3 Unified Lines of Defense: Getting Risk, Compliance, and Audit to Talk to Each Other

Bruce McCuaig
SAP
Agenda

1. Three Lines of Defense
2. Challenges and Opportunities
3. SAP Solutions for GRC
4. Additional Benefits
5. Wrap-Up and Conclusions
Agenda

1. Three Lines of Defense
2. Challenges and Opportunities
3. SAP Solutions for GRC
4. Additional Benefits
5. Wrap-Up and Conclusions
The origins of three lines of defense

All Directives must be implemented via national regulation in member states

Scope: Focus on making audit committees key players in corporate governance in EU member states

Target audience: Audit committees

Requirements and principles: Creation of terms of reference for audit committees to:

Monitor the financial reporting process

Monitor the effectiveness of
• Internal control,
• Internal audit, and, where applicable,
• Risk management

Note that the phrase “three lines of defense” does not appear in this directive
Growing demand for three lines of defense guidance
Not just a European framework anymore …
What IS the three lines of defense framework?

An optional framework involving:

• Establishing clear responsibilities, accountability, and oversight for managing risks, compliance, and controls across the enterprise

• Appropriately monitoring risk, control, and compliance functions with coordination to minimize gaps and eliminate unnecessary duplication of activities

• Board oversight and direction of three separate groups responsible for managing risks and controls. That is, those who:
  1. Own and manage risks and controls on a day-to-day basis (operating management)
  2. Monitor risk, compliance, and controls to support management
  3. Provide independent assurance about the status and effectiveness of risk and control management to the Board (internal audit)
Sound business and risk strategies come first
Three lines of defense is just one piece of the puzzle
Three lines of defense must align with the business
Successful business performance should be defended

Business Drivers
- Board and Executive Management
- Business Strategy and Objectives
- Risk Appetite

Risks
- Operational
- Financial
- Environmental
- Human Capital
- Reputation
- Technology
- Compliance
- Strategic

Organizing the Three Lines of Defense

Key questions to ask:
- Are the lines of defense focused proportionately on our key strategies and objectives?
- Do we have a shared understanding of key activities and processes that must be managed to succeed?
- Are we consciously considering whether to accept, mitigate, avoid, or transfer risks?

Set objectives, monitor results and performance, and allocate resources.
### Three lines of defense

#### Key responsibilities and activities

<table>
<thead>
<tr>
<th>1</th>
<th>First line of defense: Operational management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control business operations and own or manage risks and controls in day-to-day business activities</td>
<td></td>
</tr>
<tr>
<td>• Identifies, owns, manages, and mitigates risks</td>
<td></td>
</tr>
<tr>
<td>• Maintains effective internal controls</td>
<td></td>
</tr>
<tr>
<td>• Implements and complies with internal policies and procedures</td>
<td></td>
</tr>
<tr>
<td>• Assesses risks and controls, applying corrective actions as needed</td>
<td></td>
</tr>
<tr>
<td>• Implements recommendations by internal audit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Second line of defense: Risk and compliance management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversee, assess, and manage risk and compliance activities across the enterprise</td>
<td></td>
</tr>
<tr>
<td>• Management of the frameworks for risk, control, and compliance</td>
<td></td>
</tr>
<tr>
<td>• Monitoring risk management practices and activities</td>
<td></td>
</tr>
<tr>
<td>• Continuous monitoring of risk, control, and compliance requirements</td>
<td></td>
</tr>
<tr>
<td>• Verifying that first line of defense is operating as designed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Third line of defense: Independent assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide comprehensive and independent assurance (usually by internal audit)</td>
<td></td>
</tr>
<tr>
<td>• Automation and continuous risk-based auditing for assurance and insight</td>
<td></td>
</tr>
<tr>
<td>• Assurance regarding all elements of risk management and internal control framework</td>
<td></td>
</tr>
<tr>
<td>• Monitoring efficiency and effectiveness of operations, integrity of reporting processes, and compliance with laws, policies</td>
<td></td>
</tr>
</tbody>
</table>
Three lines of defense: A simple scenario

A manufacturing company maintains parts and raw materials inventories at each of its locations. Local warehouse managers are responsible for all aspects of inventory management and control.

