Thank you to our sponsors!

Please make sure your Zoom name reflects your registration name so we can match for CPE purposes
Harold Silverman is the Managing Director of Professional Practices at the Institute of Internal Auditors. He serves as the liaison to the International Internal Audit Standards Board, oversees the development and maintenance of all aspects of the International Professional Practices Framework. He also leads The IIA’s CAE Services offerings, including thought leadership on emerging trends and leading practices.

Silverman previously was VP of internal audit at The Wendy’s Company. Prior to Wendy’s, he was the VP of internal audit at Houghton Mifflin Harcourt Publishing Co. Harold has also held internal audit positions at Raytheon Co. and PwC, and he gained external audit experience at Arthur Andersen.
Origin

Strengths

Flaws

Review

2020 model

Future
The Three Lines of Defense, 1066 AD
1996

The Three Lines of Defense, c1996
EU Directive 2011

ECIIA/FERMA
The Three Lines of Defense

- Governing Body / Board / Audit Committee
- Senior Management
The Three Lines of Defense
The Three Lines of Defense

Senior Management

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

Governing Body / Board / Audit Committee
The Three Lines of Defense

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Governance Body / Board / Audit Committee

Senior Management
The Three Lines of Defense

1st Line of Defense:
- Management Controls
- Internal Control Measures

2nd Line of Defense:
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense:
- Internal Audit

Governance Body / Board / Audit Committee

Senior Management

External audit
The Three Lines of Defense 2013

Senior Management

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Governing Body / Board / Audit Committee

Regulator
External audit
Defend who against what?
3 LoDometer

Revise

Repair

Evolve

Refresh

Heretic

Don’t touch it

Purist

Destroy it

LoDometer®
The Three Lines of Defense
Successful?

- Useful for discussions
- Well-known
- Widely adopted
- Easy to explain
- Simple graphic
But…

- Why three?
- Why these?
- What about
  - “Blurring”?  
  - Public Sector?
  - Flexibility, scalability?
  - Unregulated industries?
  - “Independent risk management”?
• Appears/suggests:
  – Reactive, defensive
  – Structural
  – Prescriptive
  – Silos
  – Static
  – Sequential
  – Equal sizes
  – Internal audit “boxed in”
  – One way communication
  – Remote governing body and senior management
### Starting point

<table>
<thead>
<tr>
<th>Organizations</th>
<th>Risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Important</td>
<td>• Not just about stopping bad thing</td>
</tr>
<tr>
<td>• Varied</td>
<td>• Must be integrated and embedded</td>
</tr>
<tr>
<td>• Don’t exist to manage risk</td>
<td>• Part of management and governance</td>
</tr>
<tr>
<td>• Like organisms (not machines)</td>
<td></td>
</tr>
</tbody>
</table>
Governance – minimum requirements

- Governing body
- Actions
- Accountability
- Assurance and advice
- Management
- Internal audit
The Three Lines Model

- Illustrates a relationship between roles (not structural)
- There can be multiple points of interaction between the governing body and management if required:
  - CEO, CRO, etc.
Three Lines Model

GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership and transparency

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY:
↑ Accountability, reporting
↓ Delegation, direction, resources, oversight
↔ Alignment, communication coordination, collaboration
• Added context
• Principles-based, scalable, flexible
• Use of language
  – Not just defense
  – Roles not structures
  – Separating or blending roles
• Emphasize collaboration
• Distinctiveness of internal audit
<table>
<thead>
<tr>
<th>Principle</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance</td>
<td>Accountability + Actions + Assurance</td>
</tr>
<tr>
<td>2. Governing body roles</td>
<td>• Governance</td>
</tr>
<tr>
<td></td>
<td>• Alignment with stakeholders</td>
</tr>
<tr>
<td></td>
<td>• Delegating to and overseeing management</td>
</tr>
<tr>
<td></td>
<td>• Effective internal audit</td>
</tr>
<tr>
<td>3. Management roles</td>
<td>• First line roles</td>
</tr>
<tr>
<td></td>
<td>• Second line roles</td>
</tr>
<tr>
<td></td>
<td>{ Separated or blended</td>
</tr>
<tr>
<td>4. Third line roles</td>
<td>• Objective assurance and advice on everything</td>
</tr>
<tr>
<td>5. Third line independence</td>
<td>• Independent from management responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Accountable to governing body</td>
</tr>
<tr>
<td>6. Creating and protecting value</td>
<td>• Through collaboration and alignment among all roles</td>
</tr>
</tbody>
</table>
• Not about “blurring” or “crossing the line”
• About compatibility of roles:
  – Independent insight and advice are fully compatible with third line roles
  – Cannot be both responsible and independent (would require another party for assurance)
Reactions

• Mostly very positive
• Some pushback
  – Too radical
  – Not radical enough
  – What about compliance?
• Did not directly answer:
  – Is it okay for CAE to lead ERM?
Common questions

• What was the most important reason for the review?
• What do we hope the impact will be?
• Is there anything we would do differently?
What’s next?

The Three Lines and…

- ERM (COSO)
- Sustainability (WBCSD)
- Fraud (TI)
- Public Sector (INTOSAI)
- SMEs (IFAC)
Q&A

harold.silverman@theiia.org
Meet the Speakers

John Barnes
Partner, Controls Advisory
Grant Thornton
E John.Barnes@us.gt.com

John is a Partner in the Risk Advisory practice and leads our Risk Advisory Practice in the Great Lakes Region. He has more than 25 years of experience in internal audit, Sarbanes-Oxley, Specialty Attestation reports and accounting consulting services. John works with clients to deliver advisory services that identify and reduce risk to an organization. Prior to joining Grant Thornton, John held other management positions at national accounting and consulting firms. His prior experiences include providing external audits and internal controls consulting within the COSO framework and coordinating such work with all of the Big Four accounting firms.

