A firm’s ability to weather storms depends on how seriously executives take risk management when the sun is shining and no clouds are on the horizon.

<table>
<thead>
<tr>
<th>Discussion Items</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Lifecycle Overview – What's the purpose?</td>
<td>15</td>
</tr>
<tr>
<td>IT Risk Assessment Process – 5 Steps</td>
<td>30</td>
</tr>
<tr>
<td>Next Steps - Education</td>
<td>5</td>
</tr>
</tbody>
</table>

**Risk assessment**

Broadly speaking, a risk assessment is the combined effort of 1. identifying and analyzing potential events that may negatively impact individuals, assets, and/or the environment; and 2. making judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors. [Wikipedia](https://en.wikipedia.org/wiki/Risk_assessment)
Risk Assessment Lifecycle

- **Board of Directors**
  - Responsible for accepting risks

**Performance and Risk Reporting**

- **Risk Assessment**
  - (Objective Planning)

- **Risk Framework**
  - (Policies & Controls)

- **Project Plan**
  - (Strategy = Time + $)
IT Risk Assessment Process

**Risk Framework**
- Compile a list of applications, vendors and data.

**Discovery**
- Work with business and IT resources to collect relevant information based on the scope of the risk assessment.

**Risk Identification**
- Develop an understanding of the business operating model, document management’s concerns and to ensure the risk assessment results reflect leadership’s concerns and vision.

**Inherent Risk Calculation**
- Evaluate risks and threats without considering management’s controls.

**Alignment & Reporting**
- Develop reports for the Board of Directors, senior leadership, internal audit and management.
Step 1: Identify / Develop a “Risk Framework”

1. Determine who is going to perform IT risk assessment.
   - In-house: Leverage a compliance team
   - Hybrid: Leverage an outside provider for the framework, execution or reporting and supplement effort with internal resources
   - Outsource: Identify an outside provider to perform the IT risk assessment

2. Consider an Industry Framework - IIA, COSO, NIST, COBIT, ISO

3. Develop an objective approach and risk scoring method

4. Keep it simple

The enterprise security risk assessment system must always be simple enough to use, without the need for any security knowledge or IT expertise. This will allow management to take ownership of security for the organization’s systems, applications and data.”

– ISACA - Performing a Security Risk Assessment, 2010, V.1
Step 2: Discovery

Collect Information: Work with business and IT resources to collect the following information:

**Enterprise Risk Assessment:**
- List of Departments / Functions
- List of Product and Services

**IT Risk Assessment:**
- IT Risk Domains *Leverage policies*
- Assets: List of Applications, Vendors and Physical Sites
Step 3: Interviews & Risk Identification

Develop an understanding of the business operating model, document management’s concerns and to ensure the risk assessment results reflect leadership’s concerns and vision.

Consider interviewing the following:

- Department / Business Leaders
- C-Level Officers
- Head of IT / CISO
- Product Owners
- Vendor Relationship Owners

TIP: Consider using surveys depending on the scope and maturity of the risk assessment. IT risk assessments may cover 100’s of assets, in which case survey's may be more effective.
Step 4: Inherent Risk Calculation

Inherent Risk: Evaluate risks and threats without considering management’s controls.

- Risk Framework: Leverage a risk framework to specific to your industry or regulatory requirements
- Objective Scoring: Apply rankings to department functions, products/services and IT assets
- Risk Factors: Financial, Reputational, Operational, Strategic and Regulatory
- Define Impact of Risk (Likelihood & Severity)
Risk Calculation – Illustrative Example

We performed an asset inventory risk assessment based on three risk categories to help management identify and prioritize higher-risk assets:

- Sensitive: Unauthorized disclosure of this data could seriously damage the company, its business partners, employees or customers.
- Internal: Unauthorized disclosure of this data would cause isolated damage to the company, its business partners, employees or customers.
- Public: This data is considered declassified or public information that can be freely disseminated without harm

Below are the risk calculation tables for inherent and composite risk:

### DATA INHERENT RISK RATING GRID

<table>
<thead>
<tr>
<th>Volume</th>
<th>Data Type</th>
<th>Sensitive</th>
<th>Internal</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical (500+)</td>
<td>High (3)</td>
<td>Medium (2)</td>
<td>Low (1)</td>
<td></td>
</tr>
<tr>
<td>Significant (101-500)</td>
<td>Medium (2)</td>
<td>Low (1)</td>
<td>Low (1)</td>
<td></td>
</tr>
<tr>
<td>Minor (0-100)</td>
<td>Low (1)</td>
<td>Low (1)</td>
<td>Low (1)</td>
<td></td>
</tr>
</tbody>
</table>

### COMPOSITE INHERENT RISK RATING GRID

<table>
<thead>
<tr>
<th>Operational Risk</th>
<th>Inherent Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical / High (MC/H)</td>
<td>9</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>18</td>
</tr>
<tr>
<td>Low (L)</td>
<td>9</td>
</tr>
</tbody>
</table>
Step 5: Reporting & Alignment

Board of Directors:

- Risk Assessment Summary – develop a 10-15 page summary of results for senior leadership and BOD
- Project Planning – develop management action plans that include expected cost, resource commitments and measures of success.

