Transforming security and controls with SAP S/4 and peripheral systems

Deepali Filosa, VP Risk and Controls, Booking Holdings Inc
Snigdha Chiduruppa, Director, KPMG LLP

SAPinsider
Las Vegas

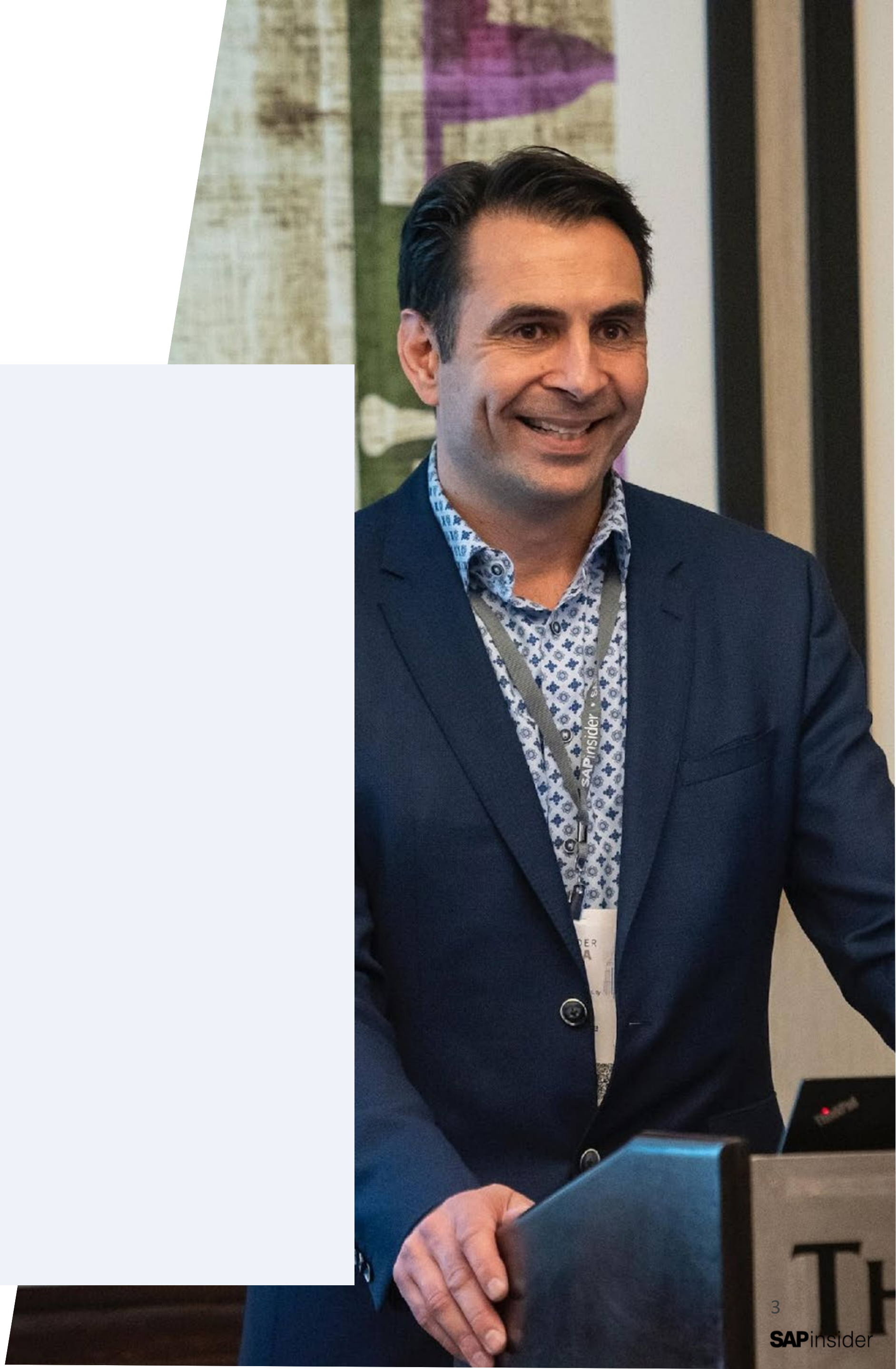
2023

In This Session

Discuss KPMG’s partnership with a Fortune 500 Technology company to integrate controls design into the finance transformation project and how to manage risk through the project phases

