Fraud Prevention Trends in Eastern Europe: Continuous Control Monitoring

2012 ACFE European Conference
March 27, 2012

Zachary Rosen
President, ACFE Czech Republic Chapter
Manager, Enterprise Risk Services
Deloitte Advisory S.R.O.
Agenda

General Introduction to Public Procurement

Anti-Fraud Initiatives within Public Procurement in Czech & Slovak Republics

Use and Illustration of Continuous Control Monitoring in the Private Sector

Q & A
Anti-Fraud Initiatives within Public Procurement

General Uses of Government Funds

* Health and social services, infrastructure building
* National security, national disasters
* Public procurement take up a considerable part of overall GDP

How Much Is at Stake?

* Procurement: 15–20% of GDP, approximately 45% government spending
* Bribery and corruption: < US $1 trillion per year
* Systemic corruption = 20–30% of procurement

Anti-Fraud Initiatives within Public Procurement

* Public procurement — a government activity most vulnerable to corruption.
* Opportunities for public and private actors to divert public funds.

Anti-Fraud Initiatives within Public Procurement

The United Nations Convention against Corruption (UNCAC)

Key Components Contained Within UNCITRAL Article 9

* Procurement advertisements, evaluation criteria, and award procedures
* Procurement record and publishing of results, e-procurement
* Competition requirements
* More participants — harder to collude and hide collusion
* All steps in process can be challenged by any potential supplier
* Optional peer and independent administrative review mechanism
* Court procedures and public hearings/sanctions for bribery
* Guidance and training on ethics and integrity

Anti-Fraud Initiatives within Public Procurement

General Uses of Government Funds

* Health and social services, national security, national disasters
* Public procurement take up a considerable part of overall GDP

<table>
<thead>
<tr>
<th>Country</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>4.00</td>
<td>4.40</td>
<td>6.20</td>
<td>6.50</td>
</tr>
<tr>
<td>Denmark</td>
<td>3.20</td>
<td>3.00</td>
<td>4.00</td>
<td>4.40</td>
</tr>
<tr>
<td>Germany</td>
<td>1.10</td>
<td>1.20</td>
<td>1.40</td>
<td>1.30</td>
</tr>
<tr>
<td>Spain</td>
<td>4.10</td>
<td>3.60</td>
<td>3.40</td>
<td>3.20</td>
</tr>
<tr>
<td>France</td>
<td>4.40</td>
<td>5.40</td>
<td>6.40</td>
<td>7.40</td>
</tr>
<tr>
<td>Italy</td>
<td>2.30</td>
<td>2.30</td>
<td>2.50</td>
<td>3.40</td>
</tr>
<tr>
<td>Austria</td>
<td>1.70</td>
<td>2.40</td>
<td>2.30</td>
<td>2.30</td>
</tr>
<tr>
<td>Poland</td>
<td>5.80</td>
<td>7.10</td>
<td>8.20</td>
<td>8.70</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>4.10</td>
<td>5.30</td>
<td>5.20</td>
<td>5.60</td>
</tr>
<tr>
<td>Slovakia</td>
<td>3.60</td>
<td>3.70</td>
<td>6.80</td>
<td>11.60</td>
</tr>
</tbody>
</table>

Source: Eurostat (2011)
Anti-Fraud Initiatives within Public Procurement

**Common Procurement Types in Czech and Slovak Republics**

**Fixed-Price Contracts**
- Utilized when agreed upon cost for goods or services are determined
- Preferable to control costs/risk transferred to provider

**Cost-Reimbursement Contracts**
- Prepared when there is uncertainty of project costs
- Government assumes more risk

**Bid-Rigging Scenarios**
- Need Recognition schemes
- Special Needs schemes
Anti-Fraud Initiatives within Public Procurement

**Anti-Fraud Initiatives in the Czech Republic**
- National plan to implement e-procurement
- Regulatory compliance and new amendments to anti-corruption law, specifically:
  - Greater protection for whistleblowers, more accountability, increased disclosure requirements, and commercial register implementation

**Anti-Fraud Initiatives in the Slovak Republic**
- Active e-procurement system
- Amendments to the anti-corruption law in 2011 for greater transparency

**Limitations**
- Cases still persist where there is lack of full disclosure
- Suspicious procurement awards to questionable suppliers
Continuous Control Monitoring
“CCM”
Today’s Environment—Challenging Regulatory Requirements

- The U.S.’s FFIEC’s “Information Security Handbook,” a Gramm-Leach-Bliley Act supplement, requires that “Financial institutions should take reasonable steps to ensure that sufficient data is collected from secure log files to identify and respond to security incidents and to monitor and enforce policy compliance.”

- The Sarbanes-Oxley Act (SOX) requires executives and auditors of publicly traded companies in the U.S. to validate the accuracy and integrity of their financial reporting. Section 404 of the Act requires that companies create and maintain effective internal controls to track financial processes and “provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statements.”