**Line 1: IT Operations** is directly responsible for controls over physical security, data protection, access, cyber risk, etc.

**Line 2: CIO** provides standards and guidance based on ISO or other IT and Cyber Security frameworks or regulations.

**Line 3: Internal Audit** provides assurance that standards and procedures are followed, risks are managed, and compliance is achieved.

**Management and the board** receive reports on overall status of IT and cybersecurity, and makes necessary decisions and resource allocations.
Who uses the three lines of defense framework?

Based on an article that appeared in the Journal of Accountancy in July 2015, “Using three lines of defense to manage internal controls” by Ken Tysiac, a recent global survey of internal auditors found that:

- 56% of organizations use this model and consider internal audit to be the third line of defense.
- 20% of respondents, including 43% in South Asia, were not familiar with the three lines of defense model.
Agenda

1. Three Lines of Defense
2. Challenges and Opportunities
3. SAP Solutions for GRC
4. Additional Benefits
5. Wrap-Up and Conclusions
But is three lines of defense working?  
It is apparent that challenges remain for many

How would you rate your organization’s ability to identify, assess and manage both current and emerging risks? Please answer on a scale from Very effective to Very ineffective.

<table>
<thead>
<tr>
<th></th>
<th>Very effective</th>
<th>Somewhat effective</th>
<th>Slightly ineffective</th>
<th>Very ineffective/Not at all effective</th>
<th>Not applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>First line of defense:</td>
<td>22%</td>
<td>53%</td>
<td>20%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Managing risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second line of defense:</td>
<td>20%</td>
<td>53%</td>
<td>22%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Managing risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third line of defense:</td>
<td>20%</td>
<td>46%</td>
<td>21%</td>
<td>9%</td>
<td>4%</td>
</tr>
<tr>
<td>Managing risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

KPMG International  
Expectations of Risk Management Outpacing Capabilities – It’s Time for Action, May 2013
Challenges to implementing three lines of defense

Organization silos and different terminology across lines of defense limiting coordination

Lack of comprehensive, effective risk management practices throughout the organization

Fragmented systems without a single source of truth shared across the enterprise

Lack of agreed-upon roles and responsibilities leading to duplication of effort or gaps in risk coverage

Cumbersome, largely manual practices that make coordination difficult and time-consuming

Inadequate interaction and communication with senior management and the board
Our study:

• **1,010** independent interviews around the world with those responsible for GRC in organizations with a turnover of at least €500M across a range of sectors

• Interviews were conducted during May and June 2015

• The full report is available [here](#)
It’s time for a change

72% See value in integrating GRC programs with enterprise architecture initiative

75% Think that GRC practices are due for an overhaul in businesses generally

48% Of organizations have not reviewed their GRC processes/technologies in the last three years
Support company performance using sound strategies and effective controls

46% Of the GRC data that an organization theoretically has access to is being used in a strategic way

34% Find that current processes and systems place too great a focus on the past, rather than strategic planning for the future

41% Control failure is seen as the second biggest risk to organizations over the next two years, behind competitive forces
Combined assurance
Moving toward GRC convergence

64% of respondents say GRC convergence is a priority for their organization

Source: KPMG, *Businesses admit time has come for convergence of GRC activities*, February 2010
Integration vs. silos in GRC processes and activities

Do you share a common process and information environment for GRC activities?

Can you see and track performance across the enterprise?

Can you see and monitor all the risks across the enterprise?

