Enterprise Risk Management and Emerging Risks
Melissa Musser, CPA, CITP, CISA

**Director, Risk Advisory – Aronson LLC**

Director at Aronson with 15 years of professional experience. Melissa delivers a comprehensive best-in-class risk based audit approach to respond to financial, compliance, operational & IT risks for small nonprofits to large global SEC organizations. Areas of focus include but not limited to:

- Establishing, maintaining and optimizing internal controls and/or Sarbanes Oxley 404 compliance programs.
- Planning, supervising and executing audits to ensure compliance with policies and regulations and to monitor achievement of corporate objectives.
- Developing and supporting Enterprise Risk Management and Internal Audit programs

Prior to joining Aronson, Melissa spent eight years in public accounting as well as five years as a manager of corporate and IT internal audit and risk management for large global SEC organizations. Melissa has sat on numerous nonprofit boards throughout her career and actively volunteers within her community. She enjoys regularly sharing her knowledge with audiences as well having published whitepapers on internal controls.

She has a Bachelor of Science Degree in Accounting with majors in both Professional Accounting and Accounting Information Systems from the University of Akron. She received a (PMBOK) Project Management Body of Knowledge Certificate while there and also holds CPA, CITP and CISA (Certified Information System Auditor) certifications.
Donna McPartland

**Privacy, Cybersecurity & Data Protection Counsel - Arent Fox LLP**

Donna is Counsel in Arent Fox’s Privacy, Cybersecurity & Data Protection practice group. Formerly Chief Privacy Official at the Graduate Management Admission Council. At the core of Donna’s practice, she draws from nearly 20 years of experience in the testing, higher education, and nonprofit industries. Donna works with a variety of clients on their global data privacy and information security issues, developing privacy programs, advising on cross border data transfers, developing privacy policies, privacy impact assessments, data governance programs, navigating information security standards, and addressing issues in advanced technologies, including biometrics. Donna also advises nonprofits on their general counsel and transactional matters. Donna has significant in-house experience that clients can rely on to help them with their privacy and security matters. Experience includes:

- Global Privacy Program Development and Management (115 countries)
- Cross Border Data Transfer Requirements
- Direct Interaction with EU and other international data protection authorities (DPAs)
- Privacy Impact Assessments (PIAs)
- Information Security including NIST, ISO, and SOC standards
- Cloud Computing, social media and new technologies
- Biometrics
- Research and Marketing

+202.350.3765 (Work)
donna.mcpartland@arentfox.com
Derek Symer

**Principal, Senior Vice President, AHT Insurance**

Derek Symer, is an experienced Property & Liability Insurance Broker based in AHT's DC Metro office. Derek focuses in the Nonprofit & Education sectors including Associations, Think Tanks, NGOs and Educational Institutions including private colleges and independent schools. In his work, Derek helps his clients analyze their risk exposures and devise targeted risk transfer and mitigation strategies to improve their total cost of risk. Within this work, Derek has particular expertise in Directors & Officers Liability, Cyber Liability, Employment Practices Liability, Media & Publishers Liability, Event Cancellation, and International coverage.

In 2005, Derek co-founded the Business Managers Roundtable, a networking and educational forum for business officers of private & independent schools. Derek and AHT are members of the National Business Officers Association (NBOA), American Society of Association Executives (ASAE), and Greater Washington Society of Certified Public Accountants (GWSCPA).

AHT has been recognized by Business Insurance as a Best Place to Work in Insurance.
Highlights & Objectives

• **Understand** the importance of a Enterprise Risk Management

• **Identify Risks** to your mission / objectives / strategic plan

• **Evaluate** the likelihood and impact of risks

• **Learn** about emerging risks and best practices in mitigation

• **Assess** the overall risk & develop a practical response
Purpose

To provide a **summary of potential events** that may affect your organization and manage risks to **provide reasonable assurance** regarding the achievement of your mission and objectives.

E nterprise

R isk

M anagement
Why is ERM on the Rise?

