and requirements are addressed and that they are continuously monitored for compliance so that coverage does not lapse.

03 Consider the financial strength and resilience of external financing partners.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

P7.1 Assess Risk Financing Need and Options

P7.2 Set Risk Financing Objectives

P7.3 Design Risk Financing Strategy

P7.4 Implement Risk Financing Strategy

Key Deliverables

Matrices Prioritized Risk Matrix

Plans Integrated Plan

P7.1 ASSESS RISK FINANCING NEED AND OPTIONS

Assess the need or desire for financing risk and the options available.

Core Sub-practices

P7.1.01

- Review risk assessment findings to determine which risks should be addressed solely by financing options.

P7.1.02

- Review residual risk after application of determined internal controls to identify risks that require financing as back up for the applied controls.

P7.1.03

- Identify options for types of risk financing appropriate to each identified risk.

P7.2 SET RISK FINANCING OBJECTIVES

Set the risk sharing objectives and limits for the given risk or portfolio of risk.

Core Sub-practices

P7.2.01

- Determine available options for particular risk sharing instruments or approaches.

P7.2.02

- Determine any mandates or policies that preclude use of a particular risk-sharing instrument or approach for particular types of risks.

P7.3 DESIGN RISK FINANCING STRATEGY

Design a portfolio of risk-sharing instruments and approaches.

Core Sub-practices

P7.3.01

- Select risks to be insured.

P7.3.02

- Select risks to be self-insured or subject to captive insurance company.

P7.3.03

- Select risks to be contractually transferred.

P7.3.04

- Select risks to be transferred to other organizational structures (subsidiary, joint venture, LLP, LLC, etc.).

P7.4 IMPLEMENT RISK FINANCING STRATEGY

Implement the risk sharing instruments or structures andÂ acquire insurance.

Core Sub-practices

P7.4.01

- Construct indemnification, assignment, warranty or other contractual language that transfers or allocates risk to other party to contracts.

P7.4.02

- Acquire insurance or establish self-insurance structures.

P7.4.03

- Define appropriate deductibles / retention levels.

P7.4.04

- Define appropriate limits / payouts.

P7.4.05

- Assign accountability for maintaining compliance with requirements of each approach.

P7.4.06

- Form organizational structures and transfer risks.

P7.4.07

- Augment or revise the prioritized risk matrix and risk optimization plan to reflect:
  - implemented risk financing, insurance nad structural controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

D DETECT

D

Detect ongoing progress toward objectives as well as actual and potential undesirable conditions and events using management actions and controls.

D1 Detective Actions & Controls

- ***D1.1*** Establish Detective Actions and Controls
- ***D1.2*** Establish Detective Process Controls
- ***D1.3*** Establish Detective Human Capital Controls
- ***D1.4*** Establish Detective Physical Controls
- ***D1.5*** Establish Detective Technology Controls
- ***D1.6*** Consolidate and Analyze Control Findings

D2 Notification

- ***D2.1*** Capture Notifications
- ***D2.3*** Filter and Route Notifications
- ***D2.4*** Adhere to Data Protection Requirements

D3 Inquiry

- ***D3.1*** Establish Multiple Pathways to Obtain Workforce and Stakeholder Views
- ***D3.2*** Establish an Organization-Wide Integrated Approach to Surveys
- ***D3.3*** Establish an Integrated Approach to Self-Assessments
- ***D3.4*** Gather information through observations and conversations
- ***D3.5*** Report Information and Findings

D1 DETECTIVE ACTIONS & CONTROLS

D1

Establish management actions and controls to detect the actual or potential occurrence of desirable and undesirable conditions and events.

Principles

01 Consider how actions and controls can detect conduct, events and conditions throughout the extended enterprise.

02 Consider the need for actions and controls that not only serve the management perspective, but also governance and assurance perspectives.

03 Use actions and controls to address performance, risk and compliance management.

04 Use a range of detective action and control types taking into consideration the need for layering without unnecessary overlap.

05 Identify actions and controls that can serve more than one purpose.

06 Define dashboards, alerts and reports at an appropriate level of detail for the intended audience.

Critical Success Factors

01 Establish a broad network of information sources to identify potential adverse events and conditions.

02 Identify weaknesses in the notification pathways so that both actual and potential issues are detected.

03 Analyze detected events and conditions for accuracy, veracity, root causes and interrelationships.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

D1.1 Establish Detective Actions and Controls

D1.2 Establish Detective Process Controls

D1.3 Establish Detective Human Capital Controls

D1.4 Establish Detective Physical Controls

D1.5 Establish Detective Technology Controls

D1.6 Consolidate and Analyze Control Findings

Key Deliverables

Descriptions	Exit Interview Checklist
Internal Standards	Control Taxonomy
Reports	Filings, Findings and Recommendations Report

D1.1 ESTABLISH DETECTIVE ACTIONS AND CONTROLS

Establish detective actions and controls to detect and discern progress toward objectives as well as real and potential undesirable events and conditions.

Core Sub-practices

- Establish management actions that detect undesirable events and conditions including: policies, processes, organizational structures, technology and other actions.
- Establish management actions that detect desirable events and conditions including: policies, processes, organizational structures, technology and other actions.
- Establish controls that ensure detective actions are effectively designed and operating.

D1.2 ESTABLISH DETECTIVE PROCESS CONTROLS

Establish process control activities and procedures that detect adverse events, noncompliance and misconduct.

Core Sub-practices

D1.2.01

- Establish detective process control activities based on analysis of financial transactions by frequency, size, location and other factors that may indicate unethical, fraudulent or noncompliant conduct.

D1.2.02

- Establish detective controls based on monitoring of movement and use of physical assets that may indicate unethical, fraudulent or noncompliant conduct.

D1.2.03

- As warranted by the risk analysis, define appropriate continuous monitoring controls.

D1.3 ESTABLISH DETECTIVE HUMAN CAPITAL CONTROLS

Establish human capital control activities and procedures that detect adverse events, noncompliance and misconduct.

Core Sub-practices

D1.3.01

- Use a performance review checklist for individuals that:
  - asks whether the individual has observed misconduct while employed,
  - inquires into suspicions of misconduct or opportunities for misconduct,
  - inquires into feelings about the effectiveness of the GRC capability and any apparent weaknesses,
  - determines feelings toward the organization, management and immediate supervisors, and
  - determines belief in the organization's commitment to stated values and policies.

D1.3.02

- Use an exit interview checklist for individuals that:
  - verifies all organization assets are returned
  - asks whether the individual observed or suspected any compliance failure, unethical conduct, unequal or bias response or discipline for misconduct, uncontrolled risks
  - inquires into feelings about the effectiveness of the GRC capability and any apparent weaknesses,
  - determines feelings of the departing individual toward the organization, management and immediate supervisors, and
  - advises how to report concerns or issues after separation.

D1.3.03

- Augment or revise the prioritized risk matrix and risk optimization plan to reflect:
  - implemented human capital controls,
  - revised current residual risk analysis, and
  - performance against planned residual risk.

D1.4 ESTABLISH DETECTIVE PHYSICAL CONTROLS

Install physical controls necessary to provide surveillance of physical preventive controls and areas where noncompliance or unethical conduct can be physically observed.

Core Sub-practices

D1.4.01

- Establish surveillance mechanisms (cameras or personnel) in high security or threat areas (e.g., hazardous materials storage, server locations, remote parking lots, etc.) to detect tampering, violence, theft, etc.

D1.4.02

- Establish mechanisms (electronic or human) to monitor entry/exit in high security areas.

D1.4.03

- Provide necessary protection of privacy and notification of surveillance where required or determined by policy to be appropriate.

D1.4.04

- Establish silent, audible, and/or visual alarm systems to communicate the detection of breaches of preventive controls and emergencies.

D1.4.05

- Establish mechanisms to track the location of high-value assets or inventory to detect their unauthorized movement (e.g., RFID systems).

D1.4.06

- Use mechanisms to detect the presence or absence of environmental conditions outside acceptable targets or thresholds (e.g., smoke alarms, chemical sniffers, emissions monitors, water quality monitoring systems, refrigeration thermostats, vacuum seal pressure sensors, etc.).

D1.4.07

- Establish mechanisms to detect the presence or absence of workforce and visitors on organizational premises to determine the need to attempt rescue of such individuals,contact family, or other responses.

D1.4.08

- Use mechanisms (electronic or manual badges) to distinguish between workforce, visitors, and unknown individuals on organizational premises so people or systems may detect inappropriate or unauthorized presence or activities.

D1.5 ESTABLISH DETECTIVE TECHNOLOGY CONTROLS

Implement and monitor automated detective technology controls to promptly identify actual or potential misconduct.

Core Sub-practices

D1.5.01

- Monitor detective technology control indicators to identify actual or potential misconduct or noncompliance, including those applied to:
  - physical access and surveillance,
  - system access controls,
  - master data controls,
  - transaction controls,
  - operational controls,
  - audit trails and log analysis,
  - testing activities,
  - performance reporting, and
  - initiative progress, status and risk reporting.

D1.5.02

- Respond to alerts, notifications, and indications of threshold variances.

D1.6 CONSOLIDATE AND ANALYZE CONTROL FINDINGS

Consolidate and analyze all information gathered through various means of detection to identify patterns of misconduct, adverse events and other weaknesses that would otherwise go unnoticed.

Core Sub-practices

D1.6.01
- Perform analysis on gathered data.

D1.6.02
- Document issues using a system or method that allows for subsequent tracking and further analysis.

D1.6.03
- Complete official required forms or reports.

D1.6.04
- Deliver forms, reports, and undocumented information and analysis (if any) according to reporting responsibilities.

D1.6.05
- Engage appropriate Respond and Resolve elements for identified issues.

D1.6.06
- Compare results of analysis with internal benchmarks (another department, business unit, etc.).

D1.6.07
- Compare results of analysis with external benchmarks (peer organization, industry index, etc.).

D2 NOTIFICATION

D2

Provide multiple pathways to report the actual or potential occurrence of undesirable conditions, events and conduct; as well as the occurrence of desirable events.

Principles

01 Provide pathways for people to notify management about BOTH undesirable and desirable events and conduct.

02 Encourage stakeholders to raise issues directly with the organization rather than via external channels.

03 Design the capability so stakeholders can trust, without fear of reprisal, that their concerns are taken seriously, are promptly and objectively assessed and addressed.