John has managed complex multi-national engagements, including board reporting and executive communications. Prior internal audit experience includes providing risk advisory services to multinational manufacturing firms, technology companies, REITS, government contractors and retailers.

Katelyn Banaszak
Senior Manager, Controls Advisory
Grant Thornton
E Katelyn.Banaszak@us.gt.com

Katelyn is a Senior Manager in the Risk Advisory practice and has a blend of experience that enables her to work on internal audit and consulting as well as SOX engagements. She has also supported corporate restructuring projects, litigation and fraud, and process improvement engagements.

Katelyn has been working primarily with international companies since joining Grant Thornton. For example, she coordinated internal audits with Grant Thornton member firms at dozens of international locations for a $17 billion automotive supplier for several years. She is currently the lead Senior Manager on a 9,000-hour annual SOX and internal audit outsourcing engagement for a $3 billion public, international manufacturing client in Grant Thornton’s Midwest region. In this capacity, she is directly responsible for supervising and delivering all SOX and internal audit procedures at operating units all over the U.S., Europe, and Asia. This involves leading fieldwork teams both domestically and internationally, performing and managing the review process to completion, and managing all related communications with the client management and external auditors.
Agenda

- Introductions
- Leadership Traits
- Emotional Intelligence: Defining Characteristics
- Leadership Essentials
- Building Personal Leadership Traits
Executive Leadership Tools and Tactics

Introductions
Executive Leadership Tools and Tactics

Leadership Traits
Poll Question #1

Which of the following are traits traditionally associated with Leadership?

A) Passion  
B) Dedication  
C) Respect  
D) All of the Above
Traits Traditionally Associated with Leadership

- Collaboration
- Compassion
- Competitiveness
- Confidence
- Dedication
- Determination
- Fearlessness
- Focus
- Honesty
- Humility
- Intelligence
- Integrity
- Passion
- Respect
- Toughness
- Vision
Emotional Intelligence

• Dan Goleman has defined emotional intelligence to be “a group of five skills that enable the best leaders to maximize their own and their followers’ performances”.
• The five components of emotional intelligence are:
  1. Self-awareness
  2. Self-regulation
  3. Motivation
  4. Empathy
  5. Social Skills
Executive Leadership Tools and Tactics

Emotional Intelligence: Defining Characteristics
Emotional Intelligence: Self-awareness

- **Self-aware Leaders** are honest with themselves; they understand their own strengths and weaknesses professionally as well as their emotions, needs and drives and how they impact others.

- **Characteristics of Self-awareness:**
  - Speaking openly and honestly without being confessional
  - Self-confidence
  - Realistic self-assessment
  - Self-deprecating sense of humor
  - Comfort in discussing weaknesses in performance

- **Weakness of Self-awareness:** Goleman’s research identified that senior executives may mistake self-awareness for weakness or lack of ‘can-do’ attitude.
Emotional Intelligence: Self-regulation

• **Self-regulation** is how one controls their feelings, emotional impulses, and bad moods. This enables leaders to build an environment based on trust and fairness which boosts productivity in the group by creating a calm business environment.

• **Characteristics of Self-regulation:**
  • Cool, calm, and collected
  • Reflective and thoughtfulness
  • Trustworthiness
  • Integrity
  • Comfort with change

• **Weakness of Self-regulation:** Demonstration of emotional control could be mistaken for lack of passion.
Emotional Intelligence: Motivation

• Effective leaders are motivated to achieve, not motivated by something. They are passionate and optimistic, have a love of learning, take pride in accomplishments, and have creativity in solving problems.

• Characteristics of Motivation:
  • Passion for the work itself
  • Energy and enthusiasm for improvement
  • Optimism under stress

• Weakness of Motivation: Motivation may be misunderstood if the motivating factors for a potential leader are external in nature rather than internal.
Emotional Intelligence: Empathy

• Leaders with empathy have thoughtful consideration of employees’ feelings while making intelligent decisions. These leaders help to reduce tension among teammates, cultivate communication, and encourage collaboration.

• Characteristics of Empathy:
  • Ability to recruit talented employees
  • Emphasis on developing and mentoring others
  • Sensitivity to environmental differences
  • Leveraging knowledge of others into business improvements

• Weakness of Empathy: Business leaders may view empathy as a weakness.
Emotional Intelligence: Social Skills

- **Social skills** is the culmination of the other four components of emotional intelligence; using the skills to find common ground within a circle of people understanding that nothing can be accomplished in isolation.

- **Characteristics of Social Skills:**
  - Skillful at managing teams
  - Effective at persuasion
  - Enthusiastic and strong collaborators
  - Effective at managing relationships

- **Weakness of Social Skills:** Socially skilled leaders may appear to be wasting time at work building the relationships, but that is actually part of the work.
Poll Question #2

Which of the following are NOT one of the components of Emotional Intelligence?

