asug
Americas' SAP Users' Group

How to Manage Enterprise and Cyber Risk Using the COSO Framework with SAP GRC Solutions

James Chiu, Director, Solution Management, SAP
Anne Marie Colombo, Cybersecurity Solution Advisor, SAP

Session ID # ASUG 84022

About the Speakers

James Chiu, CPA, CISSP

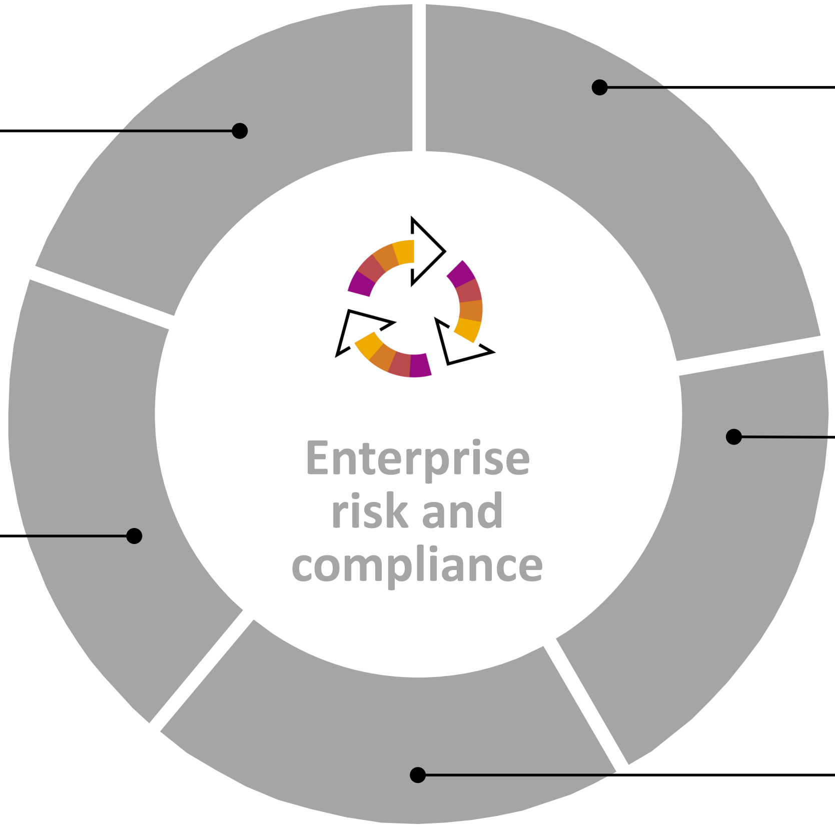
- SAP GRC Solution Owner, SAP
- Solution owner of SAP Audit Management, Process Control, and Risk Management. He has been involved with audit, risk, and compliance management and software at professional services firms and SAP for over 20 years.

Anne Marie Colombo, CISSP

- Cybersecurity Advisor, SAP
- Security Professional, 12 years, SAP Identity Access Management Solutions including Single Sign-on, Data Protection, Encryption solutions