Can you monitor compliance effectiveness at all levels of the organization?
Where GRC value is achieved through integration

1. Reduced gaps in risk and compliance processes / 71
2. Reduction in redundant or duplicative activities / 62
3. Greater ability to present information to board and senior management / 58
4. Greater ability to gather information quickly and efficiently / 57
5. Greater ability to repeat processes in a consistent manner / 48
6. Reduced impact on operations from siloed and uncoordinated risk assessments / 46
7. Reduced impact on operations from siloed training on compliance requirements / 32
8. Reduced costs of GRC processes / 32

DATA: 223 respondents who stated they have standardized to fully integrated GRC.
### Three lines of defense

**Key responsibilities and activities**

#### 1. First line of defense: Operational management

Control business operations and own or manage risks and controls in day-to-day business activities

- Identifies, owns, manages, and mitigates risks
- Maintains effective internal controls
- Implements and complies with internal policies and procedures
- Assesses risks and controls, applying corrective actions as needed
- Implements recommendations by internal audit

#### 2. Second line of defense: Risk and compliance management

Oversee, assess, and manage risk and compliance activities across the enterprise

- Management of the frameworks for risk, control, and compliance
- Monitoring risk management practices and activities
- Continuous monitoring of risk, control, and compliance requirements
- Verifying that first line of defense is operating as designed

#### 3. Third line of defense: Independent assurance

Provide comprehensive and independent assurance (usually by internal audit)

- Automation and continuous risk-based auditing for assurance and insight
- Assurance regarding all elements of risk management and internal control framework
- Monitoring efficiency and effectiveness of operations, integrity of reporting processes, and compliance with laws, policies

---

Board of directors, audit committee, and other executives
First line of defense
Operational management

Control business operations and own or manage risks and controls in day-to-day business activities

- Identifies, owns, manages, and mitigates risks
- Maintains effective internal controls
- Implements and complies with internal policies and procedures
- Assesses risks and controls, applying corrective actions as needed
- Implements recommendations by internal audit

Application of risk and control framework designed by the second line:

- Performance of controls
- Control self-assessment
- Risk assessment and response
- Policy acknowledgement and compliance
- Automation of risk and control monitoring activities
- Raising of issues encountered

SAP Process Control
Ensure effective controls and ongoing compliance

SAP Risk Management
Preserve and grow value
Second line of defense
Risk and compliance management

SAP Process Control
Ensure effective controls and ongoing compliance

SAP Risk Management
Preserve and grow value

SAP Regulation Management by Greenlight
Manage regulatory requirements and align with internal control activities

2

Second line of defense:
Risk and compliance management

Oversee, assess, and manage risk and compliance activities across the enterprise

• Management of the frameworks for risk, control, and compliance
• Monitoring risk management practices and activities
• Continuous monitoring of risk, control, and compliance requirements
• Verifying that first line of defense is operating as designed
• Monitoring adequacy and effectiveness of internal control

Continuous update of the risk and control framework; monitoring and reporting its status:

• **Control design** and review
• Review of **regulatory requirements**
• Publication of **governance policies**
• Review of **control documentation**
• Review of **internal control status** and effectiveness
• **Follow up** on issues raised
Provide comprehensive and independent assurance (usually by internal audit)

- Automation and continuous risk-based auditing for assurance and insight
- Assurance regarding all elements of risk management and internal control framework
- Monitoring efficiency and effectiveness of operations, integrity of reporting processes, and compliance with laws, policies

Critical review of the risk and control framework:

- **Audit** based on high-profile risks
- **Control test of effectiveness**
- **Review of policies** and related compliance
- **Issuing audit findings**, reports, and recommendations
- **Report to the board and audit committee**
GRC leaders manage and report on the three lines of defense framework

Communication, oversight, and coordination:

- Ensure three lines of defense are **sharing information** and supported by appropriate role definitions and policies
- Verify that activities are well-coordinated to avoid duplication of effort and to foster efficiency and effectiveness
- Report on performance
Why SAP solutions for Governance, Risk, and Compliance?
SAP GRC supports sharing and collaboration across all three lines of defense

1. First line of defense: Operational management
2. Second line of defense: Risk and compliance management
3. Third line of defense: Independent assurance

Shared regulatory frameworks

Shared risks

Shared controls and policies

Shared audit findings
SAP core solutions for three lines of defense

SAP Risk Management
Shared risk framework

SAP Process Control
Shared control and regulatory framework

SAP Audit Management
Shared audit framework
Monitor thresholds, effectiveness of risk responses, and corrective actions