What We’ll Cover

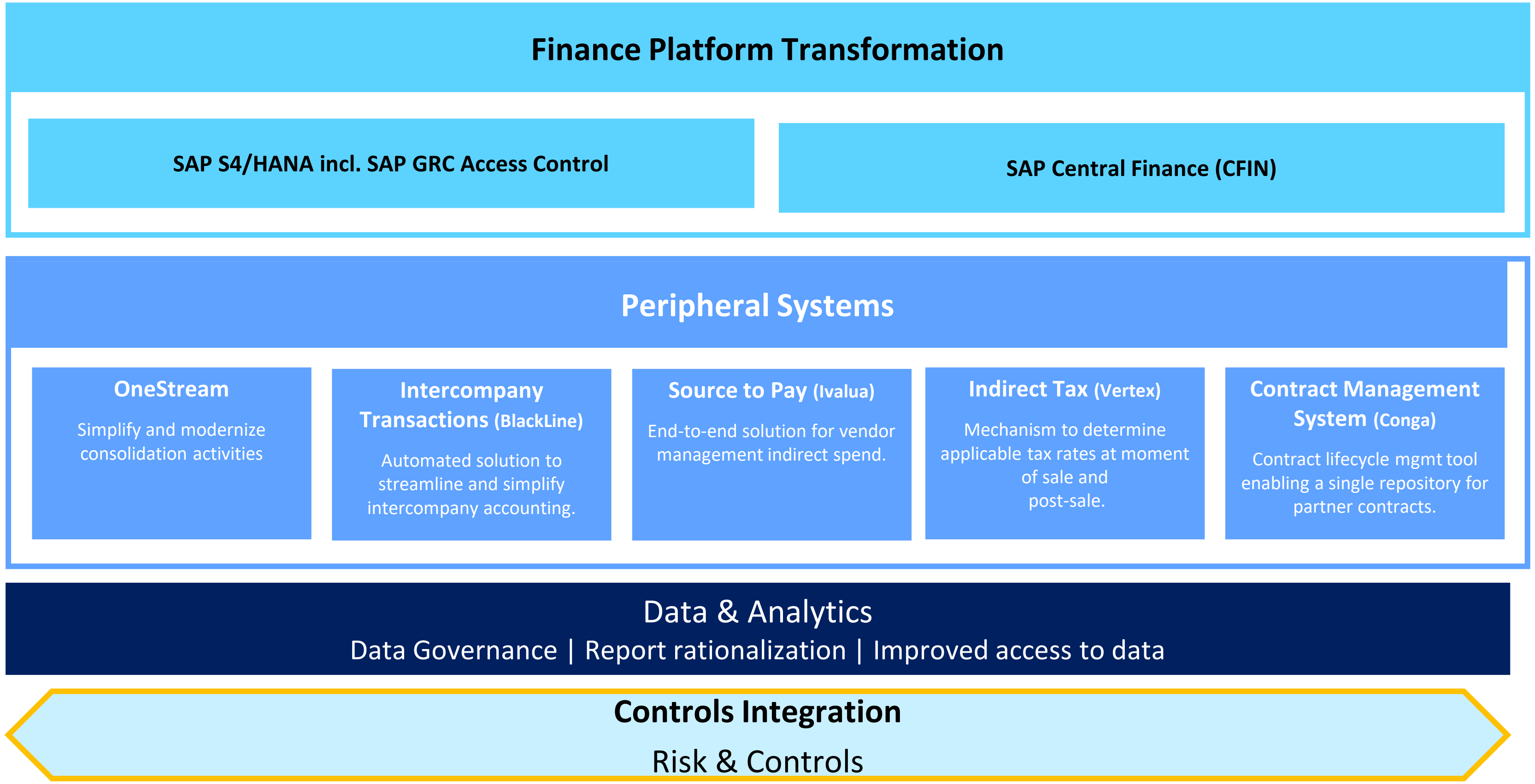
- Overview of finance transformation project
- Controls integration approach by project phase
- Engaging with stakeholders
- Wrap-Up



Overview of finance transformation project

Finance Transformation overview

Create an enterprise wide, global finance solution for all business units through a multi-year, multi-phase transformation.