- The Basel II Accord requires financial institutions to calculate credit, market and operational risks, in order to ensure that they have enough capital reserves to cover risk exposures.

- Foreign Account Tax Compliance Act, Foreign Corrupt Practices Act, UK Anti-Bribery Act
Today’s Environment—Dealing with Internal Control Weaknesses

Primary Internal Control Weakness Observed by CFEs

- Lack of Internal Controls: 37.8%
- Override of Existing Internal Controls: 19.2%
- Lack of Management Review: 17.9%
- Poor Tone at the Top: 8.4%
- Lack of Competent Personnel in Oversight Roles: 6.9%
- Lack of Independent Checks/Audits: 5.6%
- Lack of Employee Fraud Education: 1.9%
- Lack of Clear Lines of Authority: 1.8%
- Lack of Reporting Mechanism: 0.6%

Source: ACFE 2010 Report to the Nations on Occupational Fraud and Abuse
Fraud Trends Within Organizations

* Research indicates 50% of fraud cases are related to corruption in sales and procurement — collusion/kickbacks with third parties and suppliers.
* Half of all frauds reported take place within the banking, manufacturing, government administration, and retail sectors.
* Expense reimbursement fraud and cash theft are also significant fraud trends taking place in the region.
* Average total losses per fraud are estimated at $1 million.
* The perpetrator most commonly is a male already working for the organization 5+ years. Typical role for the perpetrator is in an executive or manager-level position within accounting, operations, or procurement.

Source: ACFE Report to the Nations on Occupational Fraud and Abuse, 2010
Common Red Flags in Asset Misappropriation

Larceny (Cash on hand, from deposit)

*Red Flags*

- Excessive number of cash register voids, discounts, and returns. Discrepancies between bank deposits and posting. Sudden activity in dormant banking accounts.

Skimming (Unrecorded, understated sales receivables)

*Red Flags*

- Billing for services not rendered and collecting cash, pocketing payments on customers’ accounts, issuing receipts on self-designed receipt books

Fraudulent Disbursements

*Red Flags*

- Billing — recording fictitious transactions on books to cover up theft
- Payroll — falsifying timesheets for higher amount of pay
- Expense reimbursements — paying personal expenses with business funds
Employee Red Flags

- Living beyond means, personal financial difficulties, or family problems
- Control issues — unwilling to share work duties
- Unusually close relationship with vendor/customer
- Refusal to take vacations
- Past employment or legal problems or complained about adequate pay

Management Red Flags

- Reluctance to provide information to auditors
- Management decisions dominated by individual or small group
- Weak internal control environment
- Accounting personnel are inexperienced in their duties
- Excessive number of checking accounts
- Frequent changes in banking accounts or external auditors
- Excessive number of year-end transactions
- Photocopied or missing documents
Surveys released at the Institute of Internal Audit conference “Internal Audit Solutions for Tough Times” revealed that the bruising global recession took a toll on internal audit. For example:

* 74% of internal audit functions experienced flat or declining budgets in 2009
* 33% of IA departments reduced staff sizes in the past year
* 80% of internal audit functions anticipated flat or declining budgets (among similar, related findings)
* Despite the fact that 57 percent of IA departments have increased coverage of operational risks in 2009.

Continuous controls monitoring is an emerging governance, risk, and compliance technology that monitors controls in ERP and other financial applications to improve financial governance, monitor and verify access and transactional rules, and automate audit processes.

A set of technologies applied to controls in financial applications to assist in:

* Reducing the cost of auditing through continuous auditing (CA)
* Reducing business losses through continuous monitoring (CM)
* Improving business performance by ensuring that automated process controls are working effectively and as intended
* CCM technologies are applied automatically and periodically to support processes that are repeatable, consistent, and predictable
The four technologies that make up CCM are:

**PRIMARY CONTROLS**
- **CCM for segregation of duties (CCM-SOD)** is used to manage a number of access conflicts present in ERP and financial applications.
- **CCM for transactions (CCM-T)** is used to continuously monitor ERP and financial application transaction information to improve governance and automate audit processes.

**SECONDARY CONTROLS**
- **CCM for master data (CCM-MD)** automates controls related to ERP and financial application data.
- **CCM for application configuration (CCM-AC)** is used to monitor the presence, appropriate configuration and modification of built-in application controls.
Birth and Evolution of CCM

1999 and Prior
- Manual Controls
- Fragmented Internal Audit
- Outside Audit
- Luck

2000
- Enron

2001

2002

2003

2004

2005

2006

2007

2008
- Financial Crises

2009

2010

2011 and Fwrd

Improving Processes
- Addressing Risk Framework
- SOD and Transaction Controls
- Compliance Depts.

CCM
- Data & Textual Analytics
- Minimizing Compliance Costs

Gramm-Leach-Bliley Act
- FCPA

U.S. PATRIOT Act (AML)
- EU Directive Privacy
- Sarbanes-Oxley
- Basel II

 görmek
- SEC
- German Anti-corruption Act
- HIPAA

PCAOB Audit Std 5
- Third EU Money Laundering
- FATCA
- Basel III

Frank-Dodd
Internal Control Maturity Model

How Do I Compare to Others?