Respond to risk after balancing costs and benefits

Plan risk management within the context of value to the organization

Identify risks, risk drivers, risk indicators, impacts, and responses

Analyze risk via scenarios, modeling, and other factors to understand exposure
SAP Process Control
Ensure effective controls and ongoing compliance

Support decisions and promote accountability with insightful analytics and sign-off

Document controls and policies centrally; map to key regulations and impacted organizations

Perform automated, exception-based monitoring of ERP systems

Perform periodic risk assessments to determine scope and test strategies

Evaluate control design and effectiveness; raise and remediate issues
SAP Audit Management
Transform audit to move beyond assurance

**Monitor**
Monitor the disposition of results reported to management

**Communicate**
Communicate the engagements objectives, scope, conclusions, findings, and recommendations

**Perform**
Identify, analyze, and document relevant information

**Plan**
Develop and document a plan for each engagement

**Manage**
Establish a risk-based plan, prioritize audit activities, and align with the needs of the enterprise
Introducing our demo flow
Cybersecurity in a three lines of defense world

1. Reviews risk analysis from CRO and proposes a new control
2. Creates control and triggers a self-assessment
3. Performs self-assessment and requests automation
4. Reviews self-assessment and creates KRI
5. Automates testing
6. Reviews overall control assessment report
7. Reviews risk and creates cybersecurity audit
8. Performs audit & issues findings
9. Reviews three lines of defense report
Three lines of defense offline demo
What does the three lines of defense framework look like in real life?

Link: http://demo.tdc.sap.com/SpeedDemo/aa7a60f30123953d
Putting it all together

Audit
(Auditors, fraud investigators)

Oversight
(Risk and control offices, quality, …)

Business
(Risk and control owners)
Agenda

1. Three Lines of Defense
2. Challenges and Opportunities
3. SAP Solutions for GRC
4. Additional Benefits
5. Wrap-Up and Conclusions
Beyond three lines of defense …

While not strictly suggested by the three lines of defense framework, there are many benefits to be enjoyed by going beyond:

- Three lines of defense aligned with each other, overall corporate strategies, and the business helps drive increased performance
- Focus on risks and controls related to broad business objectives helps support stronger risk management practices
- Increased collaboration reduces the footprint on the business
- Opportunity to begin exploiting technology to drive effectiveness and efficiency through automation
Continuous monitoring

Continuous monitoring is defined as the continuous risk assessment, monitoring, and evaluation of the effectiveness and the efficiency of implemented processes and internal controls.

Continuous monitoring supports top- and middle-management, as well as the audit function. It enhances effectiveness and efficiency, and provides transparency in the business processes while helping keep costs under control.
Find issues or risks sooner …

If this were an assembly line, where would you want to find defects?

- Configuration
- Master Data
- Transactions
- Segregation of Duties (SOD)
- Key Risk Indicators (KRI)
Leading indicators may indicate an emerging risk.

Verifying configuration and master data settings can help prevent issues.

Checking transactions can discover problems on a timely basis.
Key risk indicators (KRIs) in SAP Risk Management

Key risk indicators (KRIs) indicate the potential for future adverse impacts to the organization — think of KRIs as an early warning system.

KRI examples:
- Product returns as a % of products shipped
- Decline in customer satisfaction ratio
- Number of injuries per period

Leading indicators may indicate an emerging risk.
Continuous monitoring of configuration and master data in SAP Process Control

System configurations and master data settings are often key preventive automated controls.

Examples:

- Verify tolerance settings in P2P
- Verify credit limit settings in O2C
- Verify key configuration settings remain unchanged
- Check that configuration and vendor master settings prevent duplicate invoices

Verifying configuration and master data settings can help prevent issues.
Continuous monitoring in SAP GRC solutions

Transaction monitoring can find issues that have already occurred and can even help automate control performance.