Finance Platform Transformation

SAP S4/HANA incl. SAP GRC Access Control

SAP Central Finance (CFIN)

Peripheral Systems

OneStream
Simplify and modernize consolidation activities

Intercompany Transactions (BlackLine)
Automated solution to streamline and simplify intercompany accounting.

Source to Pay (Ivalua)
End-to-end solution for vendor management indirect spend.

Indirect Tax (Vertex)
Mechanism to determine applicable tax rates at moment of sale and post-sale.

Contract Management System (Conga)
Contract lifecycle mgmt tool enabling a single repository for partner contracts.

Data & Analytics
Data Governance | Report rationalization | Improved access to data

Controls Integration
Risk & Controls

Security and Controls Integration overview

Key objective is to bring the brands onto a standardized set of business processes using the same technological platform across the company, and ensure processes are compliant and control-conscious upon go-live.

Type of Controls

- ✓ Financial Controls (SOX)
- ✓ Operational
- ✓ Fraud
- ✓ Technology

Guiding Control Principles

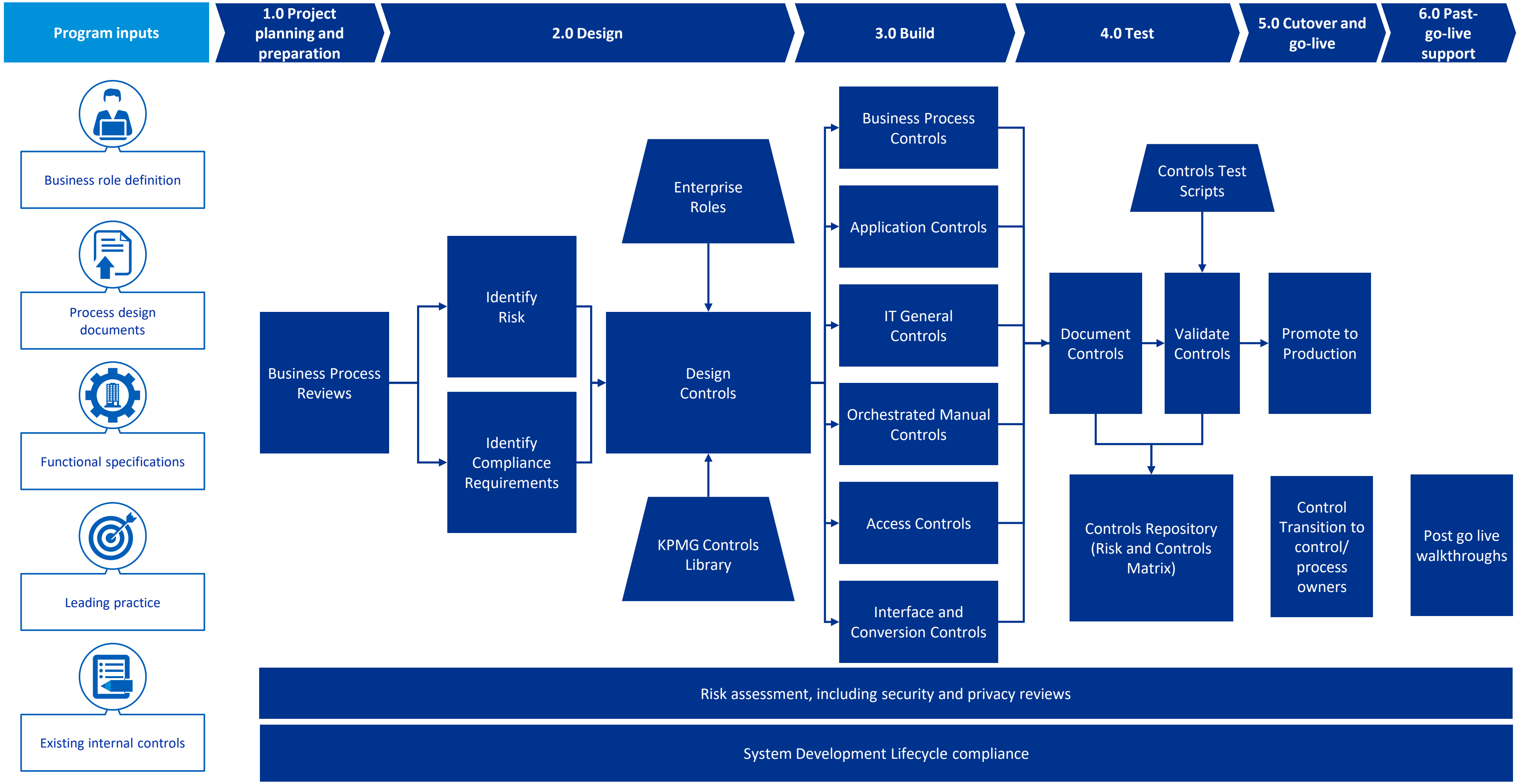
- ✓ Integrate control compliance into each workstream upfront
- ✓ Identify smart controls whenever possible
  - ○ Automated vs. Manual
  - ○ Preventative vs Detective
- ✓ Consider risk and control requirements for the future state end-to-end processes, underlying technology and data flows

