GRC Strategy Services – Implementing a GRC program

Implementing a comprehensive and innovative governance, risk, and compliance (GRC) program enables organizations to address the multiple factors that are essential in managing and controlling enterprise risk. This includes factors such as:

- Regulatory changes
- Decentralized operating model
- High number of control failures
- Talent management changes
- Cost reduction

By adopting an effective GRC strategy, executives and risk leaders are able to challenge the way they think about, respond to, and manage risk. EY help you understand the risks related to your business strategy and how to best respond to those risks. Our tailored approach to GRC integrates risk and performance management in order to create a competitive advantage in terms of risk insight and performance improvement.

EY GRC Framework: EY's GRC framework takes into account our clients' risk strategy based on business objectives, risk performance management in order to create a competitive advantage in terms of risk insight and strategy and how to best respond to those risks. Our tailored approach to GRC integrates risk and enterprise risk. This includes factors such as:

- Implementing a comprehensive and innovative governance, risk, and compliance (GRC) program
- Talent management changes
- Decentralized operating model
- Ineffective use of ERP and GRC
- Fragmented risk and compliance functions
- Inadequate use of alignment and event response time
- Agile and scalable control environment
- Cost reduction in internal and external risk activities, including monitoring and remediation
- Reduction in disruption to the business
- Improved business performance and innovation via value-based risk management

The components of GRC

- **Governance, risk and compliance domains**
  - Strategic alignment and risk management
    - Governance and strategy
      - Organization
      - Policies and standards
    - Enterprise risk management
      - Business drivers and regulatory requirements
    - Program structure and guidelines
      - Process, controls and risk management and adoption
      - Managing processes, risks and controls
      - Tools and technology
  - Risk and controls establishment and management
    - Process, risk and control definition and adoption
    - Managing processes, risks and controls
    - Tools and technology
  - Monitoring and reporting
    - Compliance monitoring and reporting
    - Risk monitoring and reporting

**GRC Strategy Services**

**Defining GRC**

GRC is a set of functions that oversees and manages risks and compliance across the organization to reliably meet company objectives. It is not just about tools and technology.

**GRC "One View"**

<table>
<thead>
<tr>
<th>All risk and compliance areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
</tr>
</tbody>
</table>

**Governance**

- Control functions, Policy Governance bodies

**Risk**

- Risk analysis, risk assessments, risk register, loss and incident database

**Compliance**

- Requirement management, control testing, findings and exceptions, evidence management

**Value to clients**

- Resolution of immediate and long-term risk exposure
- Improved risk alignment and event response time
- Agile and scalable control environment
- Cost reduction in internal and external risk activities, including monitoring and remediation
- Reduction in disruption to the business
- Improved business performance and innovation via value-based risk management

**GRC framework details**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>Sub-component</th>
<th>Description</th>
<th>Component</th>
<th>Sub-component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic alignment and risk management</td>
<td>Governance and strategy</td>
<td>- Vision, mission and strategy for corporate GRC program</td>
<td>- Determine applicable regulatory, leading practices and internal requirements</td>
<td>Process, risk and control establishment and management</td>
<td></td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>- Corporate oversight structure for GRC program</td>
<td>- Identify and inventory organizational processes</td>
<td>- Identify and inventory organizational processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Define risk management methodology, definitions, tolerances and process</td>
<td>- Evaluation of specific risks and link to the processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Perform risk identification and assessment</td>
<td>- Identification of controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Define risk treatment processes (risk acceptance and remediation)</td>
<td>- Mapping of processes, risk controls and regulations into a coordinated framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Define key risk indicators (KRI) and key performance indicators (KPI)</td>
<td>- Consolide and standardize risk and assurance activities across functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business drivers and regulatory requirements</td>
<td>- Alignment between business objectives and GRC program</td>
<td>- Develop reporting processes for risk and compliance, as well as consolidation of processes, risk and control framework for regulatory, organizational or process changes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Key legal and regulatory requirements</td>
<td>- Information and information technology ownership and support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program governance organization</td>
<td>- Organization structure and associated roles, responsibilities and accountabilities</td>
<td>- ERM tool and technology plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Communication and awareness</td>
<td>- Technology ownership and support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Process for policy and standards availability, communication and enforcement across the organization</td>
<td>- GRC tool and technology plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring and reporting</td>
<td>- Define-Policy Management program</td>
<td>Periodic and continuous monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Define process for Policy review</td>
<td>- Define risk and compliance program reporting needs and cadence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Process for policy and standards availability, communication and enforcement across the organization</td>
<td>- Develop reporting processes for risk and compliance, as well as consolidation of processes, risk and control framework for regulatory, organizational or process changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Control functions can include Compliance, Internal Audit, Enterprise Risk Management.
We utilize existing team members

- We have an established and tested set of credentials of our work
- We can continue to identify opportunities to transform your organization and agency for long-term success.

We know your people, environment, processes, and technology.

- Experience implementing GRC across the Federal government.
- Skills in risk and controls evaluations.
- Knowledge of systems and technology integration.

Credentials of our work

- We understand and can leverage GRC technology to support your GRC program.
- We can assess and optimize business performance and risk.
- We can implement and sustain GRC initiatives effectively and efficiently.

Improving Business Performance through GRC:
- Opportunities exist to transform your governance, risk, and compliance program to realize cost savings and improve mission and business performance.

Leading Federal agencies have achieved successful results by focusing on:
- Shifting risk management focus to a cross-functional approach aligned to strategic risks and business performance measures.
- Standardizing GRC processes to enhance decision making and avoid unnecessary costs.
- Embracing GRC technology to execute processes effectively and efficiently.

It’s time to act now and position your organization or agency for long-term success.

A high-level GRC roadmap

<table>
<thead>
<tr>
<th>Illustrative example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stabilize</strong></td>
</tr>
<tr>
<td>- Establish governance</td>
</tr>
<tr>
<td>- Complete control rationalization/optimization</td>
</tr>
<tr>
<td>- Agree on long-term road map and identify “quick wins”</td>
</tr>
<tr>
<td>- Define business requirements</td>
</tr>
<tr>
<td>- Select GRC technology solution(s)</td>
</tr>
</tbody>
</table>

| **Optimize**          |
| - Begin GRC technology implementation |
| - Pilot key elements of the solution |
| - Automate control execution and monitoring |
| - Deploy continuous monitoring |

| **Enhance and sustain** |
| - Continue GRC technology implementation |
| - Integrate with other functions and organizations |
| - Implement sustainability program |

**Value:**
- Resolution of immediate and long-term risk exposure
- Improved risk alignment and event response time
- Agile and scalable control environment
- Cost reduction in internal and external risk activities, including monitoring and remediation
- Reduction in disruption to the business
- Improved business performance and innovation via value-based risk management

 Enabled by GRC technology

 Enabled by change and benefits management

Who we are

- John McLain
  Principal, Government and Public Sector
  Cell: +1 410 300 2748
  Off: +1 703 747 1198
  john.mclain@ey.com

- Joe Quinn
  Senior Manager
  Cell: +1 202 257 5518
  Off: +1 703 747 0898
  joseph.quinn@ey.com

- Zane Williams
  Senior Manager
  Cell: +1 914 439 6834
  Off: +1 212 773 8658
  zane.williams@ey.com

- Garo Nalabandian
  Senior Advisor
  Cell: +1 301 675 6049
  Off: +1 703 747 0616
  garo.nalabandian@ey.com

© 2015 Ernst & Young LLP. All Rights Reserved.
1505-1451817