A) Motivation  
B) Social Skills  
C) Diligence  
D) None of the Above
Executive Leadership Tools and Tactics

Leadership Essentials
Leadership Essentials

• Stephen Covey is the author of 7 Habits of Highly Effective People. He defines leadership as “communicating to people their worth and potential so clearly that they are inspired to see it in themselves”.
  • Communication
  • Learned and practiced aspects of leadership
• Three of the Four leadership essentials related to communication are:
  • Inspire trust
  • Clarify purpose
  • Align Systems
Leadership Essentials: Inspire Trust

- Leaders who **inspire trust**, build relationships with others, and encourage others to trust them. This is done through competence, not charisma or manipulation.
- Leaders **demonstrate trust** in others by allowing teammates to deliver on their promises and live up to their expectations.
- Micromanaging or second guessing are opposite traits of the **inspire trust** leadership.
Leadership Essentials: Clarify Purpose

- Effective leaders **clarify purpose** and create shared goals by communicating with team members.
- **Collaboration** in setting goals empowers the team to be more personally invested in achieving the goals.
- Collaborative goal setting **clarifies the goal** with every person, much more than simply explaining the goal does.
Leadership Essentials: Align Systems

• Dr. Covey describes “aligning systems” as removing conflict between what an organization says it values, and what it actually values or measures.
• Companies may practice the valuation of employees in the following ways:
  • Investing in education programs, training, or conferences
  • Promoting polies and procedures that support their people such as flexible scheduling or paid time off
  • Encouraging creating out of the box problem-solving in the workplace
• Strong leaders look for ways to align systems by addressing conflicts that arise between what is said, and what is practiced.
Poll Question #3
Which of the following is a component of Leadership that we’ve talked about so far today?

A) Manipulation
B) Inspire Trust
C) Micro-Manage
D) None of the Above
Leadership Essentials: Traits

- **Traditional Leaders**
  - Only one way of doing something
  - Concerned with being right
  - Follow the manual - maintain order
  - Avoid mistakes at all costs
  - Concerned with Reliability
  - Always right
  - Accept limited, constructive feedback

- **Creative Leaders**
  - Believe in interactive way of doing things
  - Concerned with being real
  - Improvise tasks and take risks
  - Welcome to feedback as learning opportunities
  - Concerned with Validity
  - Seek conversation
Building Personal Leadership Traits
Opportunities to Lead

• **At Work**
  - Organizational Committees at Work: Day of service or other program
  - Education: Coordinate a committee to create/teach a half day seminar
  - Social Outings: Join committee to organize social outings or events

• **Outside of Work**
  - Non-Profit Board Service
  - Non-Profit Committees
  - Existing Involvements
Opportunities to Lead

• **Outside of Work (cont.)**
  • **Non-profit Board Service**: Volunteers who provide strategic and financial oversight to the organization
    • Use of professional skills to enhance the organization’s mission
    • Create networks and contacts, learn to master working with dynamic groups, and enhance communication skills
  • **Non-profit Committees**: Joining a committee of volunteers to plan small events
    • Find an organization with a mission that you support
    • Research organization foundation and events
    • Understand the time commitment and expectations
Opportunities to Lead

• Outside of Work (cont.)
  • Existing Involvements: Volunteer opportunities with established organizations such as:
    • IIA
    • AICPA
    • Alumni organizations
    • Religious organizations
Poll Question #4
Which of the following are ways to find opportunities to lead and practice your leadership skills?

A) Non-Profit Board
B) At Work
C) Professional Organizations
D) All of the Above
Opportunities to Lead: Application

• Make the Organization Better
  • **Understand the Organization**: Get to know the actual organization, board members, staff and leaders. Discuss your role with the organization to determine where you can best benefit them.
  • **Be willing to lead**: Assume leadership and responsibility for a project by following through on commitments.
  • Recruit and develop other volunteers
  • Be generous with your time, expertise and possibly your finances
Leading Principles

• The following are steps to take to excel as a leader and embody the traits of an exceptional leader:

  • **Maintain and Improve Leadership Traits:** Stay current on regulatory changes and industry trends, be conscious of current events at your company and industry and expand your network beyond your current industry.

  • **Practice Self-awareness and Social Skills:** Evaluate your strengths and weaknesses on a regular basis and make an effort to share your self-awareness skills to your colleagues. Encourage open, honest and fair communication in an open environment.

  • **Set an Example:** Tone at the top is critical for success and as a leader, ensure that you hold yourself to the highest standard.

  • **Make sure each task is understood, supervised, and accomplished:** Choosing the right person, and effectively communicating expectations for success.
Leading Principles

• **Confirm the task is complete:** Reviewing the assignment parameters, soliciting feedback and asking questions.

• **Perform thorough and timely decisions:** Make executive decisions without waiting for consensus using a decision-making framework. Solicit input as time allows.

• **Empower teammates:** Offer opportunities frequently to allow for growth and constructive feedback throughout the process. Assign tasks in broad strokes rather than specific steps to allow judgment.

• **Define your vision:** Create a clear measurable and specific idea of where you want to progress professionally. Communicate this with those around you and practice the skills to help you succeed (public speaking, writing practice).

• **Build and grow your network:** Every encounter is a chance to meet someone interesting and an opportunity to broaden your knowledge base. Cultivate connections with periodic personal outreach.
Poll Question #5
How will you (or have you) practice your leadership skills going forward in your career?

A) Non-Profit Board
B) At Work
C) Professional Organizations
D) All of the Above
Appendix
## Firm Overview

Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd. (GTIL), one of the leading global audit, tax and advisory organizations. Grant Thornton LLP has more than 8,700 professionals serving from 56 offices across the country.

<table>
<thead>
<tr>
<th></th>
<th>Grant Thornton member firms worldwide</th>
<th>U.S. member firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue (USD)</td>
<td>$5.72 billion</td>
<td>$1.95 billion</td>
</tr>
<tr>
<td>Personnel with Partners &amp; SSC*</td>
<td>56,028</td>
<td>8,730*</td>
</tr>
<tr>
<td>Partners</td>
<td>3,608</td>
<td>606</td>
</tr>
<tr>
<td>Offices</td>
<td>756</td>
<td>56</td>
</tr>
<tr>
<td>Statistics as of:</td>
<td>Sept. 30, 2019</td>
<td>Dec. 31, 2019</td>
</tr>
</tbody>
</table>

*Total personnel includes professionals in Grant Thornton’s India Service Center (ISCC and KCC) which is based out of Bangalore. SSC / KCC are joint ventures with the Grant Thornton U.S. member firm, therefore these professionals are included in U.S. employee data.