• Regulator demands
• Unanticipated risk events affecting the organization
• Emerging best practice expectations
• Emerging corporate governance requirements
• Board of Director requests

Why is this Important?

It is a proven methodology to capture your risks and visually rank them so your organization can make informed decision on how to spend your budget dollars.

Priorities
Work Smarter – Not Harder
Balance

Don’t let the loudest person in the room get all the attention
Approach

Build your ERM Framework

Identify Strategic Objectives

Identify Risks

Analyze Quantify & Prioritize Risk

Determine Risk Mitigation
Build your ERM Framework
Building a Framework

Things to consider when building your framework

– Framework – ISO vr COSO

– Where to Start – Full rollout? Phased approach?

– What Model to implement - Risk factor vrs objectives based?

– ERM Organizational position - CRO, CAE, Risk Manager, Risk Committee?
Identify Objectives

*Tie into strategy and mission*
Example Risks to Objective Categories

- Collaboration Risk
- Management & Operational Risk
- Financial Risk
- External & Reputation Risk
- Personnel & Volunteers Risk
- Grant Risk
Brainstorm Risks Events
Risk Event Identification Techniques

May include a combination of different types of techniques combined with supporting tools:

– Event Inventories
– Internal Analysis & Surveys
– Process Flow Analysis
– Current Events
– Facilitated Workshops and Interviews
Analyze, Quantify & Prioritize Risk
Methods to Rank Risk

Qualitative
A qualitative analysis would use a scale of "Low, Medium, High" to indicate the likelihood of a risk event occurring.

Quantitative
A quantitative analysis will determine the probability of each risk event occurring. For example, Risk #1 has an 80% chance of occurring, Risk #2 has a 27% chance of occurring, and so on.

Our discussion will focus on qualitative analysis
Determine Likelihood

Determine the likelihood of the specific risk materializing. For example:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Guidance</th>
</tr>
</thead>
</table>
| Certain    | - History of regular occurrence  
- The event will occur (recur)  
- No special skills or determination required: information asset easily available |
| Likely     | - The event will occur (recur) in most circumstances |
| Possible   | - Has occurred in the past  
- The event may occur (recur) at some time  
- No special skills or determination required except for time and determination |
| Unlikely   | - The event could occur (recur) at some time |
| Rare       | - No history of occurrence.  
- The event may only happen in exceptional circumstances  
- High level of technical or social engineering skill and determination required |
Types of Risk Impact

In order to align discussions around why risk are significant and what should be done about them, you should consider dividing your analysis into types of impact:

- **Strategic**
  Causes a strategic objective to fail

- **Financial**
  Incurs unanticipated costs or reduces revenues

- **Operational**
  Affects the quality or efficiency of how work gets done

- **Reputation**
  Creates negative media attention

- **Environmental, Health and Safety**
  Jeopardizes staff, volunteers or others’ well-being

- **Legal**
  Triggers arbitration or litigation against your organization

- **Technology**
  Exposes application, data, operating systems, network or infrastructure to inappropriate access/change
Determine Impact

Consider the impact should the threat materialize. For example:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>For example: Catastrophic data loss or corruption, catastrophic effect on annual budget, complete loss of primary service greater than 1 week, direct financial loss 50%, Reputation impact - legal action / extensive media attention, brand damage</td>
</tr>
<tr>
<td>Major</td>
<td>For example: Significant data loss or corruption, significant effect on the annual budget, Service disruption 1 to 5 days; direct financial loss 25%, Reputation impact - legal action / national media attention, loss of good will</td>
</tr>
<tr>
<td>Moderate</td>
<td>For example: Moderate data disclosure or corruption, service disruption 1 day; direct financial loss 10%, Reputation impact - legal action / local media, loss of good will</td>
</tr>
<tr>
<td>Minor</td>
<td>For example: Minimal data disclosure or corruption, Service disruption none/minor; direct financial loss negligible, Reputation impact - complain or legal action / minimal reputation damage</td>
</tr>
<tr>
<td>Insignificant</td>
<td>For example: minor data loss or corruption, service disruption none/minor; direct financial loss negligible, Reputation impact - none</td>
</tr>
</tbody>
</table>
Develop Risk Analysis Matrix

