Governance, Risk and Compliance

ISACA Monterrey

Sarah Adams, GRC Leader
Carlos Ruiz, SAP Specialist
Elias Rivera, Oracle Specialist
May 2013
Content

1. What is GRC
2. It’s All About Risk
3. Getting Started
4. Common GRC tools
   • SAP GRC
   • Oracle GRC
   • Accelus
   • Openpages
   • RSA Archer eGRC
5. Summary and Questions
What is GRC
Governance, Risk and Compliance (GRC)

GRC is a management model that promotes the criteria unification, as well as communication and collaboration between different stakeholders in the management and control of the organization.

**Governance**
- Strategy
- Goals and objectives
- Policies and procedures
- Structures and processes

**Risk Management**
- Identify risks
- Risk analysis
- Risk profiles
- Risk Monitoring
- Achievement of objectives

**Compliance**
- Comply with policy and procedures
- Laws and regulations
- Controls
- Activities

**Governance:**
- Manages the *risks to* the execution of the company strategy as well as the *risks from* the chosen strategy

**Risk management:**
- Determines the areas exposed to potential risks

**Compliance:**
- Is the tactical action to mitigate risk
GRC Stakeholders

Board and support committees
- Clear dissemination and consistent strategy, culture, policies and objectives
- Fast decision making and informed

Management team
Visions and uniform approaches
- Roles and responsibilities defined
- Ethics Program disseminated and applied uniformly

Comptroller
- Comprehensive risk management
- Effective and efficient internal control environment

Systems department
- Optimum level of safety
- Disaster recovery plans and business continuity plans
- Segregation of functions implemented in the systems according to the policies
- IT projects and acquisitions aligned with business strategy

Relationship with regulators
- Constant communication and collaboration "No surprises"

Legal
- Permanent tasks and coordinated
- Coordinated compliance efforts With a proactive approach

Finance
- Performance aligned to business objectives

Customer Relationship
- Clear vision of market trends and needs

Relations with suppliers
Scheduled and timely delivery

Internal Audit
- Audit plan aligned to the objectives of the organization
- Efficient audit programs
The value of GRC to your business

GRC promote the criteria unification, the effort coordination and collaboration between different characters involve in the direction of the organization through:

- The integration of the organs / government officials, administration and risk management, internal control and compliance
- Role and responsibility assignation to key personnel
- Communication channels formalization
- Applying a risk-based approach
- The implementation of a compliance program
## GRC Benefits and Organization Solutions

### Finance
- **CFO**
- Comptroller
- Finance Director
- Finance Manager

**GRC Benefits for CFO**
- Reduced time and cost for audits
- Quickly and easily Validation of compliance standards
- Reducing risk and increasing confidence in financial reporting
- Improved decision-making process through real-time diagnostics
- Generation of internal control guidelines in organizational culture

### IT
- **CIO**
- IT Director
- Application Manager
- Analyst DBA/Bus

**GRC Benefits for CIO**
- Management by exception, reducing time and costs incurred in compliance
- With less effort to respond to the compliance needs of business areas and internal audit
- Acceleration of the user provisioning process and ensures data security

### Internal Audit
- **Chief Audit Executive**
- Audit VP
- Audit Manager
- Internal Audit

**GRC Benefits for CAE**
- Quick identification of potential issues due to rapid authorization flow, giving greater visibility within the organization
- Reducing runtimes audit plans through self-managed reports and evidence centralized online
- Improved coordination and utilization of resources area
- Timely and accurate business operations (continuous monitoring)
- Improved process of remediation and risk management
It’s All About Risk
Risk Intelligence

Our GRC approach focuses on maintaining the right balance between risk and reward. An effective risk management program focuses simultaneously on value protection and value creation. We call an organization that has attained this advanced state of risk management capability a “Risk Intelligent Enterprise™.”

Deloitte’s Nine Principles for building a Risk Intelligent Enterprise

- Common Definition of Risk
- Common Risk Framework
- Roles & Responsibilities
- Transparency for Governing Bodies
- Common Risk Infrastructure
- Executive Management Responsibility
- Objective Assurance and Monitoring
- Business Unit Responsibility
- Support of Pervasive Functions

Risk Intelligent Enterprise™
The Risk Intelligent Maturity Model

Where are you on the maturity model?