04 Promote notification pathways that are appropriate for the local customs and culture.

05 Accommodate for capturing reports made via informal methods and unstructured channels.

Critical Success Factors

01 Establish notification pathways that are easy to use and conform with local customs and culture, as well as data protection requirements.

02 Train management and supervisory personnel to handle and record informal notifications

03 Define consistent escalation paths for all notification pathways

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

D2.1 Capture Notifications

D2.3 Filter and Route Notifications

D2.4 Adhere to Data Protection Requirements

Key Deliverables

Authorizations External Authorizations, Internal Authorization

Plans Communication and Reporting Plan

D2.1 CAPTURE NOTIFICATIONS

Implement a notification system that will alert the organization to incidents or suspicions of legal noncompliance, violations of company policies, and concerns or perceptions about perceived unethical conduct, GRC capability weaknesses and performance at all levels.

Core Sub-practices

D2.1.01

- Use multiple channels:
  - in person,
  - phone,
  - mail,
  - email, and
  - web.

D2.1.02

- Make some channels available 24 hours per day/7 days per week/365 days per year.

D2.1.03

- Define the notification approach and policy, including the preference for reporting to a supervisor (or other internal route) first or to the hotline first (this may differ based on type of issue and local custom and law).

D2.1.04

- Define which channels will be delivered using internal and/or external resources.

D2.1.05

- Define procedures for protecting the anonymity of notifiers in jurisdictions where that is required or allowed.

D2.1.06

- Make the notification pathways available and accessible to multiple stakeholders:
  - employees,
  - agents (contract employees acting on behalf of the entity),
  - suppliers and customers, and
  - public

D2.1.07

- Communicate the availability of the notification pathways to the workforce and other stakeholders.

D2.1.08

- Define procedures for reducing abandonment of initiated notifications, including:
  - limiting or disallowing hold time on phone notifications,
  - providing multiple language capability, and
  - training intended recipients of notifications to treat reporting individuals with respect.

D2.1.09

- Define procedures for protecting the confidentiality of all reported information during intake.

D2.1.10

- Obtain requisite internal and external approvals or licenses of the defined approach.

D2.1.11

- Consistent with local custom and law, create a policy, either separately or as part of the code of conduct, that requires employees to use one of the notification pathways if they observe or know of misconduct.

D2.1.12

- Define a policy, either separately or as part of the code of conduct, stating that the organization will not retaliate against individuals who notify the organization about misconduct or GRC capability flaws.

D2.1.13

- Document the inquiry or issue using a system or method that allows for subsequent analysis.

D2.1.14

- Train personnel (particularly those supervisory personnel expected to receive notifications through the open door policy) on how to handle notifications they receive.

D2 NOTIFICATION

D2.3 FILTER AND ROUTE NOTIFICATIONS

Vet and route notifications for handling, regardless of the pathway through which a given notification is received.

Core Sub-practices

D2.3.01

- Create uniform procedures to manage notifications, including:
  • taxonomy and uniform vocabulary for types of incidents or concern,
  • uniform notification forms or data entry fields,
  • issue routing and escalation protocols,
  • single ultimate repository for all notifications, and
  • methods by which recipients of notifications outside of hotline process enter information into the repository for processing.

D2.3.02

- Define procedures to efficiently review and confirm the validity of notifications.

D2.3.03

- Define information retention requirements associated with all notification pathways.

D2.3.04

- Track the issue as it flows through the resolution process.

D2.3.05

- Establish a procedure to deliver feedback to the notifier so that he or she understands that the issue is being processed or has been resolved.

D2.4 ADHERE TO DATA PROTECTION REQUIREMENTS

Ensure that the hotline pathway for notification complies with specific requirements established in the locale where the notice originates and where the organization operates.

Core Sub-practices

D2.4.01

- Define whether hotline (for reporting concerns) and helpline (for questions) are combined or separate.

D2.4.02

- Determine whether an anonymous reporting system is required, allowed, or not allowed in a given location or circumstance, and design hotline accordingly.

D2.4.03

- Understand data protection and privacy requirements globally applicable to your organization and design the approach so that the hotline complies with all applicable mandates.

D2.4.04

- Establish separate hotlines, or routing approaches, as needed to comply with different legal requirements based on locale of the notifier and of the organization.

D3 INQUIRY

D3

Periodically seek input to understand perceptions about the governance, assurance and management of performance, risk and compliance; and the occurrence of undesirable events and activities.

Principles

01 Provide opportunities to ask stakeholders about the governance, assurance and management of performance, risk and compliance.

02 Make workforce and stakeholders feel their views are valued by considering all feedback and taking appropriate corrective actions.

03 Use the information gained to address issues, build workforce confidence and belief in the organization's commitment to values, and improve GRC capabilitys.

04 Communicate the importance of stakeholder feedback.

05 Avoid any actual or perceived connection between an individual's response and his/her performance assessment.

Critical Success Factors

01 Gather views and information from all relevant target audiences

02 Coordinate efforts to avoid survey/self-assessment fatigue

03 Consolidate, compare and reconcile information obtained from various methods and stakeholders

04 Make sure that information gained via inquiry is used to improve the design and operation of the capability.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

D3.1 Establish Multiple Pathways to Obtain Workforce and Stakeholder Views

D3.2 Establish an Organization-Wide Integrated Approach to Surveys

D3.3 Establish an Integrated Approach to Self-Assessments

D3.4 Gather information through observations and conversations

D3.5 Report Information and Findings

Key Deliverables

Plans Communication and Reporting Plan

Reports Findings and Recommendations Report

D3.1 ESTABLISH MULTIPLE PATHWAYS TO OBTAIN WORKFORCE AND STAKEHOLDER VIEWS

Define opportunities for obtaining workforce and stakeholder views about risk, the GRC capability, conduct and organizational commitment to its stated values.

Core Sub-practices

D3.1.01

- Use key meetings or conversations with target audiences (employee council, analyst briefings, customer / business partner advisory groups, lessons learned sessions, knowledge sharing sessions, government relations meetings, ratings agency reviews, audits) to gain information.

D3.1.02

- Institute opportunities for formal individual workforce conversations.

D3.1.03

- Encourage informal conversations and establish an open door policy.

D3.2 ESTABLISH AN ORGANIZATION-WIDE INTEGRATED APPROACH TO SURVEYS

Establish a survey approach that reduces the burden on survey subjects and provides a consolidated view of information obtained from the workforce and other stakeholders.

Core Sub-practices

D3.2.01

- Define key surveys and target audiences.

D3.2.02

- Inventory existing surveys and analyze timing and content.

D3.2.03

- Map desired surveys to existing surveys for content and audiences.

D3.2.04

- Determine opportunities to consolidate or retire surveys.

D3.2.05

- Determine gaps in existing surveys as against desired surveys.

D3.2.06

- Develop additional necessary surveys.

D3.2.07

- Define maximum number of surveys that an individual should receive in any quarter.

D3.2.08

- Establish an integrated calendar of surveys.

D3.2.09

- Determine appropriate methods to increase survey response rates and candor for each survey:
  - method of delivery of survey (electronic, telephone, paper),
  - opportunity to respond anonymously,
  - incentive or reward for participating, or
  - mandating completion.

D3.3 ESTABLISH AN INTEGRATED APPROACH TO SELF-ASSESSMENTS

Establish a self-assessment approach that integrates assessment of GRC capability-related responsibilities and outcomes with other self-assessments imposed on management.

Core Sub-practices

D3.3.01
- Define key self-assessments and target audiences.

D3.3.02
- Inventory existing self-assessment requirements and analyze timing and content.

D3.3.03
- Map desired self-assessments to existing ones for content coverage.

D3.3.04
- Determine opportunities to consolidate or retire self-assessments.

D3.3.05
- Determine gaps in existing self-assessments to address GRC assessment needs.

D3.3.06
- Develop additional necessary self-assessment questions.

D3.3.07
- Establish an integrated calendar of self-assessments.

D3.4 GATHER INFORMATION THROUGH OBSERVATIONS AND CONVERSATIONS

Establish informal methods of gathering views through observations, group meetings, focus groups and individual conversations.

Core Sub-practices

D3.4.01

- Determine opportunities to gather views through existing scheduled meetings with various stakeholder groups.

D3.4.02

- Coordinate the scheduling of any focus groups or other meetings established for the purpose of discussing GRC issues.

D3.4.03

- Establish a method for information gathered by management during conversations and informal interactions with members of workforce or other stakeholders about their views to be captured.

D3.4.04

- Establish methods to observe workforce behavior and glean information about attitudes and beliefs regarding organizational commitment to values and the GRC capability.

D3.5 REPORT INFORMATION AND FINDINGS

Provide information and findings from all methods of inquiry to management.

Core Sub-practices

D3.5.01

- Analyze information and findings to identify and refer any issues requiring immediate attention.

D3.5.02

- Analyze information and findings to identify and refer information relevant to risk analysis and optimization choices.

D3.5.03

- Analyze information and findings to identify and refer for improvement any GRC capability weaknesses.

D3.5.04

- Document inquiries or issues using a system or method that allows for subsequent tracking and further analysis.

R RESPOND

R

Respond to desirable conditions and events with rewards; and correct undesirable conditions and events so that the organization recovers from and resolves each immediate issue and improves future performance.

R1 Responsive Actions & Controls

- ***R1.1*** Establish Responsive Actions and Controls
- ***R1.2*** Establish Corrective Process Controls
- ***R1.3*** Establish Corrective Human Capital Controls
- ***R1.4*** Establish Corrective Technology Controls
- ***R1.5*** Establish Corrective Physical Controls
- ***R1.6*** Monitor and Report Corrective Controls

R2 Internal Investigation

- ***R2.1*** Define the Inquiry and Investigation Process
- ***R2.2*** Prepare to Investigate
- ***R2.3*** Conduct Investigations
- ***R2.4*** Report Results of Investigations

R3 Third-Party Investigations

- ***R3.1*** Prepare for and Address Third Party Inquiries
- ***R3.2*** Prepare to Identify Third Party Investigations
- ***R3.3*** Prepare to Manage Third Party Investigations
- ***R3.4*** Prepare to Select Internal Team for Third-Party Investigation
- ***R3.5*** Prepare to Respond to Specific Third-Party Investigations

R4 Crisis Response

- ***R4.1*** Develop Crisis Response and Continuity Plans
- ***R4.2*** Identify Crisis Readiness and Response Teams
- ***R4.3*** Test Plans and Procedures
- ***R4.4*** Coordinate Plans

R5 Remediation

R5.1 Remediate the GRC capability

R5.2 Discipline Individuals

R5.3 Disclose Issue Resolution

R6 Rewards

R1 RESPONSIVE ACTIONS & CONTROLS

R1

Establish management actions and controls to reward desirable conduct; discipline undesirable conduct; recover from immediate undesirable events and conditions; and correct identified weaknesses in the capability.