<table>
<thead>
<tr>
<th>Manual-based processes and controls</th>
<th>Technology-enabled processes &amp; controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td><strong>Monitoring</strong></td>
</tr>
<tr>
<td><strong>Manual</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Automated</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Manual-based processes and controls**
- Approach not driven by risk
- Redundant controls
- Manually-intensive business & IT processes and controls
- Inefficient testing
- “Reactive” approach to identifying & addressing control issues
- Risk based approach
- Rationalized controls
- Management platform
- Manually intensive testing procedures
- Large sample sizes

**Technology-enabled processes & controls**
- Leverage application-based business & IT process controls
- User access & SOD controls
- Efficient operation of controls
- Efficient testing of controls
- Some automated testing capabilities
- Reduced sample sizes
- Continuous monitoring controls
- Efficient operation of controls
- “Proactive” approach to identifying & addressing control issues
- Demonstrated effectiveness of controls
- Sustainable compliance processes
- ROI / Business value
## CCM Value Proposition

<table>
<thead>
<tr>
<th>Quality Component</th>
<th>Issue</th>
<th>CCM Remedy</th>
</tr>
</thead>
</table>
| **Efficiency**    | • Increased pressure to reduce duplicative testing efforts and cost of compliance across multiple regulatory requirements | • Ability to analyze 100% of transactional data across the enterprise, improving the quality, effectiveness and efficiency of audits  
 |                   |                                                                      | • Timely notification of trends, patterns and exceptions supporting risk assessment |
| **Risk Focus**    | • Sample testing may not represent the risk inherent in the population  
 |                   | • Inefficient deployment of resources to test manual intensive and low risk transactions | • Early identification of risks and trends  
 |                   |                                                                      | • Designing top-down analyses to identify higher risk processes/entities/locations for more focused audit procedures |
| **Reliability**   | • Increased co-ordination between internal and external auditors to leverage testing efforts | • Provides a method to monitor for completeness and accuracy of transactions and evaluate tolerance thresholds  
 |                   |                                                                      | • Reduces effort, cost, and reliance on external resource by increasing control reliability |
| **Sustainability**| • Shift in focus from auditing to monitoring  
 |                   | • Proactive v/s. reactive | • Provides a sustainable and repeatable process to enable data and control quality improvement. |
## CCM Value Proposition – Technology Enabled Control Capabilities

<table>
<thead>
<tr>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimized Business Process</td>
<td>Technology can drive process optimization via increased efficiencies, improved visibility, and real-time decision support</td>
</tr>
<tr>
<td>Improved Management of Key Processes</td>
<td>Improved visibility into the status of operations, trends, and issues for improved decision support via technology</td>
</tr>
<tr>
<td>More Focused Internal Audit Department</td>
<td>Embed technology-enabled controls into business processes via roles &amp; responsibilities to enable Internal Audit to return to traditional focus areas</td>
</tr>
<tr>
<td>More efficient testing process</td>
<td>Technology-enabled controls reduce testing efforts: “self-tests”, reduced sample sizes, automated testing</td>
</tr>
<tr>
<td>More reliable and efficient controls</td>
<td>More effective &amp; efficient controls enable a sustainable, cost effective compliance environment</td>
</tr>
</tbody>
</table>
## CCM — Features & Benefits

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Access Control Monitoring & Segregation of Duties Monitoring | • Monitor changes to user access/roles  
• Identify SOD violations  
• Detect executed transactions that violate SOD rules | • Detect unauthorized modifications to user access/roles  
• Monitor access to sensitive transactions and data  
• Prevent SOD conflicts which increase risk of fraud/error |
| Transaction Monitoring                        | • Identify suspicious transactions for further review  
• Flag anomalies for investigation  
• Isolate transactions not in compliance with business rules | • Identify and recover inappropriate negative cash flows (e.g., duplicate payments)  
• Provide evidence of operation of controls in system transactions  
• Quickly identify data integrity issues |
| Master Data Monitoring                        | • Monitor changes to master data files (e.g., Supplier Master) for suspicious activity | • Identify & address suspicious changes to master data  
• Detect stale master file records |
| Application/Configurable Control Monitoring   | • Detect changes to system setups & control configurations that may increase risks of fraud/error | • Demonstrate the continued effectiveness of application controls |
Benefits of CCM — Regulatory Compliance and Savings

An international bank with branches in 20 countries and more than $100 billion in assets under management, utilizes Intellinx for complying with a new Basel 2 Operational Risk equivalent regulation that requires banks to maintain a very detailed audit trail of user access to customer data including all update and query activities.

* The bank had a log of some of the update transactions but none of the query transactions. Implementing a log for all the transactions required changes in thousands of mainframe application programs.
* The bank estimated that it would require about 100 programmer-months to accomplish this task, with total cost of over $1 million.
* Alternatively, the bank implemented Intellinx and achieved immediate compliance with the new regulation without changing any code, saving over $1 million.
A credit card company implemented Intellinx for detecting information leakage and internal fraud.