Stages of risk management maturity

- Initial
  - Ad hoc/chaotic
  - Depends primarily on individual heroics, capabilities, and verbal wisdom
- Fragmented
  - Risk is defined differently at different levels and in different parts of the organization
  - Risk is managed in silos
  - Limited focus on linkages between risks
  - Limited alignment of risk to strategies
  - Disparate monitoring and reporting functions
- Top down
  - Identified risk universe
  - Common risk assessment/response approach developed and adopted
  - Organization-wide risk assessment performed
  - Action plans implemented in response to high-priority risks
  - Communication of top strategic risks to the senior management team
- Integrated
  - Risk management activities coordinated across business areas
  - Risk analysis tools developed and communicated
  - Enterprise risk monitoring, measuring, and reporting
  - Scenario planning
  - Opportunity risks identified and exploited
  - Ongoing risk assessment processes
- Risk Intelligent
  - Risk discussion embedded in strategic planning, capital allocation, product development, etc.
  - Early warning system to notify board and management to risks above established thresholds
  - Linkage to performance measures and incentives
  - Risk modeling

Representative attributes

Stakeholder value
Getting Started
The GRC Framework

Governance, Risk and Compliance

Corporate Governance Management
- Corporate Governance Model Evaluation
- Corporate Governance Model Remediation
- Corporate Governance Performance Monitoring

Risk Management
- Strategic and Entity Level Risk Assessment
- Alignment of Strategic and Entity Level Risks with Operational Controls
- Development of Risk Mitigation
- Risk Monitoring

Compliance Management
- Internal Control Matrix Development and Maintenance
- SoD Matrix Development and Maintenance
- Regulatory and Legislation Compliance Development and Maintenance
- Regulatory and Legislative Compliance Observance
- Internal Control Evaluation
- SoD Analysis
- Internal Control Monitoring
- SoD and Super User Access Monitoring
- Regulatory and Legislation Compliance Monitoring
Defining Your GRC Processes

Need a repeatable process, defined as any other process in your organization would be.

**Benefits**
- Institutionalization of integrated processes
- Standardization of activities across business units
- Defined roles and responsibilities

**Defining GRC Processes**
- Flowcharts and guidelines for to be state
- Workshops and design validation

- Details of activities
- Definition of policies and rules
- Use of best practices
- Creation of processes that are new to the client

Frameworks included: OCEG (Open Compliance & Ethics Group), GRC Model (Red Book), COSO, CoBIT, ERM, CPMC

- Key stakeholders
- Refine, revise
- Finalize policies, procedures and processes
- Cultural change and adoption!
Technology to Enable GRC

IT Infrastructure

- Integrated risk management user interface
- Risk intelligence – executive view
- Compliance management
- Risk management
- Performance management

Enterprise business integration

- Consolidated reporting layer
- Management layer
- Business process layer
- Control monitoring and testing layer
- Foundation and transaction source layer

Security

Business processes

Manual controls

Automated controls

Applications

Data

Infrastructure

© 2013 Galaz, Yamazaki, Ruiz Urquiza, S.C.
Know the Capabilities of Your Tool

Although the tool is the enabler, understand the features and functions of your tool BEFORE you start on this journey.

- Better questions
- Easier upload
- More integrated
- Take advantage of what you have
- Understand the journey you are on
Common GRC tools
SAP GRC
SAP BusinessObjects GRC

SAP GRC Suite

Risk Management
Risk identification and integral monitoring

Access Control
Segregation of duties, user automated provisioning, management of super users, roles and profiles

Process Control
Comprehensive management to document, testing, monitoring and certifying the company's internal control

Global Trade Services
Risk management globally (imports and exports)

SAP Business Objects

Environment, Health, and Safety Management
Environmental and safety regulations
SAP GRC Access Control

Enhance the access request and SOD risk analysis

Key Benefits

- Manage and control access to the SAP system suitable for the defined scope.
- Indicators to monitor segregation of duties conflicts and document compensating controls.
- Monitoring users with broad access (Firefighter) in the SAP system.
- Automatic authorization flow and identification of responsible management (high, low or changes) SAP user Mexico Technology.
- Analysis preventative segregation of duties for access creation.
SAP BusinessObjects GRC

SAP GRC Process Control

*Enhance the continuous monitoring and reduce risk*

Automates compliance monitoring, control and management of internal control within the company, helps improve the effectiveness of controls in IT systems and align processes and compliance control to risk prevention and efficiency requirements.