Develop a **risk mapping for impact and likelihood** to help determine which risks need risk response. For example:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>moderate</td>
<td>moderate</td>
<td>high</td>
<td>critical</td>
<td>critical</td>
</tr>
<tr>
<td>Major</td>
<td>low</td>
<td>moderate</td>
<td>moderate</td>
<td>high</td>
<td>critical</td>
</tr>
<tr>
<td>Moderate</td>
<td>low</td>
<td>moderate</td>
<td>moderate</td>
<td>moderate</td>
<td>high</td>
</tr>
<tr>
<td>Minor</td>
<td>very low</td>
<td>low</td>
<td>moderate</td>
<td>moderate</td>
<td>moderate</td>
</tr>
<tr>
<td>Insignificant</td>
<td>very low</td>
<td>very low</td>
<td>low</td>
<td>low</td>
<td>moderate</td>
</tr>
</tbody>
</table>
## Example of a Risk Rating

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk</th>
<th>Risk Impact</th>
<th>Probability</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel/Volunteers Risk</td>
<td>Harm reputation of your organization</td>
<td>Reputation</td>
<td>Possible</td>
<td>Catastrophic</td>
<td>High</td>
</tr>
<tr>
<td>Grant Risk</td>
<td>Delays in disbursement</td>
<td>Financial</td>
<td>Possible</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Personnel/Volunteers Risk</td>
<td>stolen credentials leads to cyber incident</td>
<td>Technology</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
</tr>
<tr>
<td>Collaboration Risk</td>
<td>Loss of identity</td>
<td>Strategic</td>
<td>Rare</td>
<td>Major</td>
<td>Low</td>
</tr>
</tbody>
</table>
Determine Risk Mitigation
## Determine Risk Mitigation

<table>
<thead>
<tr>
<th>Reduce / Mitigate risk</th>
<th>Eliminate / Avoid risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activities with a high likelihood of occurring, but impact is low.</td>
<td>Activities with a high likelihood of loss and high impact.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Share / Transfer risk</th>
<th>Accept risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activities with low likelihood of occurring, but with a high impact.</td>
<td>If cost-benefit analysis determines the cost to mitigate risk is higher than cost to bear the risk.</td>
</tr>
</tbody>
</table>
Risk mitigation - Insurance

• Risk transfer involves moving risk to 3rd party via contractual arrangement

• Insurance is most common Risk Transfer mechanism

• Outsourcing: risk transfer financial offset – pre incident assessment planning. loss control property/cyber penetration testing.
Risk Examples
Example Category - Personnel/Volunteers Risk

- Injury at work
- Cause your organizations client injury
- Harm reputation of your organization
- High turnover
- Triggers a cyber security incident
Example Category - Financial Risk

- Inaccurate and/or insufficient financial information
- No financial planning (budgeting)
- Lack of financial liquidity
- Poor pricing policy (e.g., overpriced activities in grant applications)
- Excessive indebtedness
- FX losses
- Financial fraud
- High transactional costs
- Inadequate maintenance of long-term sources of funding
- Inadequate reserves and cash flow
- Dependence on a low number of revenue sources
- Inadequate investment policy
- Inadequate insurance coverage
- Funds used against the intent of donor/grantor
Example Category - Operational Risk

- Not enough beneficiaries
- Not enough well-trained Personnel
- Uncertainty about security of assets
- Competition from other organizations
- Dependence on suppliers (their strong bargaining power)
- Ineffective fundraising system
- Lack of formalized procedures
- Inefficient and ineffective IT system
- Implementing activities in a dangerous environment
- Natural disaster, fire, flood, theft
- Deviation from core mission “in search of” funding sources
Example Category - Management

- Inadequate organization structure
- Management lacks adequate experience or not well organized
- Management dominated by individual leaders
- Resignation of key personnel
- Conflict of interest
- Ineffective communication System
- No direction, strategy, and plans
Example Category - Grant Risk

- Delays in disbursement
- Lack of knowledge and skills to utilize the awarded grant
- Changes in environment preventing utilization of the awarded grant
- Undervalued contract
Emerging Risks: Privacy / GDPR

Are you ready for the General Data Protection Regulation (GDPR)? GDPR is the most important change in privacy in 20 years taking effect May 25, 2018.