**Combined statistics of Grant Thornton International Ltd (GTIL) member firms. GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. Please see GT.com for further details.

*Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. Please see GT.com for further details.
## Grant Thornton’s Solutions

<table>
<thead>
<tr>
<th>Risk and Control</th>
<th>Financial Management</th>
<th>Business Operations</th>
<th>Tax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controls Advisory</strong></td>
<td><strong>Finance Transformation</strong></td>
<td><strong>Strategy and Transformation</strong></td>
<td><strong>Transaction Structuring</strong></td>
</tr>
<tr>
<td>Internal audit</td>
<td>Post merger integration</td>
<td>Business Transformation Strategy</td>
<td>Efficient acquisition and disposition structures</td>
</tr>
<tr>
<td>Enterprise risk management (ERM)</td>
<td>Core systems implementation</td>
<td>Modern Marketing</td>
<td>Legal entity planning and optimization</td>
</tr>
<tr>
<td>Data analytics</td>
<td>Material business change</td>
<td>Digital Sales and Tech Strategy</td>
<td>Transaction integration and disintegration</td>
</tr>
<tr>
<td>Sarbanes-Oxley (SOX) Compliance</td>
<td>Audit remediation</td>
<td>ERP selection and request for proposals</td>
<td>Financing issues</td>
</tr>
<tr>
<td>Compliance Risk</td>
<td>Pension/retire medical plan annual valuations</td>
<td>Implementation management</td>
<td>Recapitalizations</td>
</tr>
<tr>
<td>Compliance risk management systems</td>
<td>Appointed Actuary service</td>
<td>Data migration</td>
<td>Cross order transaction planning</td>
</tr>
<tr>
<td>Ethics programs</td>
<td>Insurance reserve valuation, process and control</td>
<td>eGRC</td>
<td></td>
</tr>
<tr>
<td>Regulatory compliance programs</td>
<td>Long Duration Guidance &amp; Implementation (LDTI)</td>
<td>Risk sensing</td>
<td></td>
</tr>
<tr>
<td><strong>Compliance Risk</strong></td>
<td><strong>DAC &amp; reserve accounting updates</strong></td>
<td>Risk analytics</td>
<td>Risk &amp; Regulatory Technology</td>
</tr>
<tr>
<td>eGRC</td>
<td><strong>Information Technology</strong></td>
<td><strong>Performance Improvement</strong></td>
<td><strong>Financial/Business</strong></td>
</tr>
<tr>
<td>Risk sens</td>
<td>Reporting</td>
<td>Revenue and margin management</td>
<td>Tax accounting methods</td>
</tr>
<tr>
<td>Risk analytics</td>
<td>Data analysis &amp; reconciliation</td>
<td>Direct costs and supply chain</td>
<td>State and local tax incentives</td>
</tr>
<tr>
<td><strong>Risk &amp; Regulatory Technology</strong></td>
<td>Policies &amp; procedures</td>
<td>Overhead efficiency</td>
<td>Federal tax incentives</td>
</tr>
<tr>
<td>Strategic Risk</td>
<td>Managed services &amp; specialty accounting</td>
<td>Working Capital optimization</td>
<td></td>
</tr>
<tr>
<td>Strategic risk</td>
<td><strong>Financial Operations</strong></td>
<td><strong>Human Capital</strong></td>
<td>Human Capital</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Reporting</td>
<td>Cultural diligence and integration</td>
<td>Employee benefit matters</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Data analysis &amp; reconciliation</td>
<td>Compensation and benefits</td>
<td>Change in control tax planning</td>
</tr>
<tr>
<td>Risk culture</td>
<td>Policies &amp; procedures</td>
<td>Moral &amp; motivation</td>
<td>Employment tax planning</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>Managed services &amp; specialty accounting</td>
<td><strong>Integration &amp; Separations</strong></td>
<td></td>
</tr>
<tr>
<td>Crisis planning and response</td>
<td><strong>Cost &amp; Performance Management</strong></td>
<td><strong>Transaction integration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Risk</strong></td>
<td>Shared services feasibility</td>
<td>Diversitues</td>
<td></td>
</tr>
<tr>
<td>Strategy &amp; management</td>
<td>Shared services design &amp; implementation support</td>
<td>TSAs</td>
<td></td>
</tr>
<tr>
<td>Incident response</td>
<td>Shared services optimization</td>
<td>Integration Management Office (IMO)</td>
<td></td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>Cost &amp; profitability analysis</td>
<td><strong>Human Capital</strong></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Finance process optimization</td>
<td><strong>Employee benefit matters</strong></td>
<td></td>
</tr>
<tr>
<td>Access management</td>
<td>Integrated planning process</td>
<td>Change in control tax planning</td>
<td></td>
</tr>
<tr>
<td>Application security</td>
<td>Business intelligence</td>
<td><strong>Employment tax planning</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Operations Risk</strong></td>
<td><strong>Actuarial Services</strong></td>
<td><strong>Integration &amp; Separations</strong></td>
<td><strong>Human Capital</strong></td>
</tr>
<tr>
<td>Operational risk management</td>
<td><strong>Finance Transformation</strong></td>
<td><strong>Transaction integration</strong></td>
<td></td>
</tr>
<tr>
<td>Third party risk management</td>
<td><strong>Cost &amp; Performance Management</strong></td>
<td>Diversitues</td>
<td></td>
</tr>
<tr>
<td>Model risk management</td>
<td><strong>Human Capital</strong></td>
<td>TSAs</td>
<td></td>
</tr>
<tr>
<td>Market and liquidity risk</td>
<td><strong>Strategic Risk &amp; Regulatory Technology</strong></td>
<td>Integration Management Office (IMO)</td>
<td></td>
</tr>
<tr>
<td>Contract compliance</td>
<td><strong>Cost &amp; Performance Management</strong></td>
<td><strong>Human Capital</strong></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd
SOC services

SOC 1
These attestation reports are specifically intended to meet the needs of entities that use service organizations (user entities) as their financial statement auditors (user auditors) use these reports to help evaluate the effect of the controls at the service organization on the user entities’ financial statements.