Benefits

- ✓ Lower cost of compliance
- ✓ Efficient audits
- ✓ More control reliance
- ✓ Focus on key risks

Controls Integration Approach by project phase

Controls design



Program inputs

1.0 Project planning and preparation

2.0 Design

3.0 Build

4.0 Test

5.0 Cutover and go-live

6.0 Past-go-live support

Business role definition

Process design documents

Functional specifications

Leading practice

Existing internal controls

Business Process Reviews

Identify Risk

Identify Compliance Requirements

Enterprise Roles

Design Controls

KPMG Controls Library

Business Process Controls

Application Controls

IT General Controls

Orchestrated Manual Controls

Access Controls

Interface and Conversion Controls

Controls Test Scripts

Document Controls

Validate Controls

Promote to Production

Controls Repository (Risk and Controls Matrix)

Control Transition to control/ process owners

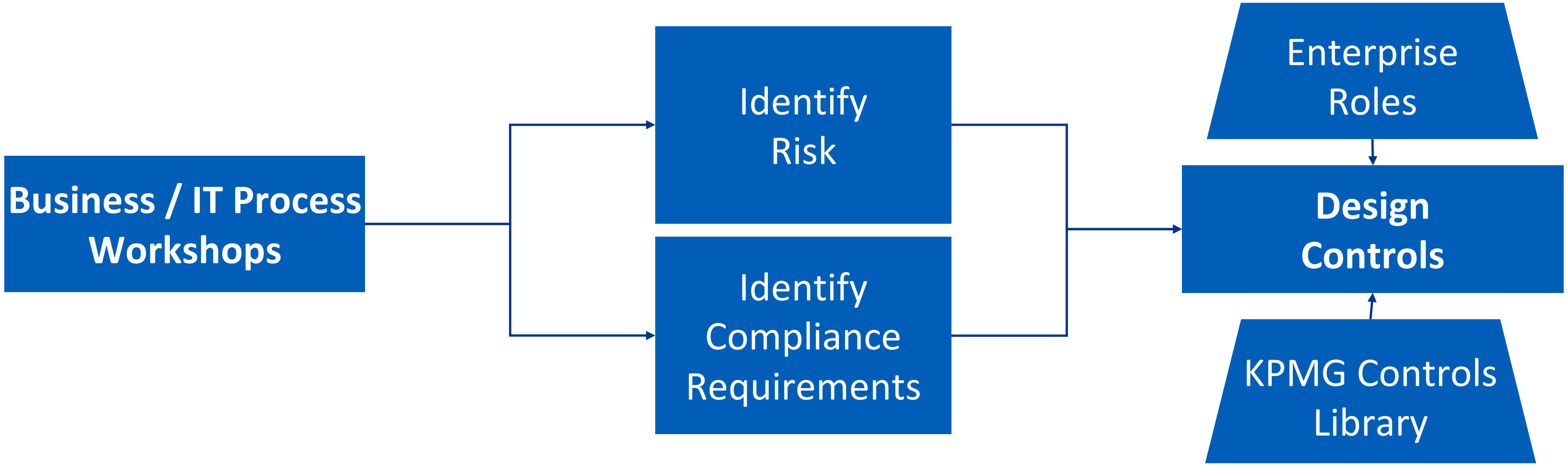
Post go live walkthroughs

Risk assessment, including security and privacy reviews

System Development Lifecycle compliance

Controls consideration early on

Having a ‘risk and controls’ seat at the Design table enabled an improved design of functional, security as well as controls requirements



Always keep the ‘end to end’ process in mind – implementations may be done by system, but the process design spans across multiple technologies and teams

Controls consideration early on

How can the Controls team contribute during Design workshops

Pre workshop

- Consolidated KPMG’s control catalogs and key risks identified within the in-scope processes

During workshop

- Understand proposed future state process / data flow and challenge status quo, encourage automation and use of standard configurable functionality
- Identify key risks within the process (rationalized for the enterprise, and specific to each business unit)
- Design high level control requirements
- Consider interim requirements while in a multi-ERP scenario