SAP Risk Management

Preserve and grow value



Plan
Plan risk management within the context of value to the organization

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

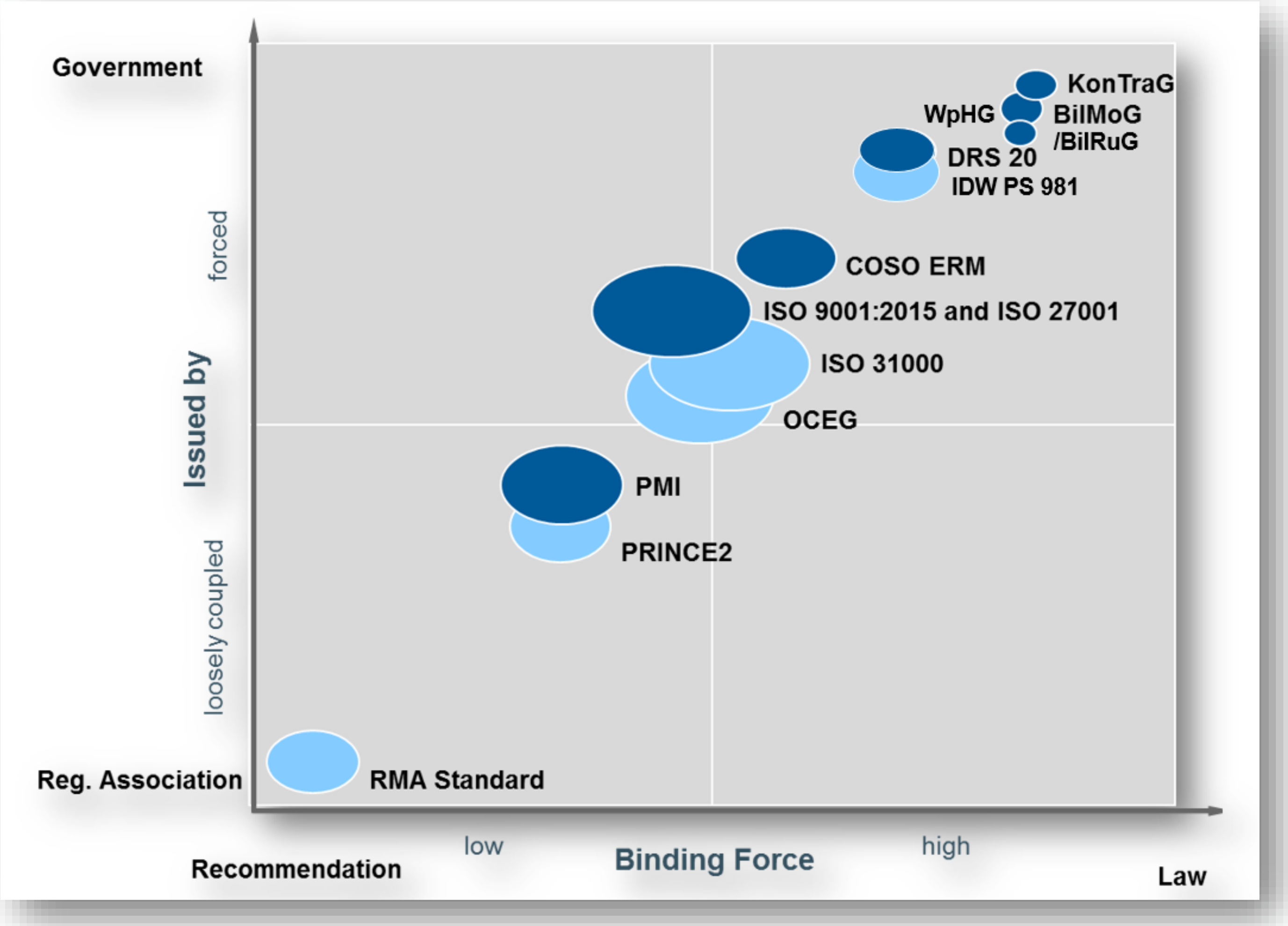
Analyze
Analyze risk via scenarios, modeling, and other factors to understand exposure

Respond
Respond to risk after balancing costs and benefits

Monitor and report
Monitor thresholds, effectiveness of risk responses, and corrective actions

How SAP is recording the risk information and assessing it

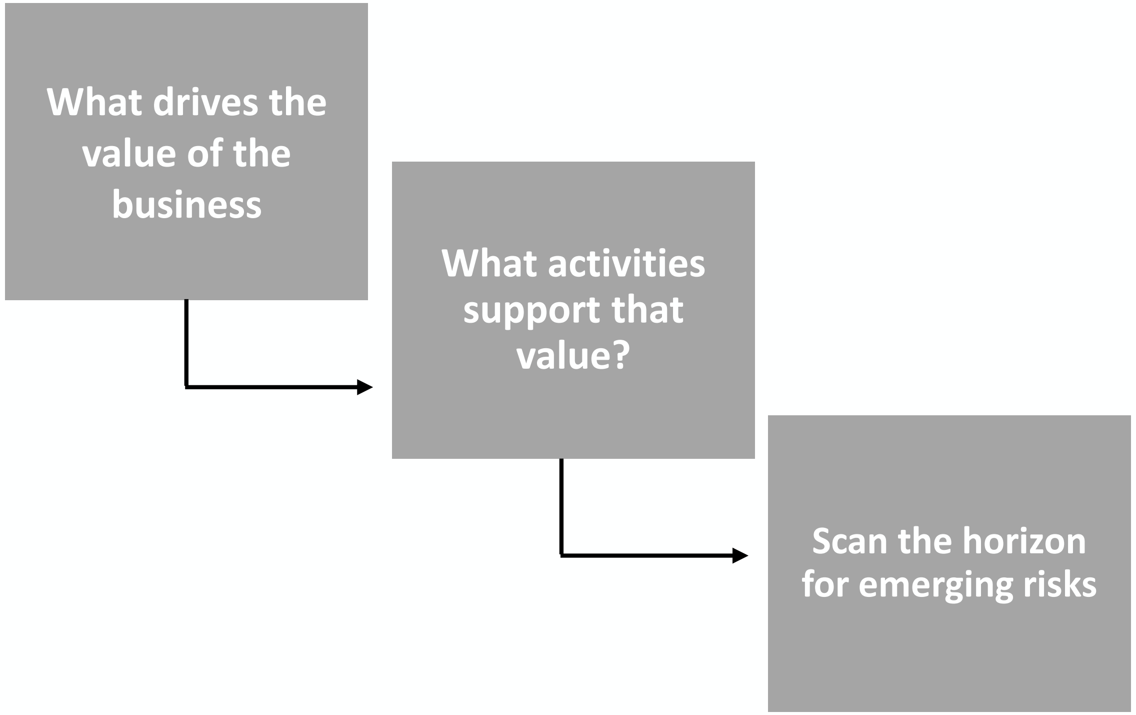
Compliance requirements



● Mandatory for SAP to comply with (size represents scope)

Plan – value proposition from planning and prioritization

Planning requires prioritization. Identify the value drivers of the business and focus on how value is created and destroyed.