Principles

01 A well designed system of controls should include corrective controls to stop, slow and recover from an adverse event.

02 Corrective controls should provide feedback about how to improve the prevention and detection of future adverse events.

03 Include actions and controls that reward desired conduct.

Critical Success Factors

01 Correct both the immediate adverse effect as well as the root cause of the adverse effect.

02 Establish an audit trail to track when corrective control activities are performed.

03 When resolving an issue, consider how the likelihood, impact and velocity of similar future events can be addressed.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

R1.1 Establish Responsive Actions and Controls

R1.2 Establish Corrective Process Controls

R1.3 Establish Corrective Human Capital Controls

R1.4 Establish Corrective Technology Controls

R1.5 Establish Corrective Physical Controls

R1.6 Monitor and Report Corrective Controls

Key Deliverables

Matrices Risk / Control Matrix

Plans Corrective Control Activity Plan

Reports Corrective Action Report

R1.1 ESTABLISH RESPONSIVE ACTIONS AND CONTROLS

Establish responsive actions and controls that reward desirable conduct; punish undesirable conduct; and correct the identified weaknesses in the capability.

Core Sub-practices

R1.1.01

- Establish corrective actions and controls that slow and reduce the effect of undesirable conduct, events and conditions.

R1.1.02

- Establish corrective actions and controls that address any weaknesses in the capability that allowed undesirable conduct, events and conditions to occur.

R1.1.03

- Establish corrective actions and controls that punish undesirable conduct.

R1.1.04

- Establish rewarding actions and controls that reward desirable conduct.

R1.1.05

- Establish controls that ensure responsive actions are effectively designed and operating.

R1.2 ESTABLISH CORRECTIVE PROCESS CONTROLS

Establish corrective process control activities to stop, slow and recover from adverse events, and deter future adverse events.

Core Sub-practices

R1.2.01

- Establish process control activities that stop and/or slow the adverse event.

R1.2.02

- Establish process control activities that restore the system to a stable state.

R1.2.03

- Establish process control activities that deter future potential adverse events.

R1.3 ESTABLISH CORRECTIVE HUMAN CAPITAL CONTROLS

Establish corrective human capital controls that stop, slow and recover from adverse events, and deter future adverse events.

Core Sub-practices

R1.3.01

- Establish controls to suspend the authority of personnel involved in or related to adverse events.

R1.3.02

- Establish controls to modify or override reporting structures once adverse events are detected.

R1.3.03

- Establish procedures to assemble corrective action teams once adverse events are detected.

R1.4 ESTABLISH CORRECTIVE TECHNOLOGY CONTROLS

Establish corrective technology controls that stop, slow and recover from adverse events, and deter future adverse events.

Core Sub-practices

R1.4.01

- Establish controls to eliminate or restrict access to appropriate technology once adverse events are detected.

R1.4.02

- Establish controls to suspend appropriate processing activities once adverse events are detected.

R1.4.03

- Establish controls to hold and archive appropriate information and documents once adverse events are detected.

R1.5 ESTABLISH CORRECTIVE PHYSICAL CONTROLS

Establish corrective physical controls that stop, slow and recover from adverse events, and deter future adverse events.

Core Sub-practices

R1.5.01

- Establish controls that secure and restrict access to appropriate physical assets once adverse events are detected.

R1.5.02

- Establish controls to lock down appropriate buildings and facilities once adverse events are detected.

R1.5.03

- Establish controls to "harden" physical infrastructure once adverse events are detected including:
  > barriers,
  > reinforcements, and
  > containment.

R1.5.04

- Establish controls to stop or slow the impact of adverse events on physical assets (e.g., fire extinguishers).

R1.6 MONITOR AND REPORT CORRECTIVE CONTROLS

Monitor and report the progress of corrective control activities.

Core Sub-practices

R1.6.01

- Establish a monitoring approach and responsible party to ensure that corrective control activities are performed.

R1.6.02

- Establish reports and identify relevant recipients to be notified when corrective control activities are performed and concluded.

R2 INTERNAL INVESTIGATION

R2

Review and be prepared to investigate allegations or indications of misconduct or GRC Capability failures to understand the facts, circumstances, root causes and appropriate resolution.

Principles

01 People need to have confidence in the process so that they will report incidents and cooperate in investigations.

02 The process must be nimble enough to address regional and situational differences in meeting legal mandates.

03 The Board and senior management should never be blind-sided, but instead must know, in a timely fashion, about an issue that can significantly affect the organization.

04 Information from the issue resolution process should flow seamlessly into processes for identifying and correcting GRC capabilityic weaknesses.

Critical Success Factors

01 Establish a tiered approach for responding to issues that have different levels of potential impact on the organization

02 Establish procedures to timely:
- Capture and validate incidents,
- Categorize incidents in a defined taxonomy,
- Escalate incidents for priority investigation,
- Identify need for in-house or external legal investigation,
- Ensure appropriate confidentiality of information and determine privilege,
- Ensure appropriate protection of anonymity and non-retaliation for reporters,
- Preserve records and other evidence (document hold),
- Complete required reporting or provide notice to outside parties, and
- Determine the need and timing to suspend any business operations

03 Identify the root cause(s) of the problem and address these

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

R2.1 Define the Inquiry and Investigation Process

R2.2 Prepare to Investigate

R2.3 Conduct Investigations

R2.4 Report Results of Investigations

Key Deliverables

Plans Investigation Management Plan

Reports Filings, Findings and Recommendations Report

R2.1 DEFINE THE INQUIRY AND INVESTIGATION PROCESS

Establish procedures for inquiring further into, and investigating, complaints or reports about compliance or ethical issues, as well as for issues detected during ongoing monitoring or periodic evaluation of the GRC capability.

Core Sub-practices

R2.1.01

- Establish a core team to process issues that are identified by complaints, expressions of concern, or other methods (additional parties may be involved on a case-by-case basis to address specific types of issues as they arise).

R2.1.02

- Define a procedure to ensure that alleged perpetrators are not involved in the processing of the issue and are removed from involvement at any point at which they are identified as potential targets of an investigation.

R2.1.03

- Develop and use taxonomies for classifying reported or identified issues and their severity level.

R2.1.04

- Establish an initial screening process to separate issues that can be quickly resolved from those that may need investigation.

R2.1.05

- Define issue management methodology including these key steps:
  - recording and categorizing an issue or question (routing of questions for answers) upon intake,
  - confirmation / validation of an issue,
  - analysis of an issue,
  - investigation of an issue,
  - escalation of an issue,
  - resolution of issue, and
  - referral for remediation / discipline of individuals.

R2.1.06

- Define policies and procedures for determining when and how to protect the confidentiality and anonymity of notifiers in accordance with applicable legal mandates.

R2.1.07

- Define policies and procedures for protecting the confidentiality of all reported information that aligns to applicable legal mandates.

R2.1.08

- Define "investigation tiers" that identify who will address issues of particular scope and type.

R2.1.09

- Define categories of issues that are escalated to the Board or a Board committee immediately upon validation, such as those that are at the "crisis" level due to impact on the organization and/or allegations of senior management wrongdoing.

R2.1.10

- Define categories of issues that are significant enough to be escalated to senior management and/or outside counsel immediately upon validation, due to the material nature of the potential effect on the organization.

R2.1.11

- Define categories of issues that are serious enough to be addressed in special investigations by designated investigators immediately upon validation, due to nature of the potential effect on the organization, for which specific procedures are established.

R2.1.12

- Define categories of issues that are anticipated in the course of business and which may be addressed based on recommendations of initial investigators by line management using specifically established procedures.

R2.1.13

- Define template plans for standard and special investigations of common issues within each investigation tier addressing :
  • processing rules,
  • provision of counsel rules,
  • privilege rules,
  • record retention rules,
  • escalation rules,
  • internal and external reporting rules, and
  • investigation management rules (need for outside legal counsel or special in-house investigators).

R2.1.14

- Periodically conduct review of reported data to determine trends, trouble spots, and controls in need of revisions, looking for concentrated patterns by:
  • geography,
  • specific location,
  • job/role,
  • employee level,
  • employee type (exempt vs. nonexempt vs. temporary), and
  • supervisor.

R2 INTERNAL INVESTIGATION

R2.2 PREPARE TO INVESTIGATE

Prepare to undertake the activities of the investigation phase of the issue resolution process.

Core Sub-practices

R2.2.01

- Define the scope of the planned investigation.

R2.2.02

- Place issue into a particular investigation tier.

R2.2.03

- Determine whether there is an obligation to immediately disclose the issue to the Board, independent auditors or regulatory agencies.

R2.2.04

- Determine if investigation will be conducted under privilege in accordance with established tier rules.

R2.2.05

- Define the investigation team, roles/responsibilities for each team member and the team leader taking into account the topic and scope of the investigation.

R2.2.06

- Define the need for outside assistance in accordance with established tier rules, including:
  • counsel,
  • accountants,
  • forensic experts , and
  • technical consultants.

R2.2.07

- Document a finding of no self-interest (or conflict) in the outcome on the part of any team member.

R2.2.08

- Define internal management that is responsible for oversight of the investigation.

R2.2.09

- Prepare investigation management plan (documents to obtain, interviews to conduct, data to analyze, anticipated reports and audience, budget, and rules of evidence to follow).

R2.2.10

- Initiate any requisite document holds in accordance with established tier rules.

R2.2.11

- If necessary, inform management of the need to suspend any relevant business processes (trading, etc.) in accordance with established tier rules.

R2.2.12

- Define which stakeholders will be informed about the results of the investigation and by what methods.

R2.2.13

- Define a procedure for preserving privilege as necessary during and after completion of the investigation in accordance with established tier rules.