- Draft security considerations based on defined process

Post workshop

- Conducted security and controls workshops with process owners, security and the implementer
- Aligned with audit stakeholders and obtained feedback

Segregation of Duties

Security design (including Segregation of Duties – SOD - management) integrated with Control design is essential for a compliant process

- Role design and build was done by Security team with Business input
- SOD and Critical Access ruleset was built by Controls team with Business input
- Compliance requirements can be achieved more efficiently with a combination of security design and control design
- Ruleset build should always consider cross-application and cross-process design

Ruleset build included –

- Understanding of future state process
- Analytical comparison against standard and golden rulesets, including Fiori apps

Transformation projects rarely result in no changes to the process design, it is recommended to not take a 'lift and shift' approach with security and ruleset design

Risk assessment

Establish a risk assessment process to identify, assess, and manage risks related to technologies supporting various project workstreams and their underlying data.

Initiatives

- ✓ Use of new technology
- ✓ Use of existing technology in a new way
- ✓ Make data accessible to other BHI entities

Guiding Principles

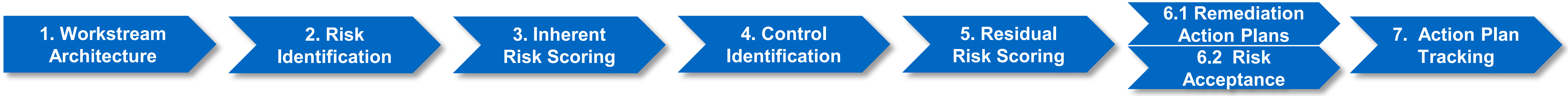
- ✓ Identify risk areas within each workstream and its underlying technology and data flows
- ✓ Determine the likelihood and the impact of each risk
- ✓ Identify the controls associated with the risk to minimize the risk exposure
  - ○ Assess if the if the residual risk is acceptable or if a mitigating action plan is required

Benefits

- ✓ Establish a framework to identify, measure, track, report and escalate risks
- ✓ Identify areas that require additional resources to minimize business disruption
- ✓ Ensure that risks inherent in daily activities are addressed