What drives the value of the business
What activities support that value?
Scan the horizon for emerging risks

Align risk management with strategies and opportunities
Document risks and link to business objectives

Model and align risks to org structure
Utilize organizational hierarchies and flexible activity structures

Create/leverage risk and activity catalogs
Use standard risk templates for consistency

Document risk appetite
Assign thresholds for inherent, planned, and residual risk

Identify – value proposition

Risks to the business are more reliably identified by business users using tools to engage the business owners.

- Utilize surveys and charting capabilities
- Harness the wisdom of business managers with surveys for identifying and assessing risks

- Aggregate by organization category
- Map risks to organization hierarchy to manage accountability

- Identify risk impacts
- Standardize risk management and make it scalable

- Prioritize via an individualized heat map
- Add value by aligning risk appetite with the needs of the business; preserve value by identifying unnecessary risks

Analyze – value proposition

Analysis of risks provides insight. Quantitative tools provide the basis for risk acceptance or rejection.

Use modeling scenarios such as Monte Carlo simulation

Understand the probable losses

Determine inherent, residual, and planned residual risk levels

Gain insight into the profile of risk levels

Run “what-if” scenarios

Anticipate impacts of related risks

Incorporate qualitative and quantitative factors including velocity

Factor in management’s judgement

Respond – value proposition

Value is created only when risk is accepted responsibly for value-adding activities.

Value is preserved when risk is minimized in non-value-adding supporting activities.

Document responses

Ensure risks are managed consistently across the organization

Assign accountability

Ensure risks are not orphaned

Launch a workflow-driven response with remediation tracking

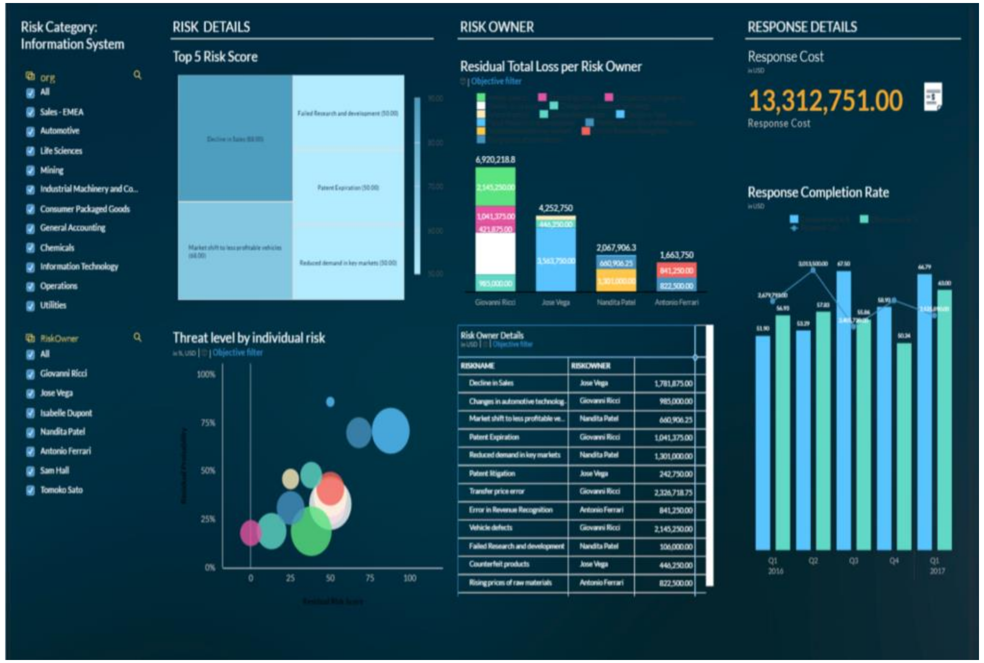
Create consistent, efficient, and auditable responses

Integrate with SAP Process Control and SAP Audit Management

Leverage the common frameworks across the three lines of defense

Monitor and report – the value proposition

Boards, executives, and stakeholders have oversight responsibilities that require monitoring and reporting capabilities.