R2.2.14

- Identify possible facts, events or circumstances that, if discovered, may require expansion of the original scope of the investigation and arrange for timely review of any discovered.

R2.2.15

- Define a procedure and protocols to coordinate the investigation with other departments in accordance with established tier rules, including:
  • public relations,
  • investor relations,
  • marketing,
  • HR and human capital management, and
  • business unit and line management.

R2.3 CONDUCT INVESTIGATIONS

Conduct investigations consistent with the plan and communicate with relevant stakeholders while maintaining appropriate privileged status.

Core Sub-practices

R2.3.01

- Notify employees who will be interview subjects.

R2.3.02

- Remind individuals involved whether as the notifier, accused or interviewee, that legal counsel and investigators represent the entity and not them individually.

R2.3.03

- Request and obtain documents, electronic data and other information.

R2.3.04

- Respond to document requests.

R2.3.05

- Analyze documents, data, and interview information to draw conclusions.

R2.3.06

- Determine which conclusions should be documented and which should be presented verbally.

R2.3.07

- Track list of items being maintained as privileged.

R2.3.08

- Track information that will be released as non-privileged, indicating that the release is intentional and controlled.

R2.3.09

- Identify root cause(s) of issue requiring investigation.

R2.4 REPORT RESULTS OF INVESTIGATIONS

Communicate investigation results to appropriate management, oversight bodies and, as appropriate, to other stakeholders and regulators.

Core Sub-practices

R2.4.01

- Communicate results and recommendations to appropriate management, oversight bodies and other stakeholders in accordance with established tier rules.

R2.4.02

- Communicate any findings of material impact (or potential thereof) to the audit committee of the Board.

R2.4.03

- If required, or determined appropriate under established tier rules, file external reports and disclosures with regulatory agencies.

R2.4.04

- Document rationale of those with requisite authority for any recommendation not being pursued.

R3 THIRD-PARTY INVESTIGATIONS

R3

Manage and respond to external inquiries and investigations.

Principles

01 Being prepared to respond to an investigation will minimize its business disruption.

02 A culture of cooperation with third-party inquiries and investigations can help to control the scope and the ultimate impact on the organization.

03 The fact that there is an ongoing external investigation, and its ultimate findings, should not be a surprise to the Board and management.

04 Cooperation does not mean capitulation and the organization may protect itself and its information during an external investigation.

Critical Success Factors

01 Establish an effective system for responding to external inquiries before they become hostile investigations

02 Have a response plan prepared for surprise investigations that involve the sudden appearance of investigators onsite and seizing of documents or premises

03 Determine the appropriate approach to cooperation in conjunction with the advice of counsel and other advisors

04 Keep track of all information provided to external investigators

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

R3.1 Prepare for and Address Third Party Inquiries

R3.2 Prepare to Identify Third Party Investigations

R3.3 Prepare to Manage Third Party Investigations

R3.4 Prepare to Select Internal Team for Third-Party Investigation

R3.5 Prepare to Respond to Specific Third-Party Investigations

Key Deliverables

Plans Investigation Management Plan

Reports Filings, Findings and Recommendations Report

R3.1 PREPARE FOR AND ADDRESS THIRD PARTY INQUIRIES

Identify and respond to questions from third parties.

Core Sub-practices

R3.1.01

- Establish multiple pathways for intake of third party questions including, but not limited to, an anonymous helpline.

R3.1.02

- Establish procedures to screen incoming third party questions, including:
  • determine if initial questions are part of an ongoing investigation,
  • refer inquiries to in-house or external counsel, and
  • assign non-investigative question to appropriate person for timely response or discussion (or refusal to provide information).

R3.1.03

- Establish accepted answers to expected questions that may be provided without further review or approval, via helpline or otherwise.

R3.1.04

- Establish a list of types of questions requiring referral to in-house legal counsel or that will not be answered without a decision by counsel.

R3.2 PREPARE TO IDENTIFY THIRD PARTY INVESTIGATIONS

Establish methods to ensure the right people know about initiated third party investigations.

Core Sub-practices

R3.2.01

- Establish procedures to ensure that questions posed to the organization via a helpline or other method, that are identified as part of or precursor to a third party investigation are forwarded to appropriate personnel responsible for vetting such investigations.

R3.2.02

- Establish policies and procedures to require internal reporting of knowledge of non-standard third party inquiries, or investigations, to appropriate management personnel.

R3.2.03

- Establish monitoring of external sources to identify onset of a third party investigation when possible.

R3.3 PREPARE TO MANAGE THIRD PARTY INVESTIGATIONS

Establish policies, procedures, and responsibility for managing various types of third party investigations.

Core Sub-practices

R3.3.01

- Establish an inventory of the types of possible third party investigations and assign management responsibility for each type (overall or within specific areas of risk concern and/or part of the organization), including:
  • compliance audit of organization as a vendor;
  • routine regulatory investigations,
  • regulatory investigations that relate to possible civil or criminal violations,
  • private party investigations related to litigation or legal claims,
  • external stakeholder investigations including investors, lenders, underwriters, listing agents,
  • grand jury investigations, and
  • physical site or document seizures by government enforcement agents.

R3.3.02

- Determine and document organizational rights and procedural safeguards in the context of each anticipated type of investigation based on investigating authority and legal basis of the investigation, taking privilege and confidentiality needs into account.

R3.3.03

- Establish policies and procedures to follow at the onset of each identified type of investigation including:
  • procedures for establishing an internal response team and team leader,
  • procedures for responding to interview requests and subpoenas,
  • procedures for responding to document requests and subpoenas,
  • procedures for responding to information that former employees or other stakeholders have been contacted for interviews or documents, and
  • procedures for responding to sudden on site presence of investigators demanding documents or seizure of the premises.

R3.3.04

- Establish procedures to disclose the existence of a particular type of investigation to the Board, independent auditors, regulatory agencies, creditors or insurers whenever there is an obligation to do so under agreements, contracts or established policies and procedures, and ensure disclosure meets any timing requirements.

R3.3.05

- Establish procedures to quickly inform senior management and the Board or audit committee of any investigation the outcome of which may be material to the organization, implicate wrongdoing by any member of management, indicate criminal wrongdoing by anyone in the organization, or lead to potential reputational damage, taking privilege and confidentiality needs into account.

R3.3.06

- Establish procedures to inform those responsible for managing the public relations and stakeholder relations of the organization about investigations as soon as possible and, to the extent necessary, within the context of a privileged discussion.

R3.3.07

- Prepare methods for determining privilege, privacy and confidentiality issues that may need to be addressed with

investigators.

R3.3.08

- Prepare methods for determining conflicts of interest of individuals involved in the investigation from either the organization or the investigating body.

R3.4 PREPARE TO SELECT INTERNAL TEAM FOR THIRD-PARTY INVESTIGATION

Establish procedures for selecting the team of individuals that will represent the organization during a specific investigation.

Core Sub-practices

R3.4.01

- Establish initial lists of the people (roles) responsible for implementing or overseeing procedures set for each type of investigation, considering that:
  - different people may be identified for investigations into different risk areas or parts of the organization,
  - different people may head up the team depending on the type of investigation, and
  - some investigations will need to be completely managed by external legal counsel.

R3.4.02

- Establish a list of outside counsel selected or approved in advance to be consulted when the need for counsel in a particular type of investigation arises and establish procedures to engage such counsel if the need arises.

R3.4.03

- Utilize established rules, policies and procedure for the type of investigation to determine which people within the organization will be responsible for overseeing the organization's role in the investigation, dealing directly with investigators, and leading the internal investigation team.

R3.4.04

- Establish procedures to screen all selected team members to ensure no conflict of interest or bias in the type of investigation and continually revisit as information arises.

R3.4.05

- Establish policies that ensure team members have clear authority and that their authority will be expressed to all personnel who may have to respond to their requests for information, documents, or interviews.

R3.4.06

- Establish policies and procedures that ensure team members are relieved of other duties as necessary to provide time required to participate effectively in the investigation.

R3.5 PREPARE TO RESPOND TO SPECIFIC THIRD-PARTY INVESTIGATIONS

Establish procedures for developing a response to a specific investigation.

Core Sub-practices

R3.5.01

- Establish procedures to determine whether there is an obligation to immediately disclose the existence of a specific investigation to the Board, independent auditors, regulatory agencies, creditors or insurers under agreements, contracts or established policies and procedures.

R3.5.02

- Prepare a standard response management plan for each type of investigation, which may be modified based on specific investigation facts and circumstances, which addresses procedures to:
  • collect or identify all requested documents and data and initiate document holds to stop any routine destruction or removal,
  • document exactly what is provided to the third party,
  • track information that will be released as non-privileged, indicating that the release is intentional and controlled,
  • track list of released items being maintained as privileged,
  • determine individuals who will need to be interviewed to fulfill investigation requests, both current personnel of the organization and former employees or agents,
  • determine if any requests for information will be refused and develop that response under legal review,
  • determine the need to negotiate confidentiality agreements regarding certain information to be delivered to the third party and whether the organization needs to seek to provide any privileged information under seal,
  • inform individuals involved in the investigation as witnesses, interviewees or otherwise, that in-house and outside counsel represent only the organization and not them individually, and document that they understand, and
  • internally and externally communicate investigation results and recommended actions.

R4 CRISIS RESPONSE

R4

Plan for and respond to crisis issues, business disruption and other significant events.

Principles

01 Protecting individuals from physical harm is essential.

02 Having a broad view of where interruption could arise is critical.

03 Business, IT, emergency management, public affairs, communications, and continuity personnel should design integrated plans.

04 Constant, clear and redundant communication is essential to successful crisis management.

05 Practice crisis response to a variety of issues including: Environmental hazards (fire, hurricane, etc.), accidents, workplace violence, data loss / breech, fraud or corruption by senior executives.

Critical Success Factors

01 Establish and practice plans to address reasonably anticipated types of crises

02 Involve all relevant internal and external roles in the planning stage

03 Communicate timely and appropriate information to relevant stakeholders during implementation of a crisis plan

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

R4.1 Develop Crisis Response and Continuity Plans

R4.2 Identify Crisis Readiness and Response Teams

R4.3 Test Plans and Procedures

R4.4 Coordinate Plans

Key Deliverables

Plans Crisis, Continuity and Recovery Plan

Reports Findings and Recommendations Report

R4.1 DEVELOP CRISIS RESPONSE AND CONTINUITY PLANS

Develop the plans for responding to various types of crises and recovering from business disruption.