In the future, aspects of the European GDPR are likely to find their way into other regulation as well, organizations should start to prepare their policies and procedures for this.
GDPR - Overview

Introduction

GDPR Requirements

Penalties

How it may impact companies

What companies can do to comply
What is the GDPR?

European Union’s new framework for data protection law replaces the 1995 Directive

One Stop Shop – EU “main establishment” of controller works with Lead Supervisory Authority

Application to Companies Worldwide - Simply offering products to and/or collecting data about persons in the EU is enough for the law to apply- Applies to Data Controllers and Data Processors

Effective Date – May 25, 2018
What is the GDPR? (cont’d)

<table>
<thead>
<tr>
<th>Principle Based – Purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful Basis Required for Processing Personal Information</td>
</tr>
<tr>
<td>Greater Protections and Rights to Individuals in the EU</td>
</tr>
<tr>
<td>Privacy Information must be clearly communicated</td>
</tr>
<tr>
<td>Data Protection Officers (regular and systematic monitoring on a large scale, or sensitive data, or public body); Associations representing categories of controllers MAY designate a DPO for their Controllers</td>
</tr>
<tr>
<td>Appropriate security of Personal Data</td>
</tr>
</tbody>
</table>
GDPR: Penalties, Complaints, Reputation

Penalties

- 20 million euro or up to 4% of total worldwide annual turnover, whichever is higher
- Member States can impose additional fines not covered by Art. 83

Complaints/Investigations

Reputational Consequences
GDPR applies......

When a company processes an EU data subject’s information if the processing is related to:

• offering or providing goods or services - even if no payment is required
• monitoring individuals in person or online
GDPR does not apply...

If the data does NOT relate to an identified or identifiable natural person or if the data is rendered anonymous in such a way that the data subject is no longer identifiable. (e.g. fully anonymized data – no identifiers; research report that only includes statistical information with no identifiers)

What about pseudonymous data?
• Pseudonymization is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. GDPR promotes the use of this.
GDPR: Controllers and Processors

**Controller:** company that alone or jointly with others determines the purposes and means of processing of personal data

**Joint Controller:** When two or more controllers determine the purposes and means of processing

**Processor:** processes data on behalf of the controller
GDPR: Processing

Any operation which is performed on personal data such as collection, storage, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction.

Examples: processing hotel room or conference registrations Selling books or online courses
"Personal data" is any information which relates to a living individual who can be identified:
• From that information
• From that information combined with other information held or likely to come into the possession of the company

**Examples**
- Name
- Postal or work or email address
- Phone number
- ID numbers (e.g. passport, license)
- Location data (usually from devices)
- Bank account details
- Expressions of opinion
- Photographs, sound recordings, film
- IP addresses
- Information stored in cookies or similar technologies
- Training records
GDPR: What is Sensitive Data?

“Sensitive data requires special handling, higher protections

Not specifically defined under the GDPR so Member States can regulate further

GDPR prohibits their processing unless exemptions are in place: explicit consent, employment obligations, etc.