Risk Owner Details

in USD | | Objective filter

RISKNAME	RISKOWNER	
Decline in Sales	Jose Vega	1,781,875.00
Changes in automotive technolog...	Giovanni Ricci	985,000.00
Market shift to less profitable ve...	Nandita Patel	660,906.25
Patent Expiration	Giovanni Ricci	1,041,375.00
Reduced demand in key markets	Nandita Patel	1,301,000.00
Patent litigation	Jose Vega	242,750.00
Transfer price error	Giovanni Ricci	2,326,718.75
Error in Revenue Recognition	Antonio Ferrari	841,250.00
Vehicle defects	Giovanni Ricci	2,145,250.00
Failed Research and development	Nandita Patel	106,000.00
Counterfeit products	Jose Vega	446,250.00
Rising prices of raw materials	Antonio Ferrari	822,500.00

- **Analytics and reports including heat maps**
- Visualize the distribution and level of risks

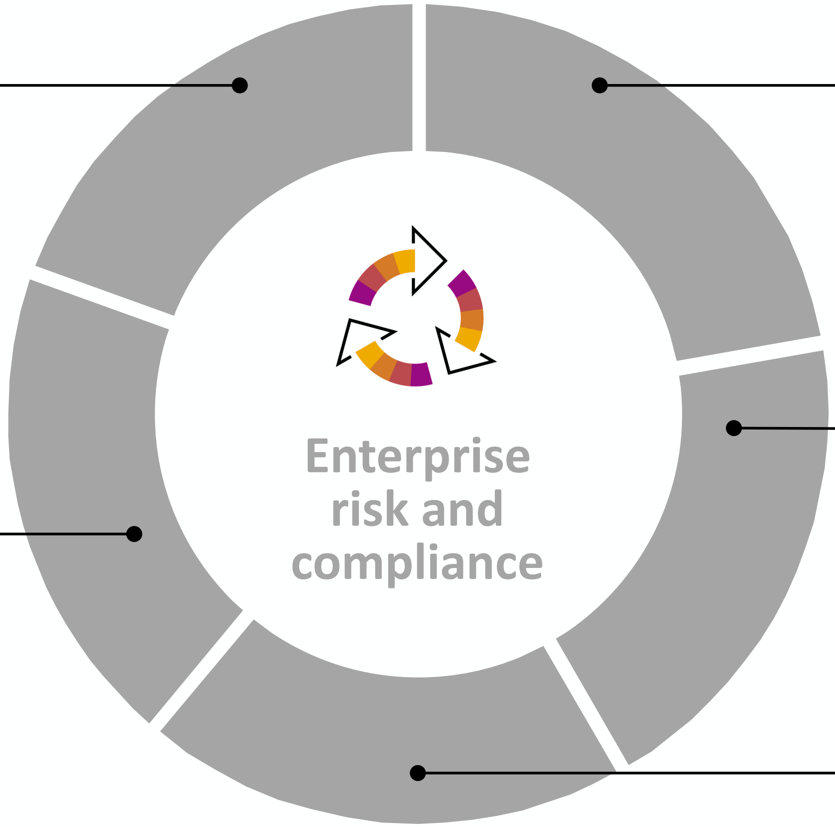
- **Notifications to risk owners via automated alerts and KRIs**
- Proactively respond to changes

- **Monitoring of response effectiveness**
- Maximize value and minimize losses

- **Assessment of impact on business objectives**
- Provide insight to the business

SAP Process Control

Help ensure effective controls and on-going compliance



Report
Insightful reporting for analysis and accountability

Evaluate
End-to-end test and issue resolution

Document
Single source of truth shared across the enterprise

Plan
Planning of focused actions to help ensure timeliness

Perform and monitor
Streamlined manual and automated performance

Document – value proposition

Streamlined, scalable support for multiple compliance regulations
Harmonized controls across financial and operational regulations

Wherever you are, whatever regulations or company initiatives you are subject to,

SAP Process Control can help you break down silos among your multiple GRC initiatives.

Reduce effort and cost

By sharing documentation and test results across regulations and company initiatives

Maintain accountability

By establishing geographic and regulatory ownership across the global enterprise

Harmonize and scale

With centralized maintenance of documentation and optional local variation and language support

Plan – value proposition

Risk assessments performed periodically
Determination of scope and test strategies

Not all internal controls are of equal importance. With top-down, risk-based scoping,

SAP Process Control can help you focus your documentation and test efforts.

Determine scope

By reviewing account materiality, as well as subprocess and control risk

Use resources wisely

By implementing risk-based test strategies that neither overtest nor undertest controls

Automate

Through selection of controls and transmittal of an evaluation workflow based on test strategies

Perform and monitor – value proposition

Automated control testing for SAP and non-SAP software systems
Exception-based, continuous control monitoring

Looking for a way to do more with less? Continuous control monitoring and automated testing

can reduce workload for business users and internal auditors while increasing timeliness and reliability.