Core Sub-practices

R4.1.01

- Identify the types of crises that might arise and create a list of specific examples of ones deemed to be either likely or of significant impact if they were to occur, including events with crisis level impacts on:
  • a physical plant or infrastructure such as weather disasters, accidents or intentional harm to structures,
  • access to data such as physical disruption to servers or technology failure,
  • protection of confidential or personally identifiable information such as theft or breach of confidential or personally identifiable data,
  • ability to operate such as technology or power interruptions, political upheaval,
  • public confidence in products or services,
  • reputation,
  • workforce such as health crises, and
  • the enterprise, the community or individuals from violent criminal conduct.

R4.1.02

- Develop business impact analysis for each listed type of crisis by:
  • refining internal and external context and risk analysis,
  • analyzing implications of loss, delay, inability to access or serve key people, systems, processes, suppliers, customers, and business partners, and
  • analyzing anticipated information loss based on archive/back-up strategies for systems and processes.

R4.1.03

- Address business continuity and recovery goals for each type of crisis by:
  • determining recovery time objectives,
  • prioritizing key business processes and critical functions,
  • selecting and documenting business continuity strategies for interim operations and recovery plans,
  • documenting information systems interim operations and recovery plans, and
  • documenting facilities interim responses and recovery.

R4.1.04

- Establish detailed response and recovery plans for each type of crisis that include the following:
  • in the case of a physical crisis, policies and procedures for coordination with first responders from local authorities on plans, procedures, and communication protocols so they can facilitate safety, rescue and emergency operations,
  • in the case of potential allegations of criminal conduct, procedures for interactions with police or prosecution authorities,
  • in the case of a data management disruption or failure, disaster recovery plans,
  • an identified communications plan and team, including legal, public relations and investor relations as appropriate,
  • policies and procedures to direct public disclosures and communications through identified organization representatives, and involve legal, public relations and investor relations as appropriate,
  • procedures for establishment of crisis response headquarters away from danger/crisis area,
  • policies and procedures that prioritize physical safety of employees and family member communications,
  • procedures to evaluate pursuing contractual or other legal rights to demand indemnification or file claims for insurance,

and

• procedures to analyze response effectiveness and performance after action.

R4 CRISIS RESPONSE

R4.2 IDENTIFY CRISIS READINESS AND RESPONSE TEAMS

Define personnel who will be responsible for crisis preparedness and those who will be deployed as crisis response teams for each type of identified crisis.

Core Sub-practices

R4.2.01

- For each type of crisis, identify the personnel who will have responsibility for maintaining readiness and monitoring for signs of impending crisis.

R4.2.02

- For each type of crisis, identify a preliminary response team in each location, amending to stay fresh as necessary to address personnel changes.

R4.2.03

- Identify leadership that is accountable for communicating with the workforce, families and external stakeholders for each type of crisis.

R4.2.04

- Determine succession authorities in the event that an individual with established authority is unavailable when a crisis arises.

R4.3 TEST PLANS AND PROCEDURES

Test and evaluate the various crisis plans and procedures.

Core Sub-practices

R4.3.01

- For each type of crisis, define a preparedness exercise plan, including:
  - scope of the exercise,
  - frequency of the exercise,
  - accountability for the preparedness exercise,
  - who will be involved, including any personnel new to the crisis management team, and
  - how the practice response will be evaluated.

R4.3.02

- Select appropriate preparedness exercise type including:
  - tabletop scenarios,
  - simulations, and
  - activation exercises.

R4.3.03

- Conduct exercises according to plan.

R4.3.04

- Evaluate performance against the plan and effectiveness of the response.

R4.4 COORDINATE PLANS

Coordinate the various continuity and response plans in anticipation of business disruption that may span more than one facility.

Core Sub-practices

R4.4.01

- Correlate local, regional and national plans.

R4.4.02

- Coordinate and rationalize recovery time objectives across plans of individual functions, departments, business units or facilities with projected resource availability.

R4.4.03

- Rationalize recovery time objectives with information systems recovery capabilities.

R5 REMEDIATION

R5

Resolve substantiated issues by fixing any weaknesses in the capability and disciplining individuals and organizations at fault.

Principles

01 The assurance that each reported issue/incident is resolved is essential to maintain credibility.

02 Responses should address the immediate issue and the underlying root causes identified, including changes to management actions and controls if necessary

03 Disciplinary measures that are applied consistently and objectively serve as deterrents.

Critical Success Factors

01 Provide timely notification about resolution of the issue to relevant internal and external stakeholders.

02 Make changes to decisions, processes or resources that contributed to or allowed the incident or issue to occur.

03 Establish a process to record and ascertain disciplinary actions and ensure that discipline is consistently applied and escalates for involvement in multiple issues.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

R5.1 Remediate the GRC capability

R5.2 Discipline Individuals

R5.3 Disclose Issue Resolution

Key Deliverables

Matrices Prioritized Risk Matrix

Reports Filings, Findings and Recommendations Report

R5.1 REMEDIATE THE GRC CAPABILITY

Resolve each reported issue/incident, document the outcome, and propose appropriate changes to the GRC capability to avoid similar issues in the future.

Core Sub-practices

R5.1.01

- Propose changes to the GRC capability to remediate points of failure that contributed to the issue or incident.

R5.1.02

- Document results including: • outcome categories, • root cause, • resolution, and • remediation.

R5.1.03

- Resolve reported issues/incidents using corrective action processes.

R5.1.04

- Revise the prioritized risk matrix to reflect the effect of detected issues and remediation activities on:
  • identified current optimization activities, and
  • likelihood and probability analysis of current and planned residual risk.

R5.2 DISCIPLINE INDIVIDUALS

Discipline individuals for misconduct.

Core Sub-practices

R5.2.01

- Define and enforce a procedure and criteria for consistent discipline given type of misconduct.

R5.2.02

- Administer appropriate discipline under applicable policies, procedures, laws, and regulations.

R5.2.03

- Track discipline decisions and include in workforce files and extended enterprise relationship records.

R5.2.04

- Periodically report to the Board on material disciplinary measures taken (and underlying facts and circumstances).

R5.2.05

- Periodically review past disciplinary actions to ensure consistency.

R5.3 DISCLOSE ISSUE RESOLUTION

When required or appropriate, disclose findings and resolution of investigations to stakeholders.

Core Sub-practices

R5.3.01

- As required, disclose results of investigations to external stakeholders.

R5.3.02

- Establish procedures to voluntarily disclose results and resolution of investigations to internal and external stakeholders as appropriate, including:
  - regulatory agencies,
  - enforcement authorities,
  - investors / underwriters,
  - customers, and
  - workforce.

R5.3.03

- Provide single point of communication with external stakeholders.

R5.3.04

- Inform stakeholders about resulting changes to the GRC capability.

R6 REWARDS

R6

Recognize and incentivize those who contribute to positive outcomes including achievement of performance, risk and conformance targets

THIS ELEMENT IS UNDER DEVELOPMENT.

M MEASURE

M

Monitor, measure and modify the capability on a periodic and ongoing basis to ensure that management actions and controls reliably achieve objectives while addressing uncertainty and acting with integrity.

M1 Context Monitoring

- ***M1.1*** Monitor External Context
- ***M1.2*** Monitor Internal Context

M2 Performance Monitoring

- ***M2.1*** Monitor and Evaluate Capability Design
- ***M2.2*** Review and Reconsider Risks
- ***M2.3*** Identify Relevant Actions and Controls
- ***M2.4*** Analyze Potential for Failure
- ***M2.5*** Identify Monitoring Information
- ***M2.6*** Perform Monitoring Activities
- ***M2.7*** Analyze and Report Monitoring Results

M3 Systemic Improvement

- ***M3.1*** Develop Improvement Plan
- ***M3.2*** Implement Improvement Initiatives

M4 Assurance

- ***M4.1*** Plan Assurance Assessment
- ***M4.2*** Perform Assurance Assessment

M1 CONTEXT MONITORING

Monitor and analyze changes in the internal and external context to determine if the capability requires change.

Principles

01 The capability must be flexible enough to respond rapidly to changes in the external and internal context in which it must operate.

02 Failure to recognize and respond to context changes may result in failure of critical capability management actions and controls.

03 The capability will be most effective if the organization identifies and evaluates anticipated changes in context in time to plan changes.

Critical Success Factors

01 Monitor the external and internal context for potential, planned and actual changes that could render any aspect of the capability ineffective

02 Assign clear accountability for tracking each aspect to identify and analyze changes

03 Develop multiple channels and resources to ensure that changes to the external and internal contexts are identified in a timely

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

M1.1 Monitor External Context

M1.2 Monitor Internal Context

Key Deliverables

Matrices Prioritized Risk Matrix

Plans Integrated Plan

Reports Findings and Recommendations Report

M1.1 MONITOR EXTERNAL CONTEXT

Continually monitor changes in the external environment that may have a direct, indirect or cumulative effect on the organization.

Core Sub-practices

M1.1.01

- Monitor stakeholder groups for changes in views and key individuals.

M1.1.02

- Monitor market conditions.

M1.1.03

- Monitor industry participants and competitors for risk and compliance issues.

M1.1.04

- Monitor other peers as defined by similar workforce size, similar business activities, and similar geographic scope for risk and compliance issues.

M1.1.05

- Monitor geopolitical changes in all relevant areas of operation.

M1.1.06

- Monitor changes in external requirements including those from:
  - laws, rules and regulations,
  - administrative guidelines and rulings,
  - significant judicial rulings,
  - regulatory guidance,
  - prosecutorial guidance,
  - legal interpretations,
  - consent orders and integrity agreements, and
  - enforcement activities,
  - contracts,
  - standards, and
  - trade association commitments.

M1.1.07

- Monitor changes in customary practices in the industry, and cultural differences in the relevant locations.

M1.1.08

- Notify individuals responsible for relevant risk optimization activities about context changes, including those that require immediate consideration.

M1.1.09

- Individuals responsible for risk analysis and optimization activities augment or revise the prioritized risk matrix and risk optimization plan to reflect, as appropriate:
  - changes in the form of additional, altered or eliminated risks and requirements,
  - revised inherent risk analysis,

- current residual risk analysis,
- categorization and prioritization,
- risk optimization strategy,
- risk optimization activities, and
- planned residual risk.