**Key Benefits**

- Support internal control areas, internal and external audit, the review of process controls and risks
- Scalable support of corporate internal control and compliance programs
- Improves performance through the identification, prioritization and focus on key risk areas.
- Achieve real-time visibility of all compliance activities and internal control.
- Protect business value with Continuous Monitoring – Automated Controls and robust policies.
- Accelerates audit cycles and reduces the cost of compliance with automation.
- Analyzes failures proactively monitors control and remediation.
SAP BusinessObjects GRC

SAP GRC Risk Management
*Preserves and enhances the value of your business*

Gives an overview of how risk factors can impact the value and business reputation. Risk Management helps identify key risk indicators and align them with events and their potential impact, so that on this basis make responsible use.

**Key Benefits**

- Enhance and support for the process of identification, measurement, monitoring and responding to business risk
- Understand the risk factors and their impact on the value, processes and business performance.
- Maps business objectives to indicators of value within the organization.
- Document and monitor Key indicators of compliance and risk mitigation
- Pictures executives and reporting
- Communication Process Control to mitigate risks with their respective controls
- Integration of surveys for identifying risks and / or opportunities
- Analysis of quantitative and qualitative risk
Common GRC tools
Oracle GRC
Oracle GRC

GRC Intelligence:
- Visibility into compliance readiness and responsiveness
- Risk and performance analytics and dashboarding
- Planning, modeling, reporting, and analysis of GRC activities

GRC Manager:
- Central GRC repository
- Documentation of critical business policies, processes, controls, risks, and issues
- Test plans and performance of control tests
- Automatic initiation of testing review and approval processes
- Capture and storage of test evidence

Application Access Controls Governor:
- SOD controls at the access point or entitlement level
- Simulation feature to report conflicts before deploying access model changes

Transaction Controls Governor:
- Allows continuous monitoring of policies, controls, and transactions within the Oracle ERP application

Preventive Controls Governor:
- Allows prevention of control violations from occurring and reduces expensive detection and remediation cycles

Configuration Controls Governor:
- Enforces data and application integrity
- Audit changes to key configurations and operational data

Oracle GRC Platform consists of three major components: GRC Intelligence, GRC Manager, and GRC Controls

GRC Intelligence

eGRC Manager

GRC Controls

Application Access Controls Governor

Configuration Controls Governor

Transaction Controls Governor

Preventive Controls Governor

Cross-Enterprise: Enables Integrated Risk and Compliance Management

Oracle Specific: Enables Control Automation and Continuous Monitoring
### Oracle GRC

#### Key Benefits

<table>
<thead>
<tr>
<th>Governance Risk and Compliance</th>
<th>Soft Benefits</th>
<th>Measurable Benefits</th>
</tr>
</thead>
</table>
|                               | • Avoid the pain of returning to significant deficiency or material weakness disclosure | **Cost Reduction**  
• Less internal / external audit costs related to security |
|                               | • Easier to detect fraud and respond quicker | • Less help desk resources to provision security and resets |
|                               | • Quality and reliability of Oracle generated audit reporting inherently more credible | • Consultant fees for form / workflow customization |
|                               | • Allows shift of ownership for access decisions from IT to Business Management | • Post-implementation remediation / rework |
|                               | • Enhanced security restrictions | • Form customization / workflow consulting |
|                               | • Ability to identify and prevent segregation of duty violations and to enforce segregation of duties compliance | • Configuration change management |
|                               | • Manage by exception; reduce time and cost of compliance | **Time Reduction**  
• Time spent on design/build/test/maintaining compliant security roles |
|                               | • Improved support of Internal Audit and LOB compliance needs with less effort | • Time spent testing authorization manager approvals |
|                               | • Consistent environments, full audit trail of changes, easier migration/upgrade | • Time spent validating compliance |
|                               | • Better decision making armed with real-time diagnostics due to timely and accurate information | • Time spent Sarbanes-Oxley, SOD, or any other initiative testing |
|                               | • Free up resources and time for core value-add activities; enhanced morale of finance staff | • Time spent conducting management review of access |
|                               | • Faster information flow and better visibility for quicker identification of potential issues | • Time to respond to user provisioning requests |
|                               | • Better utilization of audit resources and coordinated efforts | • Reduced audit time and efforts through self-service reporting and online centralized evidence |
|                               | • Fewer duplicate payments | **Costs**  
• Resources required for the implementation |
|                               | • Reduce/eliminate duplicate vendors and customers,… | • Hardware assumed under ERP infrastructure |
|                               | • Ability to identify and track changes to configurations; catch unexpected setup changes before going live | • Software license and maintenance costs |
|                               |                                                                                 | • Implementation team |
|                               |                                                                                 | • Upgrade costs |