Create your own rules

Without programming and deploy them across organizations using configurable parameters

Find issues faster

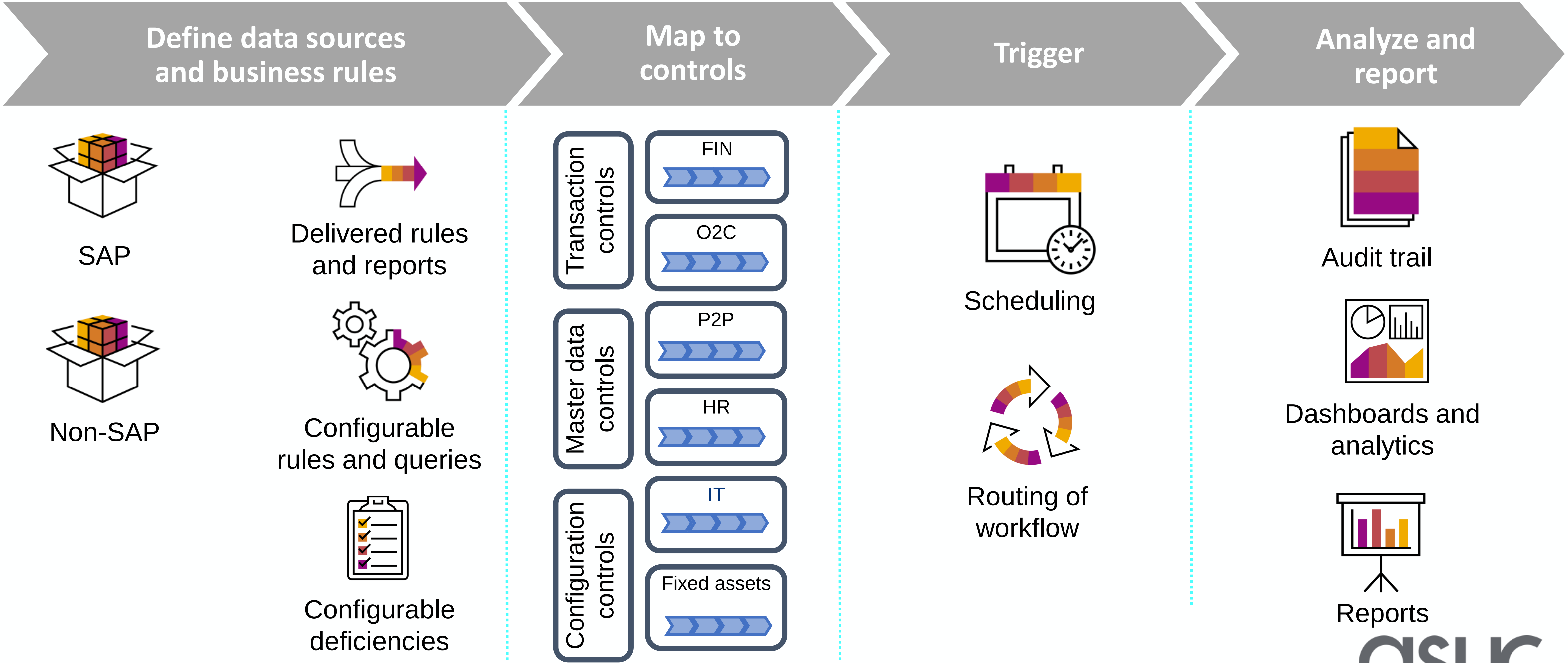
By scheduling continuous control monitoring to run on a recurring basis – "set it and forget it"

Manage by exception

By routing only exceptions through the workflow to the right person to review and correct, if needed

Automated control testing and monitoring of process flow

A high-level view of CCM process flow in SAP Process Control



Define data sources and business rules

SAP

Non-SAP

Delivered rules and reports

Configurable rules and queries

Configurable deficiencies

Map to controls

Transaction controls
- FIN
- O2C

Master data controls
- P2P
- HR

Configuration controls
- IT
- Fixed assets

Optional in version 12.0

Trigger

Scheduling

Routing of workflow

Analyze and report

Audit trail

Dashboards and analytics

Reports

FIN = finance; O2C = order to cash; P2P = procure to pay

Defining data sources

Where is the data?

SAP S/4HANA

SAP ECC

Other SAP

Non-SAP

Connectors

How to find it

HANA View

SOD (AC)

Configurable

SAP Query

Programmed

Other Ways

BW Query

How to refine it

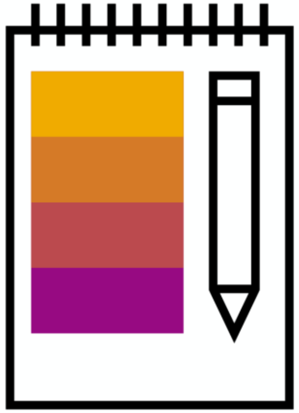
Field Selection and Labels

Filters

Evaluate – value proposition

Comprehensive control performance, evaluations, and issue management
Clear ownership and accountability with best-practice workflows

Regardless of whether you evaluate your controls with self-assessments or more-formal tests of effectiveness.