Examples

✓ Biometric data
✓ Health and genetic data (allergies)
✓ Employment data
✓ Criminal convictions
✓ Racial or ethnic data
✓ Political opinions
✓ Religious or philosophical
✓ Trade-union membership
✓ Sex life or sexual orientation
**GDPR: Key Changes**

<table>
<thead>
<tr>
<th></th>
<th>Data Subject Rights</th>
<th>Increased transparency and creating new rights. Right to Access, Right to be Forgotten, Data Portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Consent</td>
<td>Consent for processing must be freely given, specific, informed and unambiguous. Strict Requirements – see Art. 29 WP Guidance</td>
</tr>
<tr>
<td>3</td>
<td>Data Processors and controllers</td>
<td>More contract requirements to be flowed by controllers to processors (data processing agreements)</td>
</tr>
<tr>
<td>4</td>
<td>Data Protection by Design (DPbD)</td>
<td>DPbD is about ensuring that privacy is embedded throughout the organization and being able to demonstrate compliance to regulators</td>
</tr>
<tr>
<td>5</td>
<td>Cross-Border Transfers</td>
<td>This privacy-compliant cross-border data transfer strategy must have “adequate protections”</td>
</tr>
<tr>
<td>6</td>
<td>Data Breach Notifications</td>
<td>Controllers required to notify competent supervisory authority and, in certain cases, also to affected data subjects. Generally within 72 hours.</td>
</tr>
</tbody>
</table>
GDPR: Security Requirements

Flexible requirement that takes into account several factors: (1) state of the art; (2) implementation costs; (3) nature, scope, context and purposes of processing; (4) risk of varying likelihood and severity for the rights and freedoms of natural persons

Breach notification requirement: 72 hours or without undue delay

Specific callouts for: encryption, pseudonymization, backups, procedures for regularly testing/assessing/evaluating effectiveness of security measures
GDPR: What Companies Can Do To Comply?

**Organization:**
- Assemble Your Team
- Roles & Responsibilities
- Know your data
- Security Obligations

**Monitor & Enforce:**
- Encourage Communication
- Make Good Conduct Visible
- Manage Employee Error

**Processes:**
- Determine Systems tied to Data
- Employee Outreach
- Collaboration
- Training

**Document:**
- Privacy Policy
- Security Policies
- Breach Response Plan
- Document Retention Plan
GDPR: Data Governance

Data Governance

- **Policies** – data governance policy with data classification scheme
- **Processes** – roadmaps for determining governance steps
- **Data Mapping and Inventory** – required to document all data processing activities in lieu or notifications/approvals to DPAs
- **Vendor Management** – who has data, where is it, and how managed
**GDPR: Contracts for Using Processors**

- Processor must provide contractual guarantees that they use data security technology and methods that meet GDPR.

- Gap analysis and legal review of contracts and determine if amendments need to be made to meet GDPR requirements.

- Make amendments in order to continue using Processor in compliance with new requirements.
GDPR: Data Transfers

Only one part of GDPR compliance – still many other compliance requirements

Options – need to have “adequate data privacy protections”

• Standard Contractual Clauses
• Privacy Shield - Not for Trade Associations, Other nonprofits, No Banks (must have FTC jurisdiction)
• Binding Corporate Rules (GDPR gold standard, but complex)
• Country deemed by EU as having “adequate protections” (Argentina, Canada, Israel, New Zealand, Switzerland, Uruguay - NOT US)
GDPR: Standard Contractual Clauses

What are Standard Contractual Clauses?

- Pre-approved contractual language to be incorporated into agreements, unchanged.

Two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU/EEA and one set for the transfer from controllers to processors established outside the EU/EEA.
GDPR: Data Transfer Exceptions

- Consent – must be informed, explicit, more complex under GDPR
- Contract – must be necessary for performance or conclusion of a contract or implementation of pre-contractual measures taken at the data subject's request
- Public interest
- Legal claims - necessary for the establishment, exercise, or defense of legal claims
- Vital interests – necessary to protect the vital interests of data subject or of other persons (if data subject is physically or legally incapable of giving consent)
Emerging Risks: Culture and Conduct

“It takes 20 years to build a reputation, and five minutes to ruin it. If you think about that, you’ll do things differently.”