- Soft Benefits
- Measurable Benefits
- Costs

© 2013 Galaz, Yamazaki, Ruiz Urquiza, S.C.
## Oracle GRC

### Why Oracle GRC?

**Differentiators for Oracle GRC Controls Suite**

<table>
<thead>
<tr>
<th>Product Function</th>
<th>Capabilities</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC Manager &amp; Intelligence</td>
<td>Manages GRC processes, integrating robust process management capabilities</td>
<td>Central repository of business policies, processes, controls, risks and issues</td>
</tr>
<tr>
<td></td>
<td>Capture internal and external performance metrics quickly &amp; accurately</td>
<td>Reduction in costs of proving risk and compliance effectiveness across the enterprise.</td>
</tr>
<tr>
<td></td>
<td>Fact-based continuous improvement</td>
<td>Provide network of linked controls embedded within business processes</td>
</tr>
<tr>
<td></td>
<td>Comprehensive Control Solution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deploy controls across user access, actions, sensitive configurations and transactions</td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>Define and enforce fine grain access &amp; SOD rules in business terms</td>
<td>Simplify segregation of duties enforcement with identification, prevention, simulation and remediation</td>
</tr>
<tr>
<td>Configuration Controls</td>
<td>Lock down &amp; monitor critical application setups against corporate standards</td>
<td>Deliver complete audit trail (When, Who, What &amp; Why) for changes to key configurations</td>
</tr>
<tr>
<td>Transaction Controls</td>
<td>Continuously monitor for fraud and errors in business transactions</td>
<td>Ensure accuracy, test against thresholds and search for anomalies</td>
</tr>
<tr>
<td>Preventive Controls</td>
<td>Deploy preventive UI controls on risky transactions and configurations</td>
<td>Proactively restrict access to sensitive data and route key changes for approval</td>
</tr>
<tr>
<td>Predefined Content for P2P and O2C processes, system administrator setups</td>
<td>Pre-built Business objects that represent key business entities across processes</td>
<td>Reusable, Business User Friendly terms to author new objects based on policies</td>
</tr>
<tr>
<td>Pre-built Connector to EBS and PSFT</td>
<td>Includes the ETL adapter plus 100s metadata object mappings to EBS and PSFT transactional and setup tables</td>
<td>Enables customers to build their own adapters using easy to understand business objects (meta-data) out of the box.</td>
</tr>
</tbody>
</table>
Oracle GRC

Oracle GRC Manager and Intelligence

Benefits
Oracle GRC Manager and Intelligence provide the opportunity to institute an end-to-end process to manage compliance activities.

Reduced cost and complexity
- Reduce cost and complexity by managing multiple global financial mandates with one system
- Rationalized multiple compliance requirement sources
- Top-down, risk-based modeling across business units

Reduced risk
- Top-down risk decisions and control across business units
- Accountability for processes and controls
- Improve risk responsiveness with timely control and performance analytics

Improved control management
- Integrated workflow solution for testing, assessment, and mitigation activities
- Risk performance metrics and reporting
- Event notification and tracking
Oracle GRC

Oracle GRC Controls

Oracle GRC Controls provide the opportunity to deploy automated continuous monitoring.

<table>
<thead>
<tr>
<th>GRC Module</th>
<th>Challenges</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Access Controls</td>
<td>Clients are unsatisfied with current state of application data access and</td>
<td>Automate the SOD/Access life cycle detection, analysis, remediation, deployment of preventive control, and compensating control to accommodate dynamic business requirements.</td>
</tr>
<tr>
<td>Controls Governor</td>
<td>security.</td>
<td></td>
</tr>
<tr>
<td>Configuration Controls</td>
<td>Clients have ineffective controls around system integrity and security.</td>
<td>Design and implement configuration controls on field value changes, action buttons, and sensitive data based on company policy and risk appetite.</td>
</tr>
<tr>
<td>Governor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Controls Controls</td>
<td>Clients have trouble monitoring controls to prevent error and fraud from</td>
<td>Design and implement automated transaction controls to validate application and systems control effectiveness, identify suspect transactions, and route to process owners for visibility before material issues arise.</td>
</tr>
<tr>
<td>Governor</td>
<td>happening.</td>
<td></td>
</tr>
<tr>
<td>Preventive Controls Controls</td>
<td>Clients struggle with master data maintenance.</td>
<td>Design and configure policy-based access to field data within the application to enforce mandatory fields, as well as address data privacy and protection of sensitive data.</td>
</tr>
<tr>
<td>Governor</td>
<td>Data privacy and protection of sensitive data often requires extensive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>application customization.</td>
<td></td>
</tr>
</tbody>
</table>
Common GRC tools
Accelus
Accelus GRC Enterprise Solutions