SAP Process Control can streamline workflow-driven processes either online or offline.

Assign ownership and responsibility

Without the need for IT authorization or workflow experts

Avoid missed deadlines

Through automatic release of e-mail-based reminders and escalations

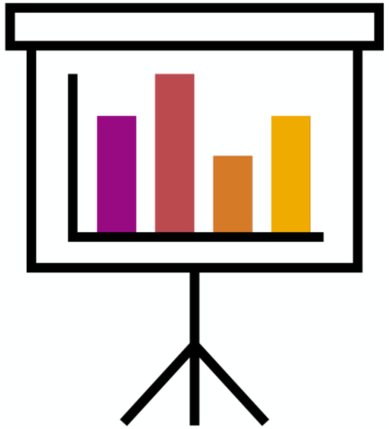
Track it all

With detailed tracking of control performance, evaluations, issues, and remediation plans

Report – value proposition

Insightful analytics to support decisions and promote accountability
Built-in or custom reports with SAP BusinessObjects Business Intelligence (BI) suite

Whether you are tracking compliance status or producing year-end reports,



SAP Process Control provides a variety of standard, configurable, and custom reporting options.

Use extensive standard reports

To get deep and real-time insight into the status of your controls and critical issues

Take action

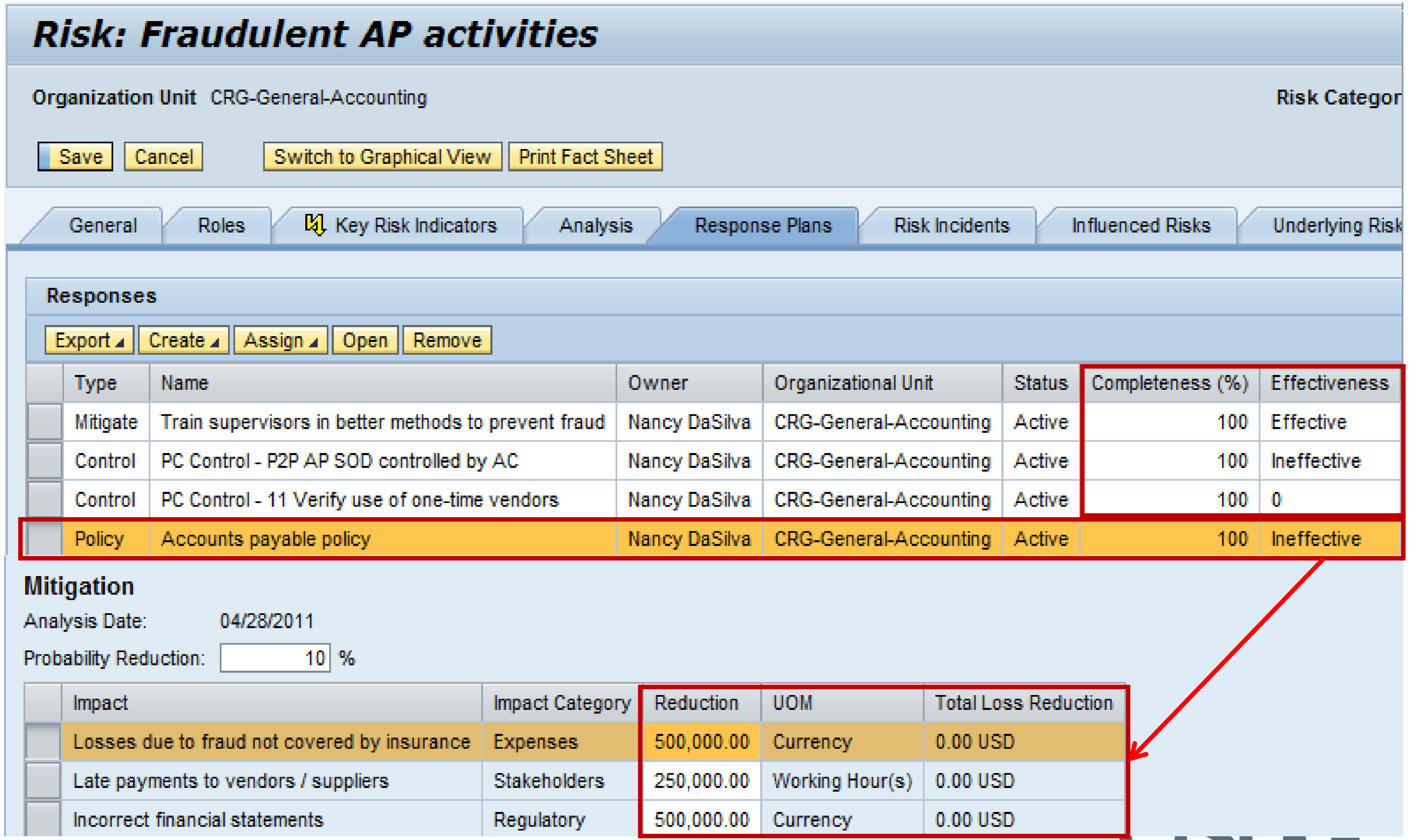
By identifying the source of problems through drilling down to the most-granular details, if necessary