Internal Audit:

- Audit Reporting – Align internal audit and compliance plans based on the nature of risks scores

Management:

- Risk Assessment Details – provide detailed results of the risk assessment to ensure management accepts the results
- Maintenance – Ensure policies, procedures and internal controls align with the risk assessment and reflect risk mitigation efforts
Leveraging business operational risk and information security risk, we categorized control gaps into three categories to help management identify and prioritize higher risk control gaps.

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Count</th>
<th>Complete</th>
<th>Gap</th>
<th>Accept Risk</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>38</td>
<td>14</td>
<td>24</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Moderate</td>
<td>64</td>
<td>31</td>
<td>31</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>13</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Count</td>
<td>115</td>
<td>49</td>
<td>57</td>
<td>2</td>
<td>7</td>
</tr>
</tbody>
</table>

Note – ‘N/A’ indicated a control was not required based on the Company’s status as a private company.
## Project Plan

<table>
<thead>
<tr>
<th>Function</th>
<th>Operating and Management Approach</th>
<th>IT FTE Support</th>
<th>Approx. Cost</th>
<th>Risk Rating</th>
</tr>
</thead>
</table>
| IT Management & Governance            | • Lack of ownership at GO Group level  
• IT priorities not aligned with business  
• IT not engaged with leadership  
• Project management and execution issues | 4 IT Managers  | $1.2M        | Red         |
| End-User Computing                    | • Globally managed end-user products  
• Implementing VDI  
• Insufficient application training for users | 4 System Admin  | $1.5M        | Yellow      |
| Voice/Data Networking                 | • Global Lync system  
• Redundancy oversight | 2 System Admin  | $1.2M        | Yellow      |
| Application Development and Support   | • Mostly 3rd party applications & support  
• Separately managed  
• Deployment challenges | 4 BIM          | $1.2M        | Yellow      |
| Security, Controls & Monitoring       | • No information security program  
• Lack of system monitoring | 1 Security Admin  | $530k        | Red         |
| IT Help Desk                          | • Ticketing system (Vendor) for tracking  
• Lack of users adhering to ticketing process | 3 Helpdesk Admins  | TBD          | Yellow      |

**Risk rating:**
- **Red**: Critical issues causing significant risk
- **Yellow**: Issues to resolve: inefficient methods & tools need refinement
- **Green**: No significant issues
- **Gray**: Incomplete information or not applicable

*Note: Ratings are based on a point-in-time snapshot of when the assessment is performed.*
## Audit Planning – Illustrative Example

<table>
<thead>
<tr>
<th>Internal Audit Unit</th>
<th>Inherent Risk</th>
<th>Maturity Level</th>
<th>Owner</th>
<th>Actual</th>
<th>Planned Scoping</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Risk and Governance (GLBA)</td>
<td>Moderate</td>
<td>3: Defined</td>
<td>3rd Party</td>
<td>•</td>
<td>• • • •</td>
</tr>
<tr>
<td>Asset Management</td>
<td>High</td>
<td>2: Repeatable</td>
<td>3rd Party</td>
<td>•</td>
<td>• • •</td>
</tr>
<tr>
<td>IT Demand, Portfolio and Project Management</td>
<td>Moderate</td>
<td>2: Repeatable</td>
<td>IA</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Technology Service Provider Management</td>
<td>Moderate</td>
<td>2: Repeatable</td>
<td>3rd Party</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Operational Security</td>
<td>Moderate</td>
<td>2: Repeatable</td>
<td>IA</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Vulnerability Program Management</td>
<td>High</td>
<td>1: Initial</td>
<td>3rd Party</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>High</td>
<td>2: Repeatable</td>
<td>IA</td>
<td>•</td>
<td>• • •</td>
</tr>
<tr>
<td>Virtualization Security</td>
<td>Moderate</td>
<td>2: Repeatable</td>
<td>3rd Party</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>High</td>
<td>2: Repeatable</td>
<td>3rd Party</td>
<td>•</td>
<td>• • •</td>
</tr>
<tr>
<td>Development, Acquisition and Change Management</td>
<td>Low</td>
<td>4: Managed</td>
<td>IA</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Data Management</td>
<td>High</td>
<td>1: Initial</td>
<td>3rd Party</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery Planning</td>
<td>Moderate</td>
<td>3: Defined</td>
<td>IA</td>
<td>•</td>
<td>• •</td>
</tr>
<tr>
<td>IT General Controls (FDICIA)</td>
<td>High</td>
<td>2: Repeatable</td>
<td>IA</td>
<td>•</td>
<td>• • •</td>
</tr>
</tbody>
</table>
Risk Assessment Lifecycle

Board of Directors
- Responsible for accepting risks

Performance and Risk Reporting

Risk Assessment
(Objective Planning)

Risk Framework
(Policies & Controls)

Project Plan
(Strategy = Time + $)
Next Steps - Education

To consider for your risk assessment:

- **Format** – small is good, use K.I.S.S approach.
- **Distribution** – who has copies and where are they kept?
- **Maintenance** – who is responsible for upkeep of the assessment – IT, audit, management?
- **Residual Risk** – determine the potential impact to IT operations based on existing controls and processes.
Thank you

John MacDonald
RSM
Risk Advisory Services Manager
John.MacDonald@rsmus.com
816-289-1826
Rex Johnson
Director - Security & Privacy Service

RSM US LLP
4801 Main St., Ste. #400, Kansas City, MO 64112
D: (816) 303-7797
M: (913) 579-6716
E: rex.johnson@rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.