M1.2 MONITOR INTERNAL CONTEXT

Continually monitor changes in the internal environment that may have a direct, indirect or cumulative effect on the organization.

Core Sub-practices

M1.2.01

- Monitor significant changes in business strategy such as:
  - changes in business objectives, values and strategy,
  - new product development,
  - expansion into new markets, and
  - mergers and acquisitions.

M1.2.02

- Monitor changes in personnel.

M1.2.03

- Monitor changes in processes.

M1.2.04

- Monitor changes in technology.

M1.2.05

- Monitor changes in culture including any significant variance of culture metrics in business units, departments, jobs, or locations.

M1.2.06

- Notify individuals responsible for relevant risk optimization activities about context changes, including those that require immediate consideration.

M1.2.07

- Individuals responsible for risk analysis and optimization activities augment or revise the prioritized risk matrix and risk optimization plan to reflect, as appropriate:
  - changes in the form of additional, altered or eliminated risks and requirements,
  - revised inherent risk analysis,
  - current residual risk analysis,
  - categorization and prioritization,
  - risk optimization strategy,
  - risk optimization activities, and
  - planned residual risk.

M2 PERFORMANCE MONITORING

M2

Monitor and periodically evaluate the performance of the capability to ensure that it is designed and operated to be effective, efficient, and responsive to the changing external and internal context.

Principles

01 Continuous monitoring of key aspects and periodic evaluation enables management and the Board to determine if the capability operates effectively and efficiently over time.

02 Monitoring provides evidence to support assertions about the effectiveness of the capability.

03 Evaluation of capability design and operation is part of the management responsibility to assure timely system corrections and improvements.

Critical Success Factors

01 Consider effectiveness of the capability to govern, manage and audit performance, risk and compliance; do not limit efforts to reviewing effectiveness of preventing or detecting conduct that would give rise to criminal or civil liability

02 Evaluate indicators that assess efficiency, responsiveness, flexibility and resiliency of the capability

03 Periodically re-evaluate the design of the capability to ensure it remains appropriate in light of changed circumstances

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

M2.1 Monitor and Evaluate Capability Design

M2.2 Review and Reconsider Risks

M2.3 Identify Relevant Actions and Controls

M2.4 Analyze Potential for Failure

M2.5 Identify Monitoring Information

M2.6 Perform Monitoring Activities

M2.7 Analyze and Report Monitoring Results

Key Deliverables

Plans GRC Strategic Plan, Integrated Plan

Reports Findings and Recommendations Report

M2.1 MONITOR AND EVALUATE CAPABILITY DESIGN

Establish a schedule for periodic re-evaluation of the appropriateness of the capability design in light of objectives, opportunities, threats and requirements.

Core Sub-practices

M2.1.01

- Define aspects of the GRC capability design to be periodically re-evaluated, including:
  • effectiveness in preventing and detecting conduct or events that violate mandated or voluntarily established requirements,
  • efficiency of the controls established as part of the system,
  • appropriateness of the selected controls relative to the level of risk, and
  • responsiveness of the system.

M2.1.02

- Select appropriate monitoring methods for each aspect of the GRC capability based on identified goals, assurance level and privilege status, such as:
  • technologies to flag incidents of non-conformance to established procedures,
  • periodic review of samples of reports, forms, or other required documentation,
  • periodic review of established metrics and performance indicators, and
  • periodic review of testing controls information.

M2.2 REVIEW AND RECONSIDER RISKS

Review any previously assessed or newly identified risks and reconsider, or assess for the first time, their priority based on the best information currently available.

Core Sub-practices

M2.2.01

- Analyze information from prevent, detect and respond activities including completed and ongoing investigations.

M2.2.02

- Analyze information from human capital control activities.

M2.2.03

- Analyze information from context monitoring.

M2.3 IDENTIFY RELEVANT ACTIONS AND CONTROLS

Review the related actions and controls in place to address high priority objectives, threats, opportunities and requirements.

Core Sub-practices

M2.3.01

- Identify the key risk optimizing activities whose failures may not be detected in a timely manner (single points of failure).

M2.3.02

- Identify the risk optimizing activities whose failure might trigger the failure of other risk optimizing activities (points of cascading failure).

M2.3.03

- Identify the risk optimizing activities that may compensate for failures in other key optimizing activities (key compensating activities).

M2.3.04

- Identify other related risk optimizing activities.

M2.4 ANALYZE POTENTIAL FOR FAILURE

Analyze the potential that risk-optimizing activities will fail and the ways in which they might fail.

Core Sub-practices

M2.4.01

- Analyze the relative complexity of the control as controls that are more complex typically have a higher degree of potential failure.

M2.4.02

- Analyze the skills required to perform a control and the availability of these skills, as skills shortages will quickly affect these controls.

M2.4.03

- Analyze the degree of automation versus manual execution of the control as:
  • Manual controls are more prone to human error than automated controls, and
  • Automated controls are more prone to voluminous and repeated error if there is a systemic issue.

M2.4.04

- Analyze prior failures associated with controls.

M2.5 IDENTIFY MONITORING INFORMATION

Identify the information to use to support the evaluation of the performance of the risk optimizing activity(s) and/or the overall performance of the GRC capability.

Core Sub-practices

M2.5.01

- Identify persuasive information that can be used to conclude that a risk optimizing activity is effective, efficient and responsive.

M2.5.02

- Consider direct information from monitoring the external and internal environments.

M2.5.03

- Consider direct information about substantiated incidents and general patterns of misconduct.

M2.5.04

- Consider direct information from testing controls.

M2.5.05

- Consider indirect information generated by business processes for operational purposes.

M2.5.06

- Ensure that information is sufficient, relevant, reliable, and timely obtained.

M2.5.07

- Determine what information may be reviewed by samples and what information requires complete review.

M2.5.08

- Determine what information must be considered that is not contained in reviewable documents or date, and determine methods for reviewing such information such as interviews or surveys.

M2.6 PERFORM MONITORING ACTIVITIES

Perform monitoring activities to support the evaluation of the performance of the system.

Core Sub-practices

M2.6.01

- Review identified documents and samples of data.

M2.6.02

- Conduct identified interviews and surveys.

M2.6.03

- Consolidate information from different sources to enable comparison and analysis.

M2.7 ANALYZE AND REPORT MONITORING RESULTS

Analyze the results of monitoring activities to identify instant weaknesses and opportunities for systemic improvements.

Core Sub-practices

M2.7.01

- Identify and analyze reasons for conflicting information.

M2.7.02

- Determine validity and reliability of information.

M2.7.03

- Determine if misconduct or control failures are occurring beyond established acceptable tolerances.

M2.7.04

- Determine if a number of instances of misconduct or control failures relate to a particular location, supervisor or manager, or individual.

M2.7.05

- Determine if a number of control failures relate to a particular process, human capital, technology, or physical control.

M2.7.06

- Report on the results and general proposed responses to appropriate internal and external stakeholders.

M3 SYSTEMIC IMPROVEMENT

M3

Use information from periodic monitoring as well as ongoing detection activities to identify opportunities for capability improvements.

Principles

01 Continual improvement is the hallmark of a mature and high performing capability.

02 Improvement efforts allow for implementation of innovations as they become available.

03 Budgeting for regular improvement activities enables continual capability maturation and efficiency.

Critical Success Factors

01 Actually ACTING on identified improvement opportunities.

02 Establish clear ownership of improvement projects

03 Include change management activities in all improvement plans to ensure that people are aware and accepting of changes.

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

M3.1 Develop Improvement Plan

M3.2 Implement Improvement Initiatives

Key Deliverables

Matrices Prioritized Risk Matrix

Plans GRC Strategic Plan, Integrated Plan

Reports Findings and Recommendations Report

M3.1 DEVELOP IMPROVEMENT PLAN

Develop a prioritized plan for implementing improvements to the program.

Core Sub-practices

M3.1.01

- Develop portfolio of improvement initiatives.

M3.1.02

- Communicate improvement plan to management.

M3.1.03

- Define any recommendations from investigation outcome reports that are not in improvement plan and provide explanation(s).

M3.1.04

- Obtain authorization to execute improvement plan.

M3.2 IMPLEMENT IMPROVEMENT INITIATIVES

Implement the specific action plans and initiatives intended to improve the program.

Core Sub-practices

M3.2.01

- Adapt existing priorities and plans to accommodate additions.

M3.2.02

- Enhance change management and program management capability as needed for additional initiatives.

M3.2.03

- Engage resources for initiatives.

M3.2.04

- Manage initiatives pursuant to project plans.

M3.2.05

- Periodically report on project and portfolio status.

M3.2.06

- Confirm that initiatives were complete as defined in the improvement plan.

M3.2.07

- Assess whether targeted improvements are achieved.

M3.2.08

- Document changes to the GRC capability, including changes, if any, to the GRC strategic plan, prioritized risk matrix, and the risk optimization plan.

M4 ASSURANCE

M4

Provide assurance to management and the Board that the capability is reliable, effective, efficient and responsive.

Principles

01 Management and the Board need independent reasonable assurance about the effectiveness and performance of the capability.

02 Either internal auditors or external auditors or evaluators may provide assurance -- keeping in mind that level of assurance will be affected by degree of objectivity.

03 The degree of assurance desired may vary at different times and for different purposes.

04 The degree of assurance increases as the level of independence and capability of the assessor increases, and is further enhanced by the use of independent, objective standards or agreed upon procedures for review.

Critical Success Factors

01 Use objective, skilled assurance personnel with experience in the subject matter of the assessment

02 Ensure independence of assurance personnel

03 Use risk assessment to focus the assurance effort

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

M4.1 Plan Assurance Assessment

M4.2 Perform Assurance Assessment

Key Deliverables

Reports Findings and Recommendations Report

M4.1 PLAN ASSURANCE ASSESSMENT

Determine scope, procedures and criteria required to provide desired level of assurance.

Core Sub-practices

M4.1.01

- Determine scope of review.

M4.1.02

- Determine level of assurance desired.

M4.1.03

- Based on schedule, cost and objectives, determine whether to define standards, procedure and criteria or to use objective, independently issued standards or agreed upon procedures for review, and if so, identify them.

M4.1.04

- Identify parties to perform assessment that supports the assurance.