Build your own

By slicing and dicing data for deeper analyses with powerful visualization possibilities

Leveraging SAP Risk Management integration

- With SAP Risk Management product integration:
  - Policies can be assigned as risk responses to reduce residual risk, depending upon completeness and effectiveness of the policy



Risk: Fraudulent AP activities

Organization Unit CRG-General-Accounting

Risk Categor

Responses

Type	Name	Owner	Organizational Unit	Status	Completeness (%)	Effectiveness
Mitigate	Train supervisors in better methods to prevent fraud	Nancy DaSilva	CRG-General-Accounting	Active	100	Effective
Control	PC Control - P2P AP SOD controlled by AC	Nancy DaSilva	CRG-General-Accounting	Active	100	Ineffective
Control	PC Control - 11 Verify use of one-time vendors	Nancy DaSilva	CRG-General-Accounting	Active	100	0
Policy	Accounts payable policy	Nancy DaSilva	CRG-General-Accounting	Active	100	Ineffective

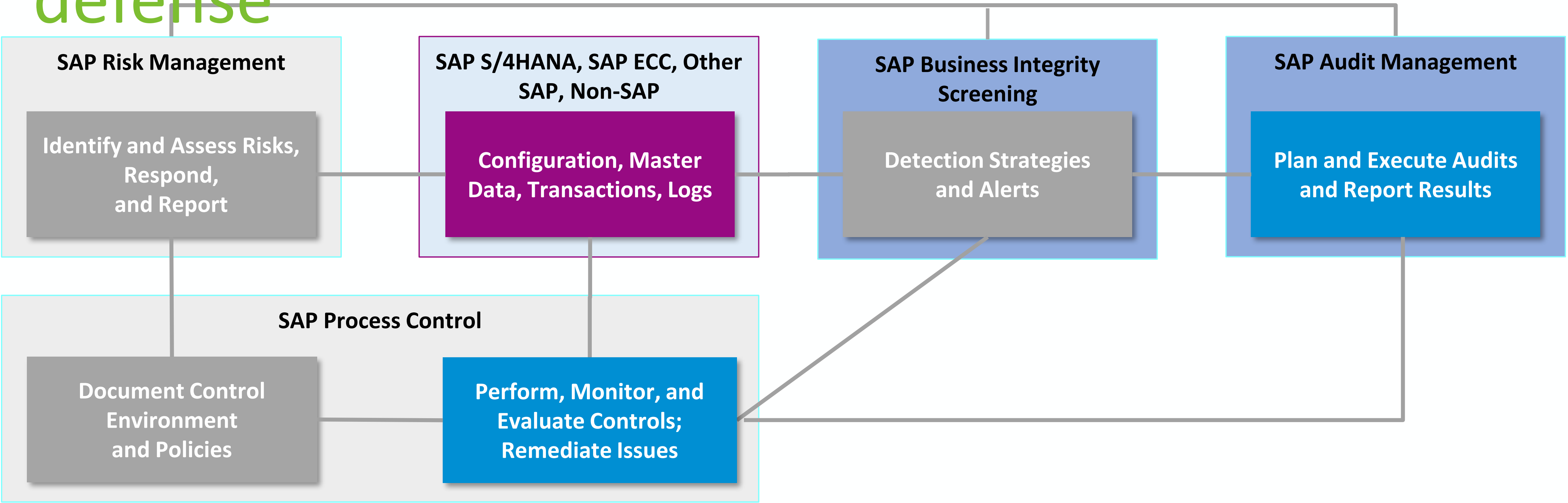
Mitigation

Analysis Date: 04/28/2011

Probability Reduction: 10 %

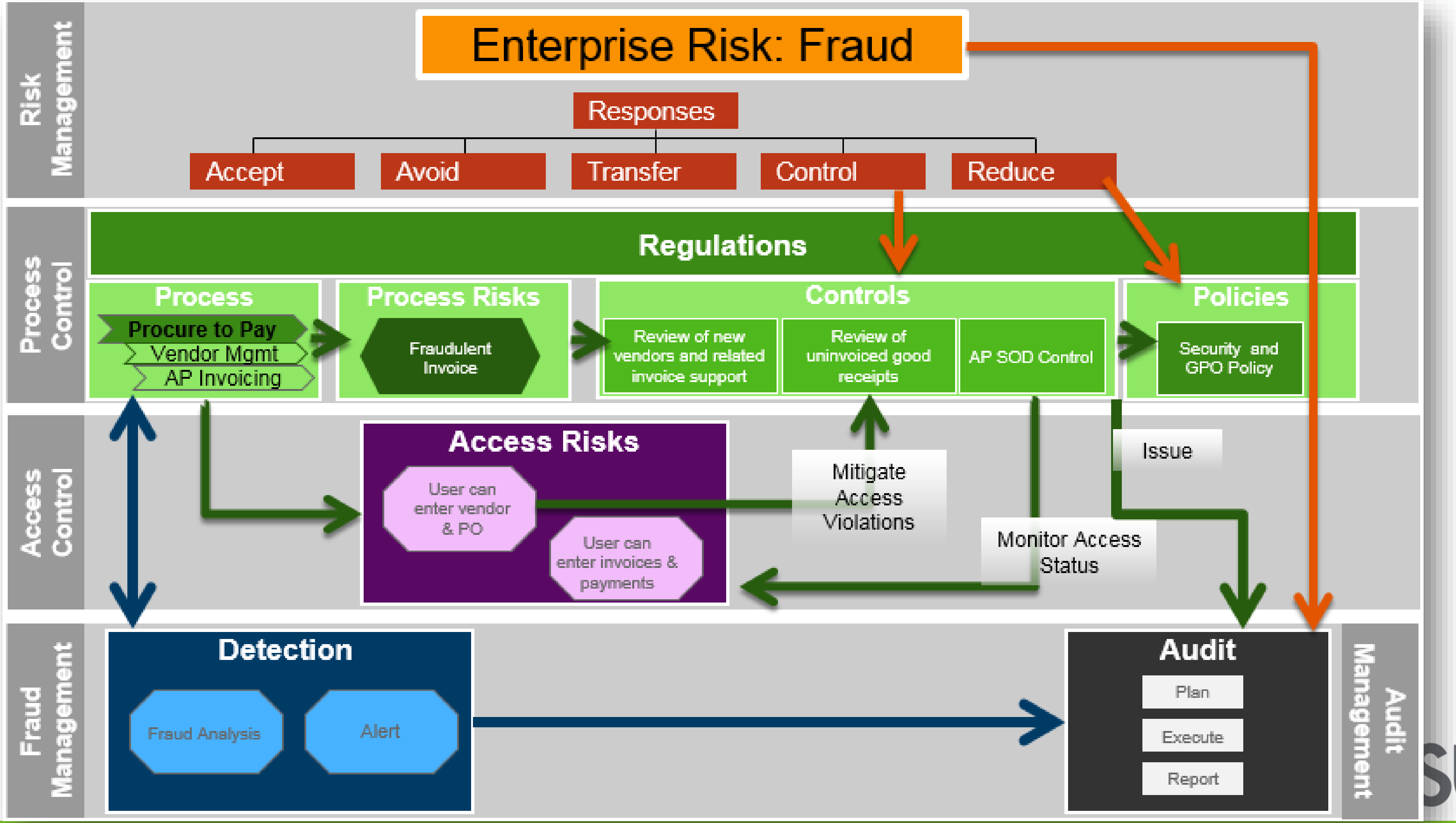
Impact	Impact Category	Reduction	UOM	Total Loss Reduction
Losses due to fraud not covered by insurance	Expenses	500,000.00	Currency	0.00 USD
Late payments to vendors / suppliers	Stakeholders	250,000.00	Working Hour(s)	0.00 USD
Incorrect financial statements	Regulatory	500,000.00	Currency	0.00 USD