* The company is using Intellinx for recording user activity in the corporate internal applications allowing the internal auditors to replay every screen and keystroke of every end-user. The company utilizes the Intellinx business rules for tracking end-user behavior patterns generating alerts on exceptions in real-time.
A large government agency with more than 11,000 employees has implemented Intellinx for recording the activity of all its end users in the internal business applications, generating a very detailed audit trail of user access to citizens’ sensitive data.

* The agency has informed all of its employees and contractors that, from now on, all their actions are being recorded in order to deter potential fraud and information leakage.
A European insurance company deployed Intellinx to detect internal fraud.

* One of the main objectives was to track activity of privileged IT users including database administrators, system administrators and programmers. Users pose a special threat due to technical knowledge and authorized access to internal servers and system resources.

* Intellinx business rules were implemented for generating alerts in real time on suspicious behavior such as an attempt to update data in a production database by a privileged user using a database utility that cannot be traced by other means except for Intellinx.
Benefits of CCM — Eliminating SoD violations and Increased Efficiency in Compliance

In addition to eliminating 83,000 SoD violations within their SAP system and strengthening their regulatory compliance, a large telecom company realized the following key benefits with the implementation of CCM:

* Establishing business stewardship over SAP access
* Achieving their goal of zero unmitigated SoD violations
* Ongoing monitoring of changes to SAP access
* Reducing effort required for SOX compliance
* Increasing business confidence in SAP
* Automating the SAP user access request and approval process
* Setting an example for other divisions, who are now following suit
ABC is currently initiating a global continuous monitoring (CM) project and plans to launch a pilot in the first regional business center. The selected software platform for CM is ACL. The scope meeting was conducted to determine the following tasks:

- Definition of CM Key Performance Indicators and manner they are measured
- Building a template for dashboards that would be used in the CM implementation
- Identification of top risks for the CM initiative and assist in finding mitigating controls and action steps
- Establishing a CM process, define roles and responsibilities
- Definition of framework for operation of the CM Center of Excellence (CoE)
- Assistance in the strategy definition of the CM initiative
- Identification of all potential future areas for CM and their prioritization
The main principle of risk management and subsequently of internal controls and (continuous) controls monitoring is to preserve value. Risks are inherently decreasing value creation. Therefore, the identification of risks is initially determined.
CCM Case — ABC Manufacturing

Managing the enterprise risks by internal controls and controls monitoring requires involvement of multiple parties within the company and group.
Focus Area 1: Governance, Risk, and Compliance (GRC)
A structured approach to enterprise risk management which respects the involvement of multiple parameters affecting the entire process. These are:

* **Governance** — Firm’s business and IT strategy, vision, culture, internal directives and common practice
* **People** — Employees, business partners and customers
* **Process** — Firm’s services and products, sets of activities together with control mechanisms, regulatory requirements transformed into processes and process outputs to assure compliance;
* **Technology** — Information systems supporting firm’s people, processes and governance.

GRC is a framework for companies’ needs to gain management oversight over risk management, compliance and losses incurred due to unmitigated risks. It consists of a set of steps, sample deliverables, and analytical solutions that can be tailored and involved on a specific engagement.
Focus Area 2: Risk Intelligence

A management approach that leverages risk for value creation and preservation.

Nine Principles for Building a Risk Intelligent Enterprise

- Governing Bodies Responsibility
- Roles & Responsibilities
- Common Definition of Risk
- Common Risk Framework
- Common Risk Infrastructure
- Executive Management Responsibility
- Objective Assurance and Monitoring
- Business Unit Responsibility
- Support of Pervasive Functions

The Risk Intelligent Enterprise

- Risk Governance
- Oversight
- Board of Directors
- Sustain and Continuously Improve
- Executive Management
- Business Units and Supporting Functions

Risk Process

- Risk Ownership
- Risk Classes
- Strategy & Planning
- Governance
- Design, Implement & Test Controls
- Monitor, Assure & Escalate
- Identity Risks
- Assess & Evaluate Risks
- Integrate Risks
- Respond to Risks
- Operations/Infrastructure
- Compliance
- Reporting
Case Example – ABC Manufacturing

Focus Area 2: Risk Intelligence

**Consolidated Reporting Layer**
The consolidated reporting layer provides information that enables executives and management to govern compliance, risk, and performance providing indicators monitoring the support for a successful Risk Intelligent entity.

**Management Layer**
The management layer provides the foundation to build an effective and efficient risk program. The management layer allows the company to support the governance, risk, and compliance environment from different views to meet multiple needs – including the opportunity to streamline controls when appropriate.

**Business Process Layer**
The business process layer connects isolated business functions and orchestrates them into cohesive business processes. This layer includes business process integration, business process management, and business activity monitoring.