Risk assessment

High-Level Approach


1. Workstream Architecture

2. Risk Identification

3. Inherent Risk Scoring

4. Control Identification

5. Residual Risk Scoring

6.1 Remediation Action Plans

6.2 Risk Acceptance

7. Action Plan Tracking

1. Understand technology landscape and data for each workstream

2. Risks are identified for each of these workstreams

3. An inherent risk rating is calculated

4. Controls are identified for each risk

5. A residual risk value is assigned based on the inherent risk and control suite

6. Identify risk owner and create a remediation action plan to mitigate risks **or** perform the risk acceptance process

7. If a remediation action plan is created, track actions for completion

Risk Category	Domains
Tech and Product	Change Management, Identity and Access Management, Logging and Monitoring, Technology Incident Management, Data Governance
Business Continuity	Business Process Disruption
Regulatory Compliance	Tax compliance, Product/Regulatory change, Privacy (GDPR)
Supplier Management	Third Party Management
Security	Data Security, Cyber Security

Testing of controls pre-go-live

Automated functionality of designed controls should be tested pre-go-live

Unit testing

Owned by technical team / implementer

End-to-end scenarios are likely to not exist to test controls

System Integration testing

User Acceptance testing

Multiple cycles of System Integration testing by technical team / implementer before moving on to business-led User Acceptance testing

Controls team input –

- Review and update test scenarios and enhance scripts to test the control objective
- Review executed test scripts to confirm control is operating per design
- Roles are tested as part of these cycles – consider Segregation of Duties considerations
- Update control design based on results of testing, if required

Scope

- Automated controls (configuration, workflows) | Interfaces | Reports

Testing should be performed beyond 'happy path' of the process. Can the system withstand/process the various scenarios of transactions?

Transition of controls to business teams

Control ownership should be formally handed over to business pre-go-live, in addition to system training that is required

- Goal is to have controls operating effectively from day 1 post-go-live
- Control owners and control performers may be different from process owners

<table>
<tr><th>Automated controls</th><th>Manual controls</th></tr>
<tr><td>Tested pre-go-live – hence reasonable assurance that they will operate effectively in the Production environment
Include technical teams in transition sessions so they understand expectations of them to support
Analytics-based review of selected configurations</td><td>Conduct transition sessions to describe how the control should be performed
Control SOPs / narratives / job aids are useful in these sessions</td></tr>
<tr><td colspan="2">Ensure control owners and control performers review and acknowledge each control –
- Description | Frequency | Regulation compliance | Evidence to be retained</td></tr>
</table>

Do not underestimate the effort and impact of this step – this is critical to avoiding control deficiencies post-go-live

Training and Organizational Change Management

Program-led functional training provided to end users to equip them to operate within the system following the future state process

While controls transition requires dedicated sessions, alignment with Training / OCM team is essential -

- Review of job aids to reconcile with control design
- Validation of access/ t-codes / Fiori apps used to perform tasks that drive controls (consider reports being used in controls)

Control operation should be aligned with the functional training

Data validation

Data validation for completeness and accuracy is critical to the successful operation using the newly implemented systems

Data cleansing	Data Extraction	Data Construction
Document the guidelines followed for cleansing of data in the source system. (eg. deletion of vendors with no bank information)	Review and confirm (by authorized user) that the data extracted from the source system is complete and accurate	Review and approve (by authorized user) the new data records being generated in the Construction step.

Data Transform	Data Load
The Data Definition document should describe the mapping of the old fields to the new; and include how new fields (if any) are being determined. The validated pre-load file should be prevented from being edited once the validation exercise is complete.	Validate data loaded to target system against the data from the source system. If there are differences, these should be investigated.