Simplified view of integration for three lines of defense


SAP Risk Management
Identify and Assess Risks, Respond, and Report
SAP S/4HANA, SAP ECC, Other SAP, Non-SAP
Configuration, Master Data, Transactions, Logs
SAP Business Integrity Screening
Detection Strategies and Alerts
SAP Audit Management
Plan and Execute Audits and Report Results
SAP Process Control
Document Control Environment and Policies
Perform, Monitor, and Evaluate Controls; Remediate Issues

- Risks and controls are shared to create a consistent enterprise view
- SAP S/4HANA, SAP ECC, Other SAP, Non-SAP data is available for monitoring risk indicators, controls, anomalies, and business partners
- Risks and controls plus test, monitoring, and screening results can be used to streamline audit performance
- Reports to management include comprehensive and consistent information from across the enterprise

Simplified view of integration for three lines of defense



Demo steps

- Overview of Implementation of risk monitoring for SAP Enterprise Threat Detection
- Create risk monitoring rules
- Check Threshold Violation
- Display risk heatmap
- Display NIST requirements
- Show remediation steps

DEMO

Thank you

James Chiu, CPA, CISSP
GRC Solution Owner
James.chiu@sap.com

Anne Marie Colombo, CISSP
Cybersecurity Solution Advisor
anne.marie.colombo@sap.com

THANK YOU