**Control Monitoring and Testing Layer**
The control layer is where the actual control activities are performed. This layer includes the automation and monitoring components provide for increased reliability, efficiency, and real-time decision support.

**The Foundation and Transaction Source Layer**
Technology infrastructure consists of the applications and protocols that manage data and communication across the enterprise.
## Risk Intelligence Program Summary

<table>
<thead>
<tr>
<th>Nine Principles</th>
<th>Phases</th>
<th>Assess</th>
<th>Develop</th>
<th>Implement</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governing Bodies Responsibility</td>
<td></td>
<td>1.1 Business and Risk Management Strategy</td>
<td>2.1 Board and Executive Management Risk Committees and Charters</td>
<td>3.1 Integrated Approach to Strategy and Risk Management</td>
<td>4.1 Board and Executive Management Performance and Risk Management Oversight</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2 Board and Executive Management Risk Oversight and Governance</td>
<td>2.2 Governance Structure</td>
<td>4.2 Business Strategy and Risk Management Execution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3 Risk Culture and Definition of Risk</td>
<td>2.3 Risk Culture, Taxonomy, Framework(s) and Metrics</td>
<td>3.2 Enhanced Risk Management Infrastructure to Support Business Operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4 Risk Treatment, Appetite and Limits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5 Risk, Compliance and Regulatory Framework(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6 Risk Management Methodology, Policies, Processes and Controls</td>
<td>2.4 Enhanced Risk Management Methodology, Policies, Processes and Controls</td>
<td>3.3 Assurance Framework, Programs and Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.7 Risk Management Technologies</td>
<td>2.5 Technology Infrastructure to Manage Enterprise Performance and Risk</td>
<td>3.4 Integrated Risk Management within Key Business Functions / Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.8 Data Governance</td>
<td>2.6 Resources, Skills and Training Program</td>
<td>4.3 Objective Assurance over the Risk Management Program</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.9 Resources, Skills and Training Activities</td>
<td>2.7 Change Management and Communications Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.10 Risk, Compliance and Regulatory Oversight Functions and Activities</td>
<td>2.8 Assurance Framework for Risk Oversight and Independent Assurance</td>
<td>4.4 Risk Processes and Controls / Escalation and Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.11 Internal Audit Function and Activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Infrastructure and Management</td>
<td></td>
<td>1.12 Enterprise and Business Unit Risks to Value Creation / Preservation</td>
<td>2.9 Risk Mitigation and Response Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.13 Risk Scenarios, Measurement, Vulnerability and Priority</td>
<td>2.10 Business Process and Control Enhancements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.14 Existing Risk Mitigation Activities / Business Processes and Controls</td>
<td>2.11 Key Risk/Performance Indicators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective Assurance and Monitoring</td>
<td></td>
<td>1.15 Risk, Compliance and Regulatory Oversight Functions and Activities</td>
<td>2.8 Assurance Framework for Risk Oversight and Independent Assurance</td>
<td>3.3 Assurance Framework, Programs and Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.16 Risk Management Methodology, Policies, Processes and Controls</td>
<td>2.5 Technology Infrastructure to Manage Enterprise Performance and Risk</td>
<td>3.4 Integrated Risk Management within Key Business Functions / Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.17 Risk Management Technologies</td>
<td>2.6 Resources, Skills and Training Program</td>
<td>4.3 Objective Assurance over the Risk Management Program</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.18 Data Governance</td>
<td>2.7 Change Management and Communications Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.19 Resources, Skills and Training Activities</td>
<td>2.8 Assurance Framework for Risk Oversight and Independent Assurance</td>
<td>4.4 Risk Processes and Controls / Escalation and Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.20 Internal Audit Function and Activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Ownership</td>
<td></td>
<td>1.21 Enterprise and Business Unit Risks to Value Creation / Preservation</td>
<td>2.9 Risk Mitigation and Response Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.22 Risk Scenarios, Measurement, Vulnerability and Priority</td>
<td>2.10 Business Process and Control Enhancements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.23 Existing Risk Mitigation Activities / Business Processes and Controls</td>
<td>2.11 Key Risk/Performance Indicators</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.24 Risk, Compliance and Regulatory Oversight Functions and Activities</td>
<td>2.8 Assurance Framework for Risk Oversight and Independent Assurance</td>
<td>3.3 Assurance Framework, Programs and Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.25 Risk Management Methodology, Policies, Processes and Controls</td>
<td>2.5 Technology Infrastructure to Manage Enterprise Performance and Risk</td>
<td>3.4 Integrated Risk Management within Key Business Functions / Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.26 Risk Management Technologies</td>
<td>2.6 Resources, Skills and Training Program</td>
<td>4.3 Objective Assurance over the Risk Management Program</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.27 Data Governance</td>
<td>2.7 Change Management and Communications Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.28 Resources, Skills and Training Activities</td>
<td>2.8 Assurance Framework for Risk Oversight and Independent Assurance</td>
<td>4.4 Risk Processes and Controls / Escalation and Response</td>
<td></td>
</tr>
<tr>
<td><strong>General Ledger</strong></td>
<td><strong>Account Payable</strong></td>
<td><strong>Account Receivable</strong></td>
<td><strong>Master Data</strong></td>
<td><strong>Payment</strong></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>-----------------------</td>
<td>-----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>✔ Conflict of interest (i.e., mandates versus customers / suppliers)</td>
<td>✔ Three-way match (PO-Delivery Notes-Invoices)</td>
<td>✔ Customer invoices booked without tax code</td>
<td>✔ Duplicate customers/vendors</td>
<td>✔ Payments to bank account numbers not registered in the master data</td>
<td></td>
</tr>
<tr>
<td>✔ Reactivated/inactive/ blocked/one-time accounts</td>
<td>✔ Vendor invoices booked without tax code</td>
<td>✔ Customers with multiple tax codes</td>
<td>✔ Missing critical customer/vendor’s master data (name, address)</td>
<td>✔ Payments to customers</td>
<td></td>
</tr>
<tr>
<td>✔ Unusual journal entries (BE GAAP)</td>
<td>✔ Link between suppliers / employees</td>
<td>✔ Link between customers/employees</td>
<td>✔ Customers/vendors with invalid VAT numbers</td>
<td>✔ Payments from vendors</td>
<td></td>
</tr>
<tr>
<td>✔ Period end testing</td>
<td>✔ Long outstanding vendor invoices</td>
<td>✔ Long outstanding customer invoices</td>
<td>Transactions booked for customers/vendors not registered in the master data</td>
<td>✔ Cash transactions above legal thresholds</td>
<td></td>
</tr>
<tr>
<td>✔ Sequence numbering testing</td>
<td>✔ Vendor invoice paid before invoice date</td>
<td>✔ Credit note amounts exceeding invoice amounts</td>
<td>✔ Etc.</td>
<td>✔ Payments with reference to public exposed persons (PEP listed)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Tax</strong></th>
<th><strong>Inventory</strong></th>
<th><strong>Payroll</strong></th>
<th><strong>Fraud</strong></th>
<th><strong>FCPA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Invalid VAT numbers</td>
<td>✔ Inventory value recalculation</td>
<td>✔ Falsified salary and hours</td>
<td>✔ Journal entries reversed after cut off</td>
<td>✔ Customers / suppliers mentioned on black lists</td>
</tr>
<tr>
<td>✔ Transactions booked using VAT codes not registered in the VAT master data</td>
<td>✔ Stock registration sanity checks</td>
<td>✔ Unauthorized benefits (pension payments/insurance payments)</td>
<td>✔ Journal entries during weekends/holidays</td>
<td>✔ Payments to customers in sensitive regions</td>
</tr>
<tr>
<td>✔ Sold to foreign country and ship to local with VAT exempt code</td>
<td>✔ Lower of cost or market</td>
<td>✔ Expenses and allowance fraud</td>
<td>✔ Concentrations of manual entries</td>
<td>✔ Cash transactions above legal thresholds</td>
</tr>
<tr>
<td>✔ Overview of the VAT rates applied including old and incorrect VAT rates</td>
<td>✔ Etc.</td>
<td>✔ Incorrect payroll payments</td>
<td>✔ Concentrations of transfers between customer/supplier’s accounts</td>
<td>✔ Large amounts posted under travel/entertainment/gift/hotel</td>
</tr>
</tbody>
</table>