M4.2 PERFORM ASSURANCE ASSESSMENT

Perform procedures, evaluate results against criteria and deliver report.

Core Sub-practices

M4.2.01

- Review monitoring reports and changes to the GRC capability previously undertaken by management as part of the assurance process.

M4.2.02

- Prepare an assurance report and recommendations for management and the Board.

I INTERACT

I

Enable the capability with technology and manage information so that it efficiently and accurately flows up, down and across the organization, extended enterprise, and to appropriate stakeholders.

I1 Information Management

- ***I1.1*** Develop a GRC Information Management Classification Structure
- ***I1.2*** Develop GRC Information Collection Policies & Procedures
- ***I1.3*** Develop GRC Information Access, Use and Transfer Policies & Procedures
- ***I1.4*** Develop GRC Information Storage & Disposition Policy & Procedures

I2 Communication

- ***I2.1*** Develop Reporting Plan
- ***I2.2*** Develop Communication Plan

I3 Technology

- ***I3.1*** Assess Technology Needs and Gaps
- ***I3.2*** Develop GRC Technology Portion of GRC Strategic Plan

11 INFORMATION MANAGEMENT

Implement and manage an information management system so that capability information is relevant, reliable, timely, secure and available.

Principles

01 Information should be reconciled and consistent across the organization to allow for efficient and accurate flow of information across the organization and to external stakeholders.

02 It is not necessary to have a single record management system across the organization, if management designs and operates multiple systems to allow the efficient reconciliation, consolidation and exchange of information.

03 Consistent definitions of terms and taxonomies ensure that different parts of the organization do not have different understandings of information, or are not operating on conflicting sets of information.

04 Data hoarding or failure to transfer relevant and necessary information to all parts of the organization that need the information is damaging.

Critical Success Factors

01 Use common definitions of terms and taxonomies to create, exchange and store information

02 Enforce a uniform information management system or systems from which information can be easily combined, compared or shared

03 Establish consistent policies and procedures regarding the retention and retrieval of information.

04 Consider additional controls that may be needed when information is maintained outside the organization

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

11.1 Develop a GRC Information Management Classification Structure

11.2 Develop GRC Information Collection Policies & Procedures

11.3 Develop GRC Information Access, Use and Transfer Policies & Procedures

11.4 Develop GRC Information Storage & Disposition Policy & Procedures

Key Deliverables

Plans Crisis, Continuity and Recovery Plan, GRC Information Management Plan

11.1 DEVELOP A GRC INFORMATION MANAGEMENT CLASSIFICATION STRUCTURE

Determine the definitions, classifications and procedures necessary to identify and manage GRC information in the organization and extended enterprise, as part of an Information Management Plan.

Core Sub-practices

11.1.01

- Define GRC capability records (GRC Records).

11.1.02

- Define and maintain a classification schema and methodology.

11.1.03

- Define an ongoing process for information inventory and classification including characteristics such as:
  - type,
  - privacy requirement,
  - confidentiality requirement,
  - preservation requirement,
  - retention requirement,
  - disposition requirement,
  - availability requirement,
  - operational/strategic value,
  - data owner,
  - source of information (data base/application, email, Excel, etc.),
  - associated business processes, and
  - associated policies.

11.1.04

- Periodically consider changes to the classification structure, and its underlying definitions and classifications, to reduce future reconciliation needs.

11.2 DEVELOP GRC INFORMATION COLLECTION POLICIES & PROCEDURES

Establish the policies and procedures necessary to collect GRC information from sources within and outside the organization and extended enterprise, as part of an Information Management Plan.

Core Sub-practices

11.2.01

- Define rules and procedures to meet requirements regarding collecting and creating information.

11.2.02

- Define policies and procedures regarding information ownership.

11.2.03

- Define a procedure and schedules or triggers for reconciling disparate information.

11.2.04

- Reconcile disparate information upon scheduled or triggering events.

11.3 DEVELOP GRC INFORMATION ACCESS, USE AND TRANSFER POLICIES & PROCEDURES

Establish the policies and procedures necessary to access, use and transfer GRC information in the organization and extended enterprise, as part of an Information Management Plan.

Core Sub-practices

11.3.01

- Define rules and procedures to meet requirements regarding managing access, authorization and authentication, including:
  - evaluation of the level of access required,
  - data owner approval,
  - administration of access (add, change, remove),
  - password requirements,
  - authentication method, and
  - access to physical storage locations.

11.3.02

- Appropriately define, mark, handle and store privileged documents, deliverables, and artifacts.

11.3.03

- Define rules and procedures to meet requirements regarding the transfer of information.

11.3.04

- Define procedures for notification, containment and response to a breach of information management access and use procedures.

11.3.05

- Define data and security models for all systems designed to enable the processes and meet requirements.

11.4 DEVELOP GRC INFORMATION STORAGE & DISPOSITION POLICY & PROCEDURES

Establish the policies and procedures necessary to store GRC information in the organization and extended enterprise in accordance with requirements and recovery objectives, as part of an Information Management Plan.

Core Sub-practices

11.4.01
- Define rules and procedures to meet requirements regarding maintaining stored information.

11.4.02
- Define the rules and procedures to meet requirements regarding retention, destruction, restoration, and disposition of information.

11.4.03
- Determine off site media storage and media rotation requirements.

11.4.04
- Define information back up schedules (source, frequency).

11.4.05
- Define rules and procedures to meet requirements regarding systematic disposition of information.

11.4.06
- Define rules and procedures to meet requirements regarding manual deletion of information.

11.4.07
- Define a procedure for the disposition of data on recycled media/hardware.

11.4.08
- Define rules and procedures to meet requirements regarding identifying and halting destruction of information.

11.4.09
- Regularly test the restoration of data from back-up storage media.

11.4.10
- Define procedures for containment and response to a breach of information storage and disposition procedures.

12 COMMUNICATION

12

Deliver relevant, reliable, and timely information to the right audiences as required by mandates or as needed to perform responsibilities and effectively shape attitudes.

Principles

01 Effective flow of information throughout the organization enables decision-making and improves performance.

02 The organization should be able to deliver consistent information to those who need it, when they need to know it.

03 The organization must be able to meet its mandatory reporting obligations and to provide reliable and understandable information to stakeholders.

04 Not all communication takes place through formal reports and informal communication may have more impact.

Critical Success Factors

01 Monitor and manage requirements for timing and content of mandated external reports

02 Establish clear policies, procedures and triggers for immediate escalation or routine reporting of information within the organization or to external stakeholders

03 Maintain a complete and accurate record of how communication was managed

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

12.1 Develop Reporting Plan

12.2 Develop Communication Plan

Key Deliverables

Plans Communication and Reporting Plan

I2.1 DEVELOP REPORTING PLAN

Establish a plan to ensure compliance with mandatory reporting requirements and provide desired reports to management, the Board, and stakeholders.

Core Sub-practices

I2.1.01

- Identify required external reports to regulators and other stakeholders, and create a matrix indicating:
  - the schedules or triggering events for each,
  - the content required,
  - the location or source of the content required,
  - the person or office responsible for preparing and filing each report,
  - the location or classification of each report copy as it will be retained in the organization,
  - the record retention and protection rules, and
  - the method for confirmation of delivery and receipt.

I2.1.02

- Define internal reports needed to allow the entity to certify there are no violations of mandates or policies, and those needed to manage the GRC capability, and prepare a matrix indicating:
  - the schedules or triggering events for each,
  - the content required,
  - the location or source of the content required,
  - the person or office responsible for preparing each report,
  - the intended recipients of each report,
  - the location or classification of each report copy as it will be retained in the organization,
  - the record retention and protection rules, and
  - the need for confirmation of receipt.

I2.1.03

- Define any additionally desired voluntary reports to stakeholders and create a matrix indicating:
  - the schedules or triggering events for each report,
  - the content required,
  - the location or source of the content required,
  - the person or office responsible for preparing and filing each report,
  - the location or classification of each report as it will be retained in the organization, and
  - the record retention and protection rules.

I2.1.04

- Define policies and procedures regarding referral for review and resolution when reports reflect performance outside targets and tolerances.

I2.1.05

- Analyze existing reporting and determine gaps against the planned reports and their desired management.

I2.2 DEVELOP COMMUNICATION PLAN

Define how the organization will manage GRC related communications that are not formal reports.

Core Sub-practices

I2.2.01

- Prepare to develop a high level communication plan by:
  - defining current behavior/knowledge state of audience,
  - defining desired state,
  - analyzing gaps, and
  - identifying areas where there is likely to be resistance to change.

I2.2.02

- Develop a high level communication plan that identifies:
  - all key program messages with identified senders and target audiences,
  - the various communication pieces that will deliver each message, and
  - the high level delivery schedule and triggering events.

I2.2.03

- Determine what methods of communication should be used for each category of message, applying multiple methods for key messages and taking into consideration the purpose of the communication (education, persuasion, information, interview), such as:
  - paper based,
  - email,
  - websites,
  - postings,
  - live events or meetings,
  - video/audio broadcast, or
  - face-to-face personal communication.

I2.2.04

- For each communications piece:
  - develop communication/messaging objective and content,
  - obtain required approvals,
  - determine who will respond to questions,
  - determine the most effective method(s) of communication,
  - determine need for redundant communication (frequency and type),
  - define primary communication methods:
    - between GRC roles
    - between GRC roles and business roles, and
    - between GRC roles and external stakeholders.

I2.2.05

- Define communication/message interdependencies and how each fits into the overall landscape of other entity communications/messages.

I3 TECHNOLOGY

I3

Enable the capability with technology that integrates with and, where appropriate, uses existing investments.

Principles

01 Not everything has to be, or can be, automated; automate when it optimizes the organization's cost and risk and the GRC performance objectives.

02 Using consistent tools to deliver similar processes offers efficiency and more accurate information.

03 Planning for GRC solutions benefits from early IT involvement in designing approaches, strategies and controls.

04 A partnership between GRC professionals and IT professionals with common understanding of needs, processes, and capabilities is essential to implementing the right technology.