SOC 2
These attestation reports are intended to meet the needs of a broad range of users that need assurance about a service organization’s controls as they relate to the security, availability, and processing integrity of the systems the service organization uses to process its users’ data and the confidentiality and privacy of the information processed by those systems.

SOC 2+ ADDITIONAL SUBJECT MATTER
This type of report is issued when an organization requests that the service auditor’s report address other criteria in addition to the applicable trust services criteria or additional subject matter, such as HITRUST or NIST, related to the service organization’s services using additional suitable criteria related to that subject matter, or both.

SOC 3
SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, and/or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2® Report. Since they are general use reports, SOC 3® reports can be freely distributed.

SOC for Supply Chain
SOC for Supply Chain report offers manufacturers, producers and suppliers the opportunity to demonstrate the resiliency of their supply chain to customers. It is a report over a system that produces or manufacturers goods relevant to security, processing integrity and availability of the system, as well as confidentiality and privacy of data used by the system.
Grant Thornton’s Thought Leadership

**Data Analytics**
- A new book from the Internal Audit Foundation and Grant Thornton LLP, explores how Internal Audit can harness the power of data analytics to address enterprise risks and controls.
- Discusses significant elements of a data analytics effort, a framework for digital transformation and how to identify the highest-value priorities.

**Internal Controls**
- A Guidance on Monitoring Internal Control Systems The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initially selected Grant Thornton to be the project leader and main contributor to the guidance on effectively monitoring the quality of internal control systems.

**Third Party Risk Management**
- Run annual TPRM conferences for IA and business
- TPRM webinars & industry roundtables
- IA Whitepapers
For additional information on today's presentation please contact:

Natalie Galbato
Grant Thornton
D +1 513 345 4585
M +1 513 417 3253
GT.COM
Questions?
Introduction to Cloud Security Auditing
Presenting

Sean A. Thomas, CISA, CISSP, CISM
Manager – IT Risk Advisory Services

Sean is a manager in the Risk Advisory Services team at Schneider Downs. He has experience with information security governance, IT risk management, and contingency planning including business continuity and disaster recovery.

Sean began his career as an application developer and has implemented application security practices for enterprise software development. Prior to his tenure at Schneider Downs, he spent nearly a decade in various IT-related roles at a public pension fund with over $14 billion in assets, most recently serving as Information Security and Privacy Officer. In this role, he developed internal controls to satisfy NIST, HIPAA, CIS Critical Security Controls, and PCI DSS. Sean also developed internal practices for third-party risk management.

Sean received an MBA in Strategy and Leadership and B.S. in Computer and Information Science from The Ohio State University. He is a member of Information Systems Audit and Control Association (ISACA) and the International Information System Security Certification Consortium (ISC²).
Schneider Downs Firm Profile

- Fourth-largest accounting firm in Western Pennsylvania and ranked in the top 60 accounting firms in the U.S.
- Headquartered in Pittsburgh, PA with offices in Columbus, OH, and Washington, DC
- Approximately 500 employees, including 50 shareholders and partners
- Serving clients both nationally and internationally
- Organizing member of PrimeGlobal, an international accounting association
- Access to subject-matter expertise to provide diverse and deep thought leadership when needed
- Significant experience in the public utility industry
Schneider Downs Advisory Services

BUSINESS ADVISORY
- Fraud Investigation
- Valuation
- Due Diligence
- Transaction Advisory

RISK ADVISORY
- Internal Audit Sourcing
- IT Audit
- Risk Management & Compliance Services
- Business Process Optimization

TAX ADVISORY
- Domestic Income Tax
- State and Local Tax
- International Tax
- Transaction Advisory
- Credits and Incentives
- Methods and Elections
- Not-for-Profit

ACCOUNTING ADVISORY
- Major Accounting Standard Adoption
- Technical Accounting Assistance
- Outsourced Accounting Services

CYBERSECURITY
- Penetration Testing
- Compliance Based Assessments
- Cybersecurity Maturity Assessments
- Digital Forensics and Incident Response

TECHNOLOGY ADVISORY
- Robotic Process Automation (RPA)
- Data Analytics
- Corporate Performance Management
- Software Selection and Project Management

RETIREMENT SOLUTIONS
- Retirement Plan
- Regulatory Consulting
- Retirement Plan Design
- Fiduciary Consulting

CORPORATE FINANCE
- Mergers and Acquisitions
- Buy Side
- Sell Side
- Corporate Finance
Risk Advisory Practice Profile

• Certified professionals bring significant experience in co-sourcing internal audit with global, public companies and working effectively with external auditors

• Ability to consistently staff all engagements with the largest team of internal audit and consulting specialists in the region with approximately 60 dedicated risk advisory, IT, and information security specialists

• Proven effective use of data analytics, robotic process automation (RPA) and other technologies to gain efficiencies and provide broader risk coverage

• Significant public utility experience to assist with execution of NiSource’s internal audit plan

• Diverse experience, with 76% of professionals having industry experience outside of public accounting

• Our IT audit team has a deep knowledge of SAP, Oracle, and a multitude of other ERP systems

• Strategically developed, professional learning and training curriculum administered through a learning management system
Global Risk Advisory Capabilities