**CCM Scripts**
General Ledger module

- Conflict of interest (i.e., mandates versus customers/suppliers; employees versus suppliers)
- Concentrations of manual entries: Reactivated/inactive/blocked/one-time accounts
- Unusual journal entries (BE GAAP) and quality of masterdata
- Duplicate payments/invoices testing — Old documents (document date versus posting date)
- Customer CN testing
  - Customers with large percentages of credit notes
  - Large CN at year end, etc.
- Period-end testing and round-amount checks
- Sequence numbering testing and cash transactions above legal threshold
- Customers/Suppliers in sensitive regions and payments to customers/from suppliers
- CODA testing
Data Analysis Detailed Modules

Account Payables module

- Three-way match (PO, delivery notes, invoices) / Reconciliations between payments and invoices based on clearing code
- Vendor invoices booked without tax code / Vendors with multiple tax codes
- Link between suppliers/employees / Indications of duplicate invoices
- Long outstanding vendor invoices / Large delay between vendor invoices and payment
- Large delay between payment date and registration of clearing / Vendor invoice booked/paid before PO date / Vendor invoice paid before invoice date / three-way match (PO, invoice, payment)
- Invoices without purchases order
- Supplier CN testing
  - Credit notes amounts exceeding invoice amounts
- Vendors in sensitive regions / Payments to bank accounts not registered in the master data
- Different currencies for the same vendor / Indications of duplicate vendor payments
- Vendors with foreign bank accounts
Account Receivables module