Critical Success Factors

01 Identify the technology requirements for GRC throughout the organization

02 Keep track of what technology solutions are currently used in the organization to address GRC needs

03 Assess existing technology components for applicability to identified needs

04 Include the GRC technology plan in the overall IT technology plan

Guidelines and Practices

Red Book 2.1 - GRC Capability Model

I3.1 Assess Technology Needs and Gaps

I3.2 Develop GRC Technology Portion of GRC Strategic Plan

Key Deliverables

Plans GRC Strategic Plan

I3.1 ASSESS TECHNOLOGY NEEDS AND GAPS

Identify gaps and underperforming systems in existing technology environment.

Core Sub-practices

I3.1.01

- Identify key processes controls that are less error-prone and more efficient if enabled by technology.

I3.1.02

- Define GRC technology requirements.

I3.1.03

- Understand existing technology environment.

I3.1.04

- Map functionality requirements to existing capabilities.

I3.1.05

- Identify redundancies in existing technology solutions.

I3.1.06

- Select among existing systems, the system(s) that best fit functionality requirements.

I3.1.07

- Identify unmet functional requirements.

I3.1.08

- Identify priorities for solution enhancement or additions.

I3.2 DEVELOP GRC TECHNOLOGY PORTION OF GRC STRATEGIC PLAN

Develop plan for implementing technology to enable GRC processes and information flows.

Core Sub-practices

I3.2.01

- Determine which technology solutions must share information or develop/store easily combined or compared information.

I3.2.02

- Decide what existing solutions can and should be enhanced or extended to apply to similar needs in other parts of the organization or GRC capability.

I3.2.03

- Decide what new solutions should supplement or replace existing solutions.

I3.2.04

- Decide whether to build or buy identified new solutions.

I3.2.05

- Develop a plan for the prioritized initiatives to build, buy, or enhance technology capabilities using IT methodologies (GRC Technology Plan).

I3.2.06

- Determine ownership and responsibility for ongoing resources and budget of enabling technology components.

I3.2.07

- Reconcile timeline conflicts between GRC technology implementation priorities and GRC strategic plan and IT strategic plan.

DEL.A - Authorizations

DEL.A.01 - External Authorizations

a grant of approval, authority or acceptance from an entity or geopolitical authority outside the control of the organization receiving it

Referenced in: P1 , D2

DEL.A.02 - Internal Authorization

a grant of approval, authority or acceptance from an individual vested with accountability or responsibility for a particular activity, function, process, or entity

Referenced in: O1 , O3 , D2

DEL.A.03 - GRC capability Charter

a document from a governing authority defining the purpose, objective and authorization of an individual or group to undertake activities within the specified scope

Referenced in: O1

DEL.A.04 - Segregation of Duties

a document reflecting that the responsibilities of some roles or positions should be kept distinct from the responsibilities of other roles or positions as a protective measure to prevent fraud, error, or conflict of interest

Referenced in: O3 , P1

DEL.D - Descriptions

DEL.D.01 - Role / Job Descriptions

a detailed explanation of the responsibilities and expectations of an individual in a particular role or job, generally including:
• accountabilities and supervisor/oversight responsibilities,
• reporting obligations,
• individual performance measure and objectives, and

• skills, qualifications and experience.

Referenced in: O2 , P1

DEL.D.02 - GRC Technology Data Model Descriptions

a document describing the structure and relationships among data within a key GRC Technology Component

Referenced in: P1

DEL.D.03 - Helpline FAQ Descriptions

a complete, detailed description of the questions that are frequently asked to the helpline, together with the preferred guidance and any information or related resources to provide to the caller or of use to the helpline staff

Referenced in: P4

DEL.D.04 - Exit Interview Checklist

A document listing the activities to be conducted and questions to be asked during an interview with an internal stakeholder before his/her departure from the organization

Referenced in: D1

DEL.I - Internal Standards

DEL.I.04 - Control Taxonomy

A common vocabulary for describing the categories of controls along several dimensions:

Dimension 1
- preventive,
- detective and
- corrective controls

Dimension 2
- process
- human capital
- technology
- physical controls

Referenced in: D1

DEL.M - Matrices

DEL.M.01 - Policies and Related Procedures Matrix

a table correlating each policy to its attributes and other policies or procedures, and, optionally, to the training, reports or other sources for evidence of compliance

Referenced in: P1 , P3

DEL.M.02 - Prioritized Risk Matrix

a table correlating each risk to its attributes such as:
- classification or prioritization,
- sources of risk (event, trend, requirement, etc.),
- inherent risk analysis (likelihood, impact, duration),
- current implemented optimization activities,
- current residual risk analysis (likelihood,impact, duration),
- planned optimization activities, and
- planned residual risk analysis.

Referenced in: A1 , A2 , A3 , P1 , P4 , P5 , P7 , R5 , M1 , M3

DEL.M.03 - Risk / Control Matrix

A listing of risks mapped to related proactive, detective and responsive actions and controls.

Referenced in: P1 , R1

DEL.P - Plans

DEL.P.01 - Awareness and Education Plan

a synopsis reflecting the order, timing, audience, and responsibility for all communications and educational activities to be undertaken over the course of a year or multiple years to promote general awareness of:
- the organization's commitment to meeting its GRC requirements;
- the GRC capability capabilities;
- the avenues for resolving questions about GRC responsibilities and expectations;

• the GRC capability activities designed to meet GRC requirements,and
• to educate regarding the specific responsibilities of the general workforce,the extended enterprise,and those in GRC specific roles.

Referenced in: P4

DEL.P.02 - Communication and Reporting Plan

a schedule that sets out the structures, processes and resources to deliver information (whether to inform or to persuade) to those with authority and responsibility to act at appropriate times to affect or monitor a program or initiative. A plan would include:
• target audience,
• objectives of the communication,
• method of delivery,
• timing of delivery,
• who is accountable and responsible for the communication and who should be consulted regarding the communication, and
• for a series of communications, the dependencies betweeen them and relative timing.

Referenced in: P6 , D2 , D3 , I2

DEL.P.03 - Crisis, Continuity and Recovery Plan

a document or series of documents that sets out the structures, processes, protocols and resources to respond to a crisis event, to deliver interim operations pending full resumption of business and to recover from the impacts of an adverse event. Such plans would include:
• names and contact information for key response personnel,
• identification and responsible owners of key assets, processes, systems, supply relationships, and customer relationships,
• designation of safety, evacuation coordinators and evacuation sites and paths,
• key stakeholder contact points (police, fire, utilities, media, employee representatives, investor relations, analysts, etc.), and
• components of this deliverable would include:
  • succession of authority;
  • emergency operations plan;
  • interim operations plan;
  • information systems recovery plan;
  • resumption of operations plan;
  • emergency operating procedures; and
  • test plans.

Referenced in: R4 , I1

DEL.P.05 - GRC Information Management Plan

a document that sets out the structures, processes and resources to manage GRC information through-out the information life-cycle. Would include:
• classification schema for records, and
• policies and procedures related to:

- capture of information;
- access, use and transfer of information; and
- storage, retention, disposition and retrieval of information.

Referenced in: I1

DEL.P.06 - GRC Strategic Plan

a document that details the structures, processes, technologies, resources, objectives and measures to establish and maintain the capability needed to achieve the mission and vision. Components would include:

- charter,
- mission / vision statement,
- outcomes and maturity milestones(with correlation to business objectives)
- business case,
- measurement strategy (metrics, indicators, calculation method, frequency of measurement, nature and frequency of reporting),
- organization chart,
- human capital / vendor relations plan (for implementation and ongoing operations),
- financial plan (start-up and operations),
- technology plan,
- assurance plan, and
- implementation plan.

Referenced in: C3 , O1 , O3 , M2 , M3 , I3

DEL.P.07 - Investigation Management Plan

a document that sets out the structures, processes, protocols and resources to perform and conclude an investigation. Plan would include:

- investigation governance structure,
- investigation team,
- communication and reporting plan,
- operating and communication procedures,
- budget,
- projected schedule of activities, and
- technology plan (for team management, investigation mangement, and information management).

Referenced in: R2 , R3

DEL.P.08 - Integrated Plan

a document that details the processes and resources allocated to reliably achieve objectives while addressing uncertainty and acting with integrity.

Referenced in: A3 , P1 , P4 , P5 , P7 , M1 , M2 , M3

DEL.P.09 - Specialized GRC Curriculum Plan

a synopsis reflecting the order and timing of all courses of study for each of the GRC capability roles and may include a detailed description of each course:
• name of course,
• course objectives,
• skills to be attained, and
• options for attendance (online, video, live) together with the skills pre-requisites for each course.

Referenced in: O2

DEL.P.10 - Corrective Control Activity Plan

A plan that details the steps to stop or slow an adverse event from impacting an organization; and restoring the system to a stable state.

Referenced in: R1

DEL.R - Reports

DEL.R.01 - Filings

an official document submitted to a governmental authority (administrative, regulatory, legislative or judicial).

Referenced in: P6 , D1 , R2 , R3 , R5

DEL.R.02 - Findings and Recommendations Report

a presentation or statement of the outcome of an activity or analysis together with recommendations for change and/or improvement.

Referenced in: P1 , P2 , P4 , P5 , D1 , D3 , R2 , R3 , R4 , R5 , M1 , M2 , M3 , M4

DEL.R.03 - Corrective Action Report

Listing of corrective control activities performed in the period under analysis, grouped by type of corrective control as well as category of adverse event corrected. Information from prior periods may be included for comparison and analysis.

Completed, ongoing and future activities should be details relative to plan.

Referenced in: R1

DEL.S - Statements of Position

DEL.S.01 - Code of Conduct

a guide linking an organization's values and principles with rules of professional conduct

Referenced in: P2

DEL.S.02 - Ethical Decisions Guidelines

the organization's recommendation on the factors to consider along with applicable requirements, policies and philosophies in determining the proper course of action when faced with an ethical dilemma

Referenced in: P2

DEL.S.03 - Mission/ Vision/ Values Statement

an oral or documented description of the main aims, core beliefs, values, intended future state and overall plan that guide the organization's actions and inspires people to act toward that future state

Referenced in: C4

DEL.S.04 - Statement of Organizational Objectives

a declaration of the tangible results that the organization expects to achieve through execution of its mission and vision

Referenced in: C4

GRC CAPABILITY MODEL™

OCEG is a nonprofit think tank that helps organizations drive Principled Performance by reliably achieving objectives while addressing uncertainty and acting with integrity

www.oceg.org

OCEG®
DRIVING PRINCIPLED PERFORMANCE®