Internal Audit Strategy/Governance
- IA Strategic Assessment and Planning (Strategy, Structure, People, Process, Technology)
- Internal Audit Benchmarking and Metrics
- Robotic Process Automation (RPA) for Internal Audit
- Internal Audit Quality Assurance Reviews (QARS)
- Quality Assurance and Improvement Plan (QAIP)

Risk Management Services
- Integrated/coordinated compliance and assurance with other lines of defense
- Enterprise Risk Management (ERM) Program Assessment
- Third Party Risk Management Program Assessment
- SOX Compliance Program Assessment
- Merger/acquisition integration and due diligence
- SOC1/2 Assessments

Information Technology Auditing
- Cybersecurity Services
- Compliance (i.e. GDPR, HIPAA, PCI, NIST, ISO, etc.)
- Disaster Recovery/ Business Continuity
- Pre/post system implementations reviews
- IT General Controls

Process and Compliance Auditing
- Operational Audits
- Audits of Compliance (i.e. export compliance, corporate policy compliance, FCPA compliance, federal awards compliance, etc.)
- SOX Compliance Testing
- Data Analytics
What is the ‘cloud’?
Poll #1

How technical are you?
• Very
• Somewhat
• Not at all
## Shared Responsibility Model

<table>
<thead>
<tr>
<th>CUSTOMER DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLATFORM, APPLICATIONS, IDENTITY &amp; ACCESS MANAGEMENT</td>
</tr>
<tr>
<td>OPERATING SYSTEM, NETWORK &amp; FIREWALL CONFIGURATION</td>
</tr>
<tr>
<td>CLIENT-SIDE DATA ENCRYPTION &amp; DATA INTEGRITY AUTHENTICATION</td>
</tr>
</tbody>
</table>

### SOFTWARE

- COMPUTE
- STORAGE
- DATABASE
- NETWORKING

### HARDWARE/AWS GLOBAL INFRASTRUCTURE

- REGIONS
- AVAILABILITY ZONES
- EDGE LOCATIONS
## Shared Responsibility Model

<table>
<thead>
<tr>
<th>Responsibility per cloud service model</th>
<th>IaaS (Infrastructure as a Service)</th>
<th>PaaS (Platform as a Service)</th>
<th>SaaS (Software as a Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC (Security Governance, Risk &amp; Compliance)</td>
<td>Green</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Data Security</td>
<td>Green</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Application Security</td>
<td>Green</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Platform Security</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>

Customer Responsibility

Shared Responsibility

Provider Responsibility
Shared Responsibility Model
Planning a Cloud Security Audit

1. Inventory Providers
2. Assess Risk
3. Determine Scope
Inventory Providers

Who is using the service?

What business functions are supported?

What types of data does the service store and/or process?

Was the service procured through an approved process?
Poll #2

How confident are you in the completeness of your organization’s cloud provider inventory?

• Very

• Somewhat

• Not at all
Assess Risk

**Availability**
- What happens if the service goes down?
- What service level agreements (SLAs) are in place?

**Integrity**
- How is data processing validated?
- What is the impact of incorrect data?

**Confidentiality**
- What data types are processed or stored by the service?
- Where is the datacenter?
- What are the data breach notification requirements?
Determine Scope

When possible, extend existing control frameworks to cloud environments.

The Cloud Security Alliance provides a free mapping of common frameworks to a cloud environment in its Cloud Controls Matrix (CCM).
Poll #3

Which of the following does your organization currently adhere to, if any? (Select all that apply)

- COBIT
- NIST
- CIS Controls
- HIPAA
- ISO
- HITRUST
- Other
## Determine Scope

### Documenting the Control Environment

1. Start from selected framework
2. Filter controls by Delivery Model
3. For Service Provider controls, map available sources of assurance (i.e., SOC reports, ISO certification, etc.)
4. Identify any Service Provider controls that require additional assurance
5. For Tenant/Consumer controls, map internal ownership and control activity

<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM V3.0 Control ID</th>
<th>Updated Control Specification</th>
<th>Architectural Relevance</th>
<th>Corp Gov Relevance</th>
<th>Cloud Service Delivery Model Applicability</th>
<th>Supplier Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-01</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.</td>
<td>X X X X X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Assurance or Consulting?

Less mature control environments may benefit from a consulting engagement focused on bringing internal activities in line with a standard framework.
## Determine Scope

### Using ISACA’s Standard Audit Programs
ISACA publishes standard audit programs for popular cloud platforms free to ISACA members.

<table>
<thead>
<tr>
<th>Process Sub-area</th>
<th>Ref. Risk</th>
<th>Control Objectives</th>
<th>Controls</th>
<th>Control Type</th>
<th>Control Classification</th>
<th>Control Frequency</th>
<th>Testing Steps</th>
<th>Ref. Framework/Standards</th>
<th>Ref. Workpaper</th>
<th>Fail/Pass</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Auditing</td>
<td></td>
<td>Network security architecture is baselined and supports the enterprise’s security requirements.</td>
<td>AWS network security architecture is routinely reviewed and compared against enterprise-defined security requirements. Periodic reports are produced and sent to appropriate personnel for review. Any deficiencies are addressed in a timely manner.</td>
<td>Interview responsible and/or accountable personnel to determine whether a security network architecture standard exists and has been formally documented and applied to the environment.</td>
<td>1. 1. Interview responsible and/or accountable personnel to determine whether a security network architecture standard exists and has been formally documented and applied to the environment. 2. Determine the frequency of reviews that assess compliance of the network security architecture with the documented standard. 3. Determine how compliance of the network security architecture with the documented standard is assessed (e.g., python scripts run Center for Internet Security® (CIS) AWS security benchmarks daily and produce reports to security, etc.).</td>
<td>3. 3. Obtain and inspect completed compliance reviews and confirm that any instances of noncompliance are remediated in a timely manner.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The enterprise can identify and take timely action against inappropriate network traffic.</td>
<td>The enterprise has deployed a security information and event management (SIEM) capability to define normal traffic patterns and report suspicious events to personnel in a timely manner. SIEM configuration and event logs are routinely assessed by the enterprise to ensure the tool functions as intended.</td>
<td>Interview responsible and/or accountable individuals (security, networking, etc.) to determine if network baselines have been established to facilitate an understanding of standard versus abnormal network behavior. Baselines may include indicators such as volume input/output, top resources or AWS applications that generate traffic on a daily basis, etc. Confirm the following:</td>
<td>1. Interview responsible and/or accountable individuals (security, networking, etc.) to determine if network baselines have been established to facilitate an understanding of standard versus abnormal network behavior. Baselines may include indicators such as volume input/output, top resources or AWS applications that generate traffic on a daily basis, etc. Confirm the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommended uses for these programs:**
- Template to document the control environment
- Recommended steps for auditing a given control
- Guidance on control design