- Customer invoices booked without tax code / Customers with multiple tax codes
- Indications of duplicate invoices / Long outstanding customer invoices
- Large delay between customer invoices and payment
- Large delay between payment date and registration of clearing
- Three-way match (SO, invoice, payment) / Invoices without sales order
- Credit note amounts exceeding invoice amounts
- Customer CN testing
  - Customers with large percentages of credit notes / Large CN at year end
- Customers in sensitive regions / Different currencies for the same customer
- Customers with large cash transactions
Data Analysis Detailed Modules

**Master Data Testing module**
- Duplicate customers/vendors (based on name, VAT number, address, bank account #)
- Missing critical customer/vendor’s master data (name, address)
- Customers/vendors with invalid VAT numbers
- Transactions booked for customers/vendors not registered in the master data

**Payment module**
- Payments to bank account numbers not registered in the master data
- Payments to customers / Payments from vendors / Cash transactions above legal thresholds
- Payments with reference to public exposed persons (PEP listed), blacklisted entities
Data Analysis Detailed Modules

**Tax module**
- Invalid VAT numbers
- Transactions booked using VAT codes not registered in the VAT master data
- Sold to foreign country and ship to local with VAT exempt code
- Overview of the VAT rates applied including old and incorrect VAT rates
- Link between intercompany and customer invoice on the VAT numbers
- Invoices without VAT or hidden VAT

**Inventory module**
- Inventory value recalculation
- Stock registration sanity checks
- Lower of cost or market
Data Analysis Detailed Modules

Payroll module

- Falsified salary and hours
  - Large number of payments / frequency of payments / payments outside normal payment times
  - Large amounts paid / Large salary increases / Large bonus (general + in comparison/w gross salary)
  - Large number of hours / overtime (per day, week, month) / Large number of vacation days
- Unauthorized benefits (Pension fund & Insurance payments)
  - Large amounts / Large amounts in comparison with gross salary / Increases
- Incorrect payroll payments
  - Reconciliation time registration — payroll (hours worked, vacation days)
  - Duplicate payments / Recalculations (deductions) / Reconciliation amounts paid – amounts calculated
- Peer group analysis (hours, salary amount, bonus amount, expenses)
- VAT and tax reporting
Data Analysis Detailed Modules

Expense & allowance fraud

- Large allowances / Allowances amounts (variances within allowance category)
- Increases / Large expenses / Increases/change in behavior / Expenses abroad / Large expenses in-country
- Expenses during weekend/holiday/vacation/absence (in-country/abroad)
- Restaurant expenses / Fuel expenses (<> company car list)
- Ghost employees
  - No vacation / No deductions (taxes, social security, etc.) / Duplicates on employee list (name, address, bank account)
  - Invalid registration number / Blank address or PO Box / No time registration
  - Employees older than retirement age / Payments after leaving date
  - Reconciliation company address book — payroll list (ghost employees)
Fraud module

- Comparison of company mandates of directors with customer / supplier master data
- Comparison of HR master data with customer/supplier master data
- Concentrations of manual entries / Concentrations of transfers between customer/supplier's accounts
- Concentrations of credit notes, rebates, discounts / Concentrations of purchase orders just below the signatory thresholds
- Reactivation of dormant accounts / Use of deleted/blocked accounts
- Use of accounting codes not registered in the chart of accounts / Journal entries reversed after cut off
- Journal entries during weekends/holidays / Sold to on party and ship to another party
- Sold from or to one party and payments to or from another party
Identification of Relevant Business Risks
* Perform analysis and identification of risks applicable for ABC at regional business center location.
* Identification of risks to be based on existing internal documentation related to risk management process (risk assessment, controls framework).

CM Strategy Development and the Definition of the CM Process
* Defined based on detailed tasks descriptions followed by assignment of responsible ABC staff.
* Development of a feasible timeframe for executing, implementing, and accepting the tasks from the CM implementation strategy.
* Definition of CM Key Performance Indicators and the manner in which they are measured. The CM KPIs and measurement techniques will be defined as a set of metrics, technical adoption descriptions, responsibility definition, and workflow/escalation definition.

CCM Dashboards
* Extremely useful for CCM and can be created during CCM implementation.
* Dashboards provide summary reports regarding the effectiveness of the controls monitoring environment, and as such, are dependent on the monitored controls. Deloitte’s approach is to diversify CM Dashboards according to risk areas (e.g., fraud, compliance, governance, etc.)
Establishing CCM Process /
Defining Roles & Responsibilities

- The CM process will be defined in the form of a flowchart depicting the individual tasks of specific roles and followed by a narrative explaining the flowchart. Every process or sub-process follows the principle of Deming’s cycle (PDCA — plan, do, check, act) in order to assure the continuous improvement over time. Every process or sub-process will also have an RACI (definition of responsible, accountable, consulted and informed parties) matrix included. The objective of establishing the CM process is to move from an ad-hoc or manual controls testing and monitoring environment to a to semi-automated or fully automated and monitored environment:

<table>
<thead>
<tr>
<th>Manual-based processes and controls</th>
<th>Technology-enabled processes &amp; controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td><strong>Monitoring</strong></td>
</tr>
<tr>
<td>- Approach not driven by risk</td>
<td>- Continuous monitoring controls</td>
</tr>
<tr>
<td>- Redundant controls</td>
<td>- Efficient operation of controls</td>
</tr>
<tr>
<td>- Manually-intensive business &amp; IT</td>
<td>- “Proactive” approach to identifying &amp;</td>
</tr>
<tr>
<td>processes and controls</td>
<td>addressing control issues</td>
</tr>
<tr>
<td>- Inefficient testing</td>
<td>- Demonstrated effectiveness of controls</td>
</tr>
<tr>
<td>- “Reactive” approach to identifying &amp; addressing control issues</td>
<td>- Sustainable compliance processes</td>
</tr>
<tr>
<td>- Risk based approach</td>
<td>- Reduced sample sizes</td>
</tr>
<tr>
<td>- Rationalised controls</td>
<td>- Efficient testing capabilities</td>
</tr>
<tr>
<td>- Management platform</td>
<td>- Large sample sizes</td>
</tr>
<tr>
<td>- Manually intensive testing</td>
<td>- Leverage application-based business &amp; IT process controls</td>
</tr>
<tr>
<td>procedures</td>
<td>- User access &amp; SOD controls</td>
</tr>
<tr>
<td>- Efficient operation of controls</td>
<td>- Efficient operation of controls</td>
</tr>
<tr>
<td>- Efficient testing of controls</td>
<td>- Some automated testing capabilities</td>
</tr>
<tr>
<td>- Demonstrated effectiveness of</td>
<td>- Reduced sample sizes</td>
</tr>
<tr>
<td>controls</td>
<td></td>
</tr>
<tr>
<td>- Sustainable compliance processes</td>
<td></td>
</tr>
<tr>
<td>- ROI / Business value</td>
<td></td>
</tr>
</tbody>
</table>

Case Example — ABC Manufacturing
With the migration towards automated and continuous monitoring of internal controls, changes will also be required to the reporting and overview dashboards.
Definition Framework for CCM Operation — ABC Manufacturing

Model 1 — Centralized Delivery

Characteristics
- Centralized — skilled resource pool resides within the CoE
- Delivers end-to-end CM deployment services to business areas
- Establishes and governs standards, guidelines and processes for CM technologies/tool use, based on industry best practices and internal experience

Benefits
- Best coordination of scarce resources across Client X
- Establishes center of best practice and expertise
- Better ability to manage quality of project deliverables
- Offers a career path for CM resources

Challenges
- Difficult to allocate costs for CoE to business areas
- High number of skilled FTE required to staff CoE to provide end-to-end delivery
- Business areas will have to relinquish control over project delivery to the CoE
- Robust CM CoE resource planning and project prioritization is required

Model 2 — Pooled Resources

Characteristics
- Hybrid — centralized, small pool of resources within CoE who are assigned to projects managed by business areas
- Assists business areas with projects as internal consultants
- Provides guidance and consults on CM technologies/tools usage, standards, guidelines, processes, and best practices

Benefits
- Resource optimization with opportunity to build CM expertise in business areas
- Facilitates knowledge transfer and best practice sharing through resource rotation
- Offers a career path for CM resources

Challenges
- Difficult to allocate costs for CoE to business areas
- Availability of required skilled FTE for CoE in business areas
- Business areas may be challenged in releasing CM resources back to CoE
- Business areas need to have enough CM expertise to build business cases and execute projects

Model 3 — Knowledge Center

Characteristics
- Decentralized — small resource pool resides within the CoE; larger group of SMEs staffed within the business
- Provides guidance and governance on CM technologies/tools usage as well as standards, guidelines, processes and best practices
- Delivers training on CM technologies/tools

Benefits
- Best fit with decentralized funding model
- Minimal additional CoE headcount
- Quick implementation of the CoE

Challenges
- Limited focus on enterprise-wide program initiatives, more project-focused
- Less sharing of knowledge and best practices across business areas
- Business area-specific initiatives and priorities take precedence over CoE responsibilities
- Tool process, standards, and guidelines difficult to manage across projects
Public and private sectors are focusing their attention on technology through government e-procurement and CCM.

CCM monitoring is a key component of the compliance evolution.

CCM can enhance effectiveness of controls and increase efficiencies.

CCM facilitates timely intervention to decrease risk/increase compliance.

As companies begin to evolve their compliance environments, they will increasingly leverage technology for automated and monitoring controls.
You Decide

* What was the total amount of fraud uncovered at your company last year?
* What was not uncovered?
* Would an investment in CCM be worth it if you could reduce your fraud losses from 5% to 3%?
* Does it make sense to work smarter and not harder?
* Wouldn’t a risk-based approach on strategic GRC issues make more sense?
Q & A
Zachary Rosen
Manager, Enterprise Risk Services
Deloitte Advisory S.R.O.
Tel: +420 605 513 236
E-mail: zrosen@deloittece.com
“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.