The accountability for validating Completeness and Accuracy should be with the business teams (data owners)

Go/No-go decision

Controls Integration team should have a seat at the table during this decision

Have a prepared list of open items

- Tasks to be completed prior to go-live (before freeze, during freeze)
- Tasks to be completed after go live
- Risk mitigation / acceptance if any of these tasks are unable to be performed

Communicate the open items with stakeholders sufficiently prior to the go/no-go decision

Frequent communication with stakeholders is key

Post-go-live – process and control walkthrough

This provides management to assess the process and controls after hypercare and update control framework

- Management led activity to identify where design may not match execution
- Also helps in identifying potential audit issues so remediation / mitigation can be performed
- Determine if the open items under risk acceptances / risk mitigation pre-go-live have been addressed
- Update control framework as required

Timing this activity appropriately is crucial – between hypercare and audit cycles, such that there is still time to remediate issues identified

Engaging with stakeholders

Engaging with stakeholders

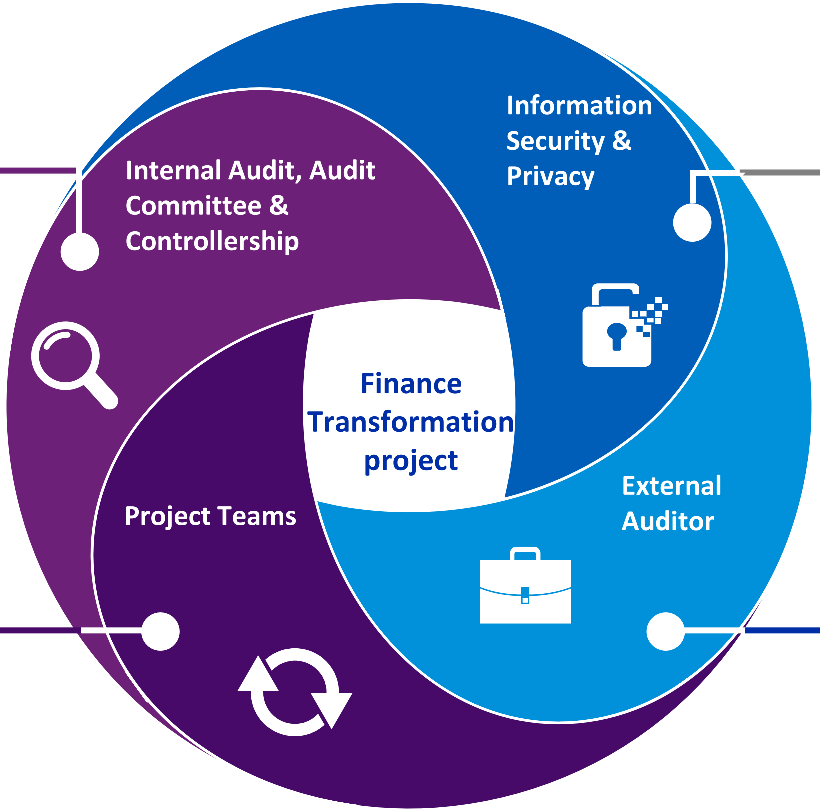
With multiple teams working towards the same end-goal, it is key to stay connected throughout the project lifecycle.

We as KPMG:

- Engage Audit and Risk Stakeholders regularly to align with compliance standards and requirements
- Provide visibility into changes made to compliance documents, RCMs, flows
- Support due diligence activities to validate effectiveness of controls implemented

We as KPMG:

- Collaborate with deployment teams, including business stakeholders, System Implementer, and control owners, to validate business process design and controls
- Provide real-time insights into the effectiveness of the security and control design and support implementation throughout project lifecycle


Internal Audit, Audit Committee & Controllership
Information Security & Privacy
Finance Transformation project
Project Teams
External Auditor

We as KPMG:

- Periodically assess IT Controls, including cyber, cloud and third party risk considerations
- Provide insights into security and role design, SOD and critical access, data governance, and other relevant IT risks
- Assess segregation of duties and sensitive access and build GRC rule set

We as KPMG:

- Engage with External Auditor proactively to align with compliance standards and requirements
- Communicate changes to the existing control framework and interim controls transparently
- Assess and communicate impact of changes on SOX compliance and Financial Statement risks

Engaging with the Audit stakeholders

Bringing the auditors along the controls journey has been key in minimizing surprises for both management and the audit teams (internal and external audit)

In collaboration with the business teams and project teams, pre-go-live walkthroughs of the following areas were held –

- Business and IT processes and proposed control design
- Segregation of duties and Sensitive access ruleset development
- Testing strategy and plan
- Data validation strategy and plan
- Cutover considerations
- Functional training and controls transition

Controls team is responsible for periodic touchpoints with the Audit teams to provide them with an update on the project – Opportunity to obtain feedback and course-correct if needed.