---

**Amazon Web Services® (AWS®) Audit Program**

**Network Configuration and Management**
Determine Scope

Considerations When Seeking Additional Assurance

**Cloud Provider Controls**
SOC Reports (Type 2)
- Qualified, Adverse, or Disclaimer Opinion
- Test Results (Section 4)

ISO 27001 Certification
- Control Exclusions

**Third-Party Assessments**
- Cost of outsourcing vendor assurance to an experienced third-party assessor

**First-Party Assessments**
- Staff skillsets
- One-sided vendor relationships (i.e., Microsoft, Amazon, Google vs. you)

**Tenant/Consumer Controls**
SOC Reports
- Complementary User Entity Controls

**Built-In Audit Tools**
- Azure Secure Score, etc.
Wrap-Up

Keys to a Successful Cloud Security Audit

1. Understand Your Environment
   • Look for “shadow” cloud instances
   • Be clear on what data types each provider handles and what business functions they support

2. Follow an Industry-Standard Controls Framework
   • Make sure controls are documented and align with a framework appropriate to your organization
   • When possible, design cloud controls to align with those that employees are already accustomed to working with

3. Leverage Existing Assurance
   • Reduce the scope of the audit by leveraging existing work performed as part of a SOC report, ISO certification, etc.
   • Note gaps in controls or testing that must be addressed by the tenant or customer
Poll #4

Do you feel more prepared to perform a cloud security audit?

• Much More Prepared

• Somewhat More Prepared

• Not More Prepared
RAISING THE BAR WHILE LOWERING RISK
INTERNAL AUDIT – MANAGING RISK IN SYSTEMS IMPLEMENTATION

IIA – Columbus Chapter Presentation
October 21, 2020
Your Speakers

Joe Corro
Director
ERP Implementation Risk
Joe.Corro@rsmus.com

Kari Sklenka-Gordon
Principal
ERP Implementation Risk Practice Leader
Kari.Sklenka-Gordon@rsmus.com

Petre Ghitescu
Director
ERP Implementation Risk
Petre.Ghitescu@rsmus.com
Agenda

- Opening remarks and introductions
- Current trends and market analysis
- What are the big “risk rocks”?
- Managing risk
- Lessons learned
CURRENT TRENDS & MARKET ANALYSIS

Systems Implementations
How big is the pie?

- Global software market is expected to hit $41B by 2020 and $49 billion by 2023 (marketwatch.com) (alliedmarketresearch.com)
- Mid-size business adoption of new ERP software will grow at a rate of 7.9% (alliedmarketresearch.com)
- ERP and CRM software types make-up 53% of the new installations (2018 ComputerWeekly/TechTarget IT Priorities Survey)
- Cloud based ERP’s are gaining market share at a rate of 4.9% annually, but on-premise still accounts for 57% in 2020 (Allied Market Research)
What about the ERP slice?

- Technology enablement and competitive advantage;
  - Leverage new technologies including mobile apps to improve operational business performance and customer experience
  - AI data-driven decision making; centralization of data
- Reduce labor costs with more automation
- Reduce maintenance expenses and shift infrastructure support to the cloud maintained by others
- Systematic improvements to meet security and compliance regulations
- Replacement of outdated, or end-of-life, unstable technology
## Most Common ERP Implementation Trends in 2020

<table>
<thead>
<tr>
<th>Trend</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile Implementation Methodology/Approach</td>
<td>More rapid deployment; less formality of business requirement and system design documentation</td>
</tr>
<tr>
<td>Out-of-the-box software functionality</td>
<td>Business process transformation likely required</td>
</tr>
<tr>
<td>Cloud-centric platforms</td>
<td>Less support on company, but business continuity plan needs reviewed and revised; usually results in a lack of performance testing</td>
</tr>
</tbody>
</table>
Polling Question

Are you implementing or upgrading a new ERP in the next 18 months?

A) Yes
B) No
THE BIG “RISK ROCKS”

Systems Implementations
Questions you should ask

Have you re-assessed your infrastructure and the ripple effect of introducing a major IT platform to your business ecosystem?

Can your organization withstand and recover from a disaster or temporary loss of system availability?

Has your organization assessed the degree and velocity of change?

Do you have a clearly defined and commonly understood decision-making framework?

Is “risk management” part of your implementation team’s DNA?

Can you trace the decomposition of all macro & micro processes down to detailed requirements?

Will your documentation withstand an audit?

Are both the implementation team and business stakeholders aligned on how much data cleansing is ‘good enough’ vs. ‘not enough’?