Solution built to handle the diverse requirements of internal audit, internal controls management, risk management, policy management, legal, and compliance professionals, the Thomson Reuters Accelus suite of products provides solutions for documentation and workflow, regulatory news and information, global compliance screening, board management, and regulatory disclosure.
Accelus Solution Suite

Key Benefits

- Provides visibility, transparency and oversight over GRC processes
- Monitor and track regulatory rule changes
- Mitigate risk hiding in client relationships and related human networks
- Identify and mitigate legal, regulatory and business risk
- Maintain effective policies and demonstrate supervision
- Streamline, audit, risk management, and internal control processes
- Efficiently address required regulatory disclosure deadlines
Common GRC tools

OpenPages
OpenPages

Is an integrated governance, risk and compliance platform that enables companies to manage risk and regulatory challenges across the enterprise. It provides a set of core services and functional components that span risk and compliance domains including operational risk, policy and compliance, financial controls management, IT governance and internal audit.
OpenPages

Key Benefits

Features

**Operational Risk**
- Identify, manage, monitor and high level reports
- Risk evaluation and self-assessments
- KRI, Scenario analysis

**IT Risk**
- IT risk evaluation
- Identified critical risk, controls and gaps

**Internal Audit**
- Definition, planning, execution and reporting audit for all business lines
- Automated workflows and configurable reports

Benefits

**Operational Risk**
- Reporting risk standardized
- Improve risk operational processes
- Improves visibility into risk exposure, reduces loss and improve business performance.

**IT Risk**
- IT risk and control management according to a business process
- Multiple risk silos unification

**Internal Audit**
- Empowers audit department
- Enables auditors to automate and manage internal audits, and conduct broader risk and compliance management activities.
Common GRC tools
RSA Archer eGRC
RSA Archer eGRC

RSA Archer eGRC solutions allow you to build an efficient, collaborative enterprise governance, risk and compliance (eGRC) program across IT, finance, operations and legal domains. With RSA Archer eGRC, you can manage risks, demonstrate compliance, automate business processes, and gain visibility into corporate risk and security controls.

Adapt enterprise governance, risk management, and compliance (eGRC) products to the Organization requirements, build applications, and integrate with other systems.
RSA Archer eGRC

Key Benefits

**Flexibility.** The Platform offers a point-and-click interface for building and managing business applications. Non-technical users can automate processes, streamline workflow, control user access, tailor the user interface and report in real-time.

**Unified.** Provides a common platform to manage policies, controls, risks, assessments and deficiencies across lines of business. This unified approach eases system complexity, strengthens user adoption and reduces training time.

**Collaborative.** The Platform enables cross-functional collaboration and alignment. Business users across IT, finance, operations and legal domains can work together in an integrated framework using common processes and data.
Summary and Questions
Deloitte se refiere a Deloitte Touche Tohmatsu Limited, sociedad privada de responsabilidad limitada en el Reino Unido, y a su red de firmas miembro, cada una de ellas como una entidad legal única e independiente. Conozca en www.deloitte.com/mx/conozcanos la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios profesionales de auditoría, impuestos, consultoría y asesoría financiera, a clientes públicos y privados de diversas industrias. Con una red global de firmas miembro en más de 150 países, Deloitte brinda capacidades de clase mundial y servicio de alta calidad a sus clientes, aportando la experiencia necesaria para hacer frente a los retos más complejos de los negocios. Cuenta con alrededor de 200,000 profesionales, todos comprometidos a ser el modelo de excelencia.

Tal y como se usa en este documento, “Deloitte” significa Galaz, Yamazaki, Ruiz Urquiza, S.C., la cual tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría, consultoría fiscal, asesoría financiera y otros servicios profesionales en México, bajo el nombre de “Deloitte”.

Esta publicación sólo contiene información general y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro, ni ninguna de sus respectivas afiliadas (en conjunto la “Red Deloitte”), presta asesoría o servicios por medio de esta publicación. Antes de tomar cualquier decisión o medida que pueda afectar sus finanzas o negocio, debe consultar a un asesor profesional calificado. Ninguna entidad de la Red Deloitte, será responsable de pérdidas que pudiera sufrir cualquier persona o entidad que consulte esta publicación.