Engaging with the Audit stakeholders

Bringing the auditors along the controls journey has been key in minimizing surprises for both management and the audit teams (internal and external audit)

- Feedback from audit teams was evaluated with the project team
- Feedback not implemented was documented with alternate mitigation factors or risk acceptance
- Timing of audit feedback is key – should be obtained such that it is feasible to act upon it
- Controls team plays the liaison between the business / project teams and audit teams, but ownership or project areas should remain with management

Ask your auditors for key areas of focus / concern for them

Audit areas of focus

Program Governance

- Project risk assessment and organizational alignment
- Adherence to project milestones
- Project charter, processes and procedures
- Go-Live Healthcheck

General IT Controls

- Review changes to the IT general controls
- Perform pre-implementation SAP Basis and GITC review
- Fiori Front-End Server and ancillary systems review

Access and Segregation of Duties

- Security and role design strategy including Fiori
- Assess SoD ruleset design
- Assess users and roles configuration against the design

Data Conversion and Migration

- Conversion and migration strategy
- Accuracy and completeness of data mapping and conversion and supporting documentation

Cloud Security

- Evaluate cloud security
- Assess relevant user entity controls design

Business Process Controls

- Review changes to the Risk and Control Matrices
- Assess changes to reports used for performing manual controls
- Testing automated controls configuration

Testing

- Assess testing strategy and approach for User Acceptance Testing (UAT), SIT, Integration, Unit, Regression, Change Management
- Review testing results and defect management

Interfaces

- Assess the interfaces strategy including UAT
- Test accuracy and completeness of the data transfer

Cut-Over and Hypercare

- Assess pre-go live and cut-over procedures
- Test hypercare controls

Cyber Security and Privacy

- Evaluate cyber security strategy
- Assess key cyber security configurations
- Review privacy considerations against system design

Control and compliance documentation

Controls and compliance package to help maintain compliance post go live

Risk and Control Matrix (Business and IT) (AuditBoard ready)	SOD ruleset	Controls mapped to pre-go-live test scripts
Process flow and process narrative	Old vs. new mapping of controls	Auditor feedback addressed
SOX impact assessment memo	SOC report mapping	SDLC checklist (incl Data Conversion if relevant)
Pre-go-live control walkthroughs and training	Go-live criteria (incl Open items / risk mitigation / risk acceptance)	Post-go-live control walkthroughs

Wrap Up

Ongoing compliance results have included -

- Increase in control automation
  - Entirely manual processes have seen up to 75% increase in control automation
  - Processes transformed from ECC to S/4 with some automation already – between 10 – 50% increase in control automation
- A more standardized control framework that is tailored to a process designed for all business units
- SDLC compliance requirements being adhered to through the project phases
- More timely identification of potential issues by management enabling remediation and containment of the issue

Where to Find More Information

1.Make a smooth transition to SAP S/4 HANA
2. Cross application security and controls
3. The value of controls integration
4. Energizing risk and compliance on your S/4 journey

Key Points to Take Home

- Design controls with the end-to-end process in mind
- Control testing is key prior to going live
- Controls and security must be integrate for a successful outcome
- Invest the effort in control training/transition
- Controls team does not own the controls, the Business team does.

Thank you! Any Questions?

Speakers

Deepali Filosa - https://www.linkedin.com/in/deepalifilosa/

Snigdha Chiduruppa -

https://www.linkedin.com/in/snigdha-chiduruppa-3ab30067/

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.