Are controls and security seen as a separate or silo’d functions in the Design and/or Test phases?
Foresight vs. hindsight

**Proactive Indicators**
- New software product
- Business transformations
- New executive team
- Strategic business initiatives
- Sourcing strategy changes
- Facilities/capital program
- Merger and acquisition integration
- Regulatory compliance requirements
- Any of these factors noted above with an agile implementation methodology

**Reactive Indicators**
- Project reschedules and overruns
- Project performance issues
- Timeline issues
- Budget overruns
- Quality issues at any phase including significant testing failures during UAT testing
- Scope reduction
- Regulatory issues
- Suspected client and supplier agency issues
- Stakeholder frustrations
- Steering and project team discord
- Missed commitments
How will project distress manifest itself?

- Per Gartner, 55%-75% of ERP implementations fail
- Causes:
  - Insufficient schedule and resource planning
  - Lack of technology adoption with employees and/or for customers
  - Project teams and/or stakeholders not aligned with methodology
  - Data inaccuracies; loss of data
  - Fraud
  - Exposure to new cyber security vulnerabilities
  - Insufficient control consideration
  - Expected automation improvements don’t work
  - New technology enables existing processes rather than transforming them
  - Inability to operationalize and maintain the system due to system complexities and not having the right resources to support the new software
Polling Question

Of those of you who are implementing a new ERP, which implementation methodology approach are you planning to use?

A) Waterfall
B) Agile
C) Hybrid
D) N/A
<table>
<thead>
<tr>
<th>Client</th>
<th>Problem overview</th>
<th>3\textsuperscript{rd} Line of Defense Involvement</th>
</tr>
</thead>
</table>
| Client A | In process of implementing SAP S4/HANA coupled with major process transformation.  
Growing project team discord due to re-work, missed deadlines, and pressure to re-cover.  
Project schedule that failed to clearly identify critical path and method for allocating (and balancing) limited resources on most important activities.  
Mounting concern and inability to prove all requirements have been captured and built. | Project governance assessment to scrutinize project’s decision-making and escalation processes.  
Schedule diagnostics to assess structural viability of the project schedule.  
Requirements traceability testing to confirm and validate the many-to-one and one-to-many relationships between numerous design, build, and testing documents. |
| Client B | Oracle Cloud implementation with multiple, localized releases due to utility customer segmentation.  
Complex multi-layered, multi-release schedule that does not always align with over-arching strategies  
Fear that future state system will be operational but not compliance-worthy or audit ready. | Detailed assessment of project strategies for each of the implementation’s major domains - including design, testing, data migration, organizational change management, etc.  
Re-design approach to synergize controls design with process design. |
| Client C | Implementing Ceridian Dayforce to replace and transform its HCM, recruiting, time & expense, benefits and compensation processes.  
Growing leadership concerns that test phase might not accurately validate future state processes. | Re-performance to validate a sample of test scenarios to ensure both test steps and conclusions reached are appropriate. |
The value Internal Audit can bring to an implementation

- Increased confidence in the integrity of the business requirements (you are getting what you paid for)
- Improved visibility and transparency of program risks and performance
- Increased likelihood of technology enablement of automation
- Independent professional advice for solutions
- Secure environment
When is the optimal time to perform an implementation risk assessment?

At any point during, or even after the implementation

General ERP implementation phases

Planning/ Project Prep  Design/ Blueprint  Build/ Configure  System Freeze/ Cutover  Go-live/ Hyper-care

Agile methodology combines these phases
Trends from external auditors

- External auditors are focused at a minimum on the following areas:
  - SDLC General Controls (system changes)
  - Data Migration
  - IT General Controls
  - Segregation of Duties
LESSONS LEARNED
Systems Implementations
# Top Ten Lessons Learned

<table>
<thead>
<tr>
<th>Install the right leadership and form the right team with continuity</th>
<th>Assign experienced leadership and establish a team that covers the requirements with balance and cohesion for the program lifecycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design the proper governance and decision making</td>
<td>Design and execute a governance framework that is commensurate to the complexity of the program with clearly delineated roles and responsibilities</td>
</tr>
<tr>
<td>Use the right methodology and program processes</td>
<td>Employ a proven implementation method appropriate to the design objectives of the program, adapting the program approach accordingly</td>
</tr>
<tr>
<td>Develop requirements, understand uncertainty and acceptance criteria</td>
<td>Determine requirements, understand uncertainty by requirement, priority drivers, talent matched, estimated and then tenaciously manage scope</td>
</tr>
<tr>
<td>Take the time to properly plan</td>
<td>Develop schedules that contain the proper degree of rigor, are logically correct with clear understanding of the critical path of activities</td>
</tr>
<tr>
<td>Define budgets according to the context</td>
<td>Develop budgets that factor in team capability, environment, quality and size and then implement appropriate cost management practices</td>
</tr>
<tr>
<td>Establish effective stage-gate criteria and governance</td>
<td>Direct, design and implement a quality management plan and stage gate assurance process. Know when to terminate programs. Earlier is better.</td>
</tr>
<tr>
<td>Design and execute to a fully developed risk management plan</td>
<td>Establish start-up and forward looking view on risks, determine risk response actions, map risks to the schedule, show impacts and monitor</td>
</tr>
<tr>
<td>Know where you are and develop a basis for level of confidence</td>
<td>Design and execute to a performance management plan that provides program situational awareness and transparency to all governance levels</td>
</tr>
<tr>
<td>Get an independent expert opinion</td>
<td>Conduct objective, fact-based reviews at key points in the program</td>
</tr>
</tbody>
</table>
Q&A / OPEN FORUM
THANKS FOR ATTENDING!
LOOK FOR THE SURVEY AND CPE EMAILS SOON

Thank you to our sponsors!