-Warren Buffett
## Culture and Conduct Risk: Recent Examples

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For-Profit World</strong></td>
<td>Wells Fargo – Banking Scandal</td>
</tr>
<tr>
<td></td>
<td>Volkswagen – Emissions Scandal</td>
</tr>
<tr>
<td><strong>Individuals</strong></td>
<td>Harvey Weinstein</td>
</tr>
<tr>
<td></td>
<td>Matt Lauer</td>
</tr>
<tr>
<td></td>
<td>Others</td>
</tr>
<tr>
<td><strong>Non-Profit World</strong></td>
<td>Hotchkiss – Tick-Bite = $41 million</td>
</tr>
<tr>
<td></td>
<td>NRA</td>
</tr>
<tr>
<td></td>
<td>OXFAM</td>
</tr>
</tbody>
</table>
Culture & Conduct Risk: Tone from the Top

Ensure cultural values are reflected in the organization’s:

- Strategy
- Risk appetite
- Compliance frameworks
- ACTIONS
Culture & Conduct Risk: Independent Assurance

Organizations should demonstrate due diligence by conducting independent risk reviews / health checks over the following areas:

- Strategy
- Policies & practices
- Training
- Investigation procedures
- Review of KPIs
Emerging Risks: Third-Party

Fees and fines related to third-party risk may be significant, the long-term brand and financial impact of reputation loss can be much worse. A third party engagement can be ended, reputation loses are often far more severe than any fine.
### Why Manage and Assess Third-Party Risks?

<table>
<thead>
<tr>
<th>Third-Party Risk Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security</td>
</tr>
<tr>
<td>Intellectual Property Theft</td>
</tr>
<tr>
<td>Manufacturing Quality Control</td>
</tr>
<tr>
<td>Data Protection</td>
</tr>
<tr>
<td>Safety / Occupational Hazard</td>
</tr>
<tr>
<td>Money Laundering</td>
</tr>
<tr>
<td>Bribery and Corruption</td>
</tr>
<tr>
<td>Political Exposure</td>
</tr>
<tr>
<td>Social Responsibility</td>
</tr>
<tr>
<td>Fraud</td>
</tr>
<tr>
<td>Wage and Hour Violations</td>
</tr>
<tr>
<td>Conflict Minerals</td>
</tr>
</tbody>
</table>
TPRM – Third Party Risk Management

TPRM is the process of analyzing and mitigating risks to your company by parties OTHER than your own company.

• TPRM can reduce likelihood of:
  ✓ data breach costs
  ✓ operational failures
  ✓ vendor bankruptcy
  ✓ reputation damage
TPRM Third-Party Stratification Example

Tier 1
- Critical vendors (10%) – PII + critical systems

Tier 2
- Major vendors (40%) – PII OR critical systems

Tier 3
- Vendors (50%) – commodities/low risk purchases
TPRM Third Party Due Diligence Example

Due Diligence is the process by which the vendor is reviewed to determine its suitability for a given task.

- Risk Assessment (Documentation, Categories of Risk,)
- Financial projections & review
- Insurance Review
- Background check
- Legal Review
- Vendor Audits and/or SOC reports
ERM - Critical Success Factors

- Obtain senior management approval and involvement
- Designate committees or individuals to champion
- Develop Procedures
- Involve business and technical experts
- Formalize reporting to leadership
Develop ERM Procedures

- Who is responsible for initiating and conducting risk assessments
- Who will participate
- What steps will be followed
- How disagreements will be handled and resolved
- What approvals will be needed
- How assessments will be documented
- How documentation will be maintained
Formalize Risk Reporting

1. Updated Risk Universe
   - Enterprise Universe
   - Survey Results

2. Risk assessment criteria
   Use risk assessment criteria to prioritize risks – identify the most significant risks to the organization

3. Prioritized risk heat map

4. Mitigation Plans
   Identify risk mitigation plans for top 10 most significant risks
Any Questions?

Derek Symer, AHT
703.669.1121
DSymer@ahtins.com

Melissa Musser, Aronson
240.364.2598
mmusser@aronsonllc.com

Donna McPartland, Arent Fox
202.350.3765
donna.mcpartland@arentfox.com