Examples:
- Identify and review prior period transactions
- Locate duplicate vendor invoices
- Review transactions over a threshold amount for a given G/L account

Checking transactions can discover problems on a timely basis.
Achieve higher confidence with lower costs
Achieve higher confidence with lower costs (cont.)

<table>
<thead>
<tr>
<th># controls</th>
<th>Less</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Controls</td>
<td>✗ Manual work</td>
<td>✓ Reliability</td>
</tr>
<tr>
<td></td>
<td>✗ Pushback from business</td>
<td>✓ Capture of expertise</td>
</tr>
<tr>
<td></td>
<td>✗ Cost of audit prep</td>
<td>✓ Best practices</td>
</tr>
</tbody>
</table>

Today: Manual Controls

Tomorrow: Automated Controls

Today: Manual Controls

Time: Today, Tomorrow
Achieve higher confidence with lower costs (cont.)

- **Today**
  - Manual Controls

- **Tomorrow**
  - Automated Controls
    - More
    - Controls
    - Granularity
    - Frequency of checks
    - Consistency
    - Manual Controls

- **The day after**
  - Automated Controls
  - Manual Controls
Auditors benefit several ways from automation

Key risk indicators can give auditors advance warning of important risk exposure

Control performance and testing is documented in and can be reviewed from a central location from a single source of truth

Many controls can be tested on a purely automated basis

Business rules for monitoring can also serve as an introduction to continuous auditing

… All saving the auditor time for more value-adding activities!
Customers benefit from SAP implemented for three lines of defense

<table>
<thead>
<tr>
<th>Support for CFO</th>
<th>Efficiency Gains</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helps CFO to respond to challenges of an increasingly global world with regards to Risks and Compliance in their <strong>Stewardship Role</strong> as well as in their <strong>Business Partner Role</strong></td>
<td><strong>Increased efficiencies</strong> through reduction of redundancies and new synergies between processes, subject matter experts, employees, and systems</td>
<td><strong>Greater transparency</strong> and access to information with standardized GRC methodologies, processes, and tools</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Overview</th>
<th>Risk Monitoring</th>
<th>External Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Improved overview</strong> of all relevant risks by combining and leveraging Strategic Risk Management, Operational Risk Management, and internal control systems</td>
<td><strong>Continuous and real-time risk monitoring</strong> throughout the organization on all levels</td>
<td><strong>Improved internal and external reputation</strong> with strict adherence to compliance and regulations</td>
</tr>
</tbody>
</table>
Agenda

1. Three Lines of Defense
2. Challenges and Opportunities
3. SAP Solutions for GRC
4. Additional Benefits
5. Wrap-Up and Conclusions
## Where to find more information

<table>
<thead>
<tr>
<th>SAP GRC on sap.com</th>
<th>SAP Community Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP GRC Value Calculators</td>
<td></td>
</tr>
<tr>
<td>SAP Process Control</td>
<td></td>
</tr>
<tr>
<td>SAP Audit Management</td>
<td></td>
</tr>
<tr>
<td>SAP Risk Management</td>
<td></td>
</tr>
<tr>
<td>SAP GRC Research</td>
<td></td>
</tr>
<tr>
<td>Managing Risk in an Age of Complexity</td>
<td></td>
</tr>
<tr>
<td>SAP GRC Three Lines of Defense for Audit Demo</td>
<td></td>
</tr>
<tr>
<td>Three Lines of Defense Demo</td>
<td></td>
</tr>
</tbody>
</table>
7 key points to take home

- Three lines of defense is widely accepted but often not fully or well implemented
- A single source of truth across the company is key for an effective three lines of defense framework
- Technology, especially continuous monitoring and automation, can provide up-to-date information available to all who need it
- SAP solutions for GRC provide a single technology platform, enabling cross-line and iterative communication
- An integrated GRC landscape provides a variety of benefits beyond simply supporting three lines of defense
- SAP GRC solutions help establish defined roles with clear accountability
- Auditors and management benefit from having real-time information in a single location
Thank you

Bruce McCuaig
Director, Product Marketing
SAP Governance, Risk and Compliance

bruce.mccuaig@sap.com
www.sap.com/grc