Governance Risk and Compliance
Practitioners perspective

A case study on SAP GRC AC
BOSCH - GRC

About
- BOSCH

Architecture
- IT Architecture
- SAP Architecture

GRC @ BOSCH
- AIM
- GRC Program Management
**COSO - Internal Control Framework**

**Objectives of Internal Control**
- Safeguard of Assets
- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

**COSO Cube: Components of Internal Control**
- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring Activities

**COSO Internal Control framework embedded in Business Process & Performance Management**

*Business Performance*
- Control Environment
- Information & Communication
- Strategic
- Control Activities
- Tactical
- Risk Assessment
- Operational
- Monitoring

*Activities*
- Objectives: KPI
- Activities: Compliance

*Business Model*
- Business Model: External Environment
Internal Control Framework: Through the Looking Glass

Authorization Issues
- Lack of Controls on Stand Alone systems
- Controls Not in place
- Processes not Well Laid
- Inadequate Reporting

Failures Modes

Internal Control System
- Entity level Controls
- Activity level Controls
- IT General Controls

Process Controls

Authorization Controls

Solution
BOSCH - GRC

What is in CXO’s mind?

- What are the top risks and opportunities?
- What is the status of compliance requirements?
- Does excessive access introduce opportunity for fraud and errors?
- Are controls in place and shared across your organization?
- Are controls effective?
- Are risk responses ready and effective?

Change in External Environment

- Accounting Standards
- Global Trade Practices

Shift in Regulatory Requirements
- SOX
- Companies Bill, 2012
- Clause 49
- Amendments in Statutes

Global Business Models
- Complex & Dynamic

Inside a CXO’s mind!!
What is in CXO's mind?

- What are the top risks and opportunities?
- What is the status of compliance requirements?
- Does excessive access introduce opportunity for fraud and errors?
- Are controls in place and shared across your organization?
- Are controls effective?
- Are risk responses ready and effective?

Shift in Regulatory Requirements
- SOX
- Companies Bill, 2012
- Clause 49
- Amendments in Statutes

Change in External Environment
- Accounting Standards
- Global Trade Practices

Global Business Models
- Complex & Dynamic

ERM

Compliance Engine

AIM

Robust Internal Audit
Manage compliance

What is in CXO's mind?

What is the way forward???
The 3 Challenges in Compliance

**Availability**
- Right Information at the Right Time

**Scalability**
- Add new Business units / divisions / levels
- Append Regulation changes / Add new requirements

**Coverage**
- Adequate coverage of relevant regulatory requirements
SAP in BOSCH

- 26 GB’s
- 140 Countries
- 285 Manufacturing sites
- 700 + Sales offices
- 1,93,000 SAP Licenses
- 1200 SAP Instances
- 3000 + Job Functions
- 2000+ IT Applications/9000 SAP Z Apps
- 08 + SAP Vertical Templates

Bosch runs its ‘Global Business leadership movement’ on SAP
**BOSCH - GRC**

**Policy, Guidelines, Directives**
- Master Data
- Chart of Accounts
- Central Authorization Concept
- Uniform Business division Process
- Industry Based Templates
- Common Processes for Industry Verticals

**Template based Role Implementation**
- SPOC for New / Changes to Process / Configurations / Developments
- Single Process Owner / Module Owner hierarchy
- Continuous Process and Application Innovation and Development structure
- Common Ruleset, Organization Structure, Business Process and Controls, Risk Hierarchy

**3 Tier Classification Of Critical authorizations**
- Routine SoD checks for Roles and Users
- Master Data Derivation from Central MD Systems
- Application Configuration, Process Documentation, Systems Audit

**Corporate Governance (non-ERP)**

**Automation Capability**

**IT VIEW**
- ERP
- Non-ERP
- ERP
- Non-ERP
Manage and Monitor Compliance requirements

- Evaluation of controls (via Test plans, Surveys, Assessments and CCM Methodology – Continuous Control Monitoring)
- Controls and testing of controls can be Manual/ Semi-Automated/ Automated
- Schedule plans for any organization level
- Trigger alerts, reminders and notifications through customized workflows

Identify and rectify the non-conformances

- Use CAPA (Corrective Action Preventive Action) for the issues raised
- Test and monitor the rectified issues

Compliance Engine*

- Comprehensive report for evaluations and assessments including Exception Reporting
- Better insight into Compliance profile for Confident Sign-off

*Compliance Engine is an RBEI add-on (delivered through SAP GRC 10.0 : Process Control and ECC)
SAP GRC Access Control 10.0

**Prevent and Sustain SoD violations**
- Access Risk Analysis
  - Identify, analyze and resolve all SoD and audit issues related to regulatory compliance. Provides Preventive, Detective and Mitigation Controls

**SAP GRC 10.0 Access Control**

**Get Clean Stay Clean Stay in Control**
- Business Role Management
  - Provides a single enterprise role repository for role design, testing and maintenance to enforce standardization and SoD compliance
- Access Request Management
  - End-to-end access provisioning approval process by combining roles and permissions with workflow.
- Emergency Access Management
  - Systematic handling of emergency situations concurrently managing the risk for the special access
Project AIM

**AIM = Access and Identity Management**

Management of authorizations for IT-applications, concentration to risky processes and data worth to be protected.
Why Project AIM

➢ Risks for the Bosch Group
   • Cash outflow (unjustified outflow of funds/goods)
     e.g. An associate in the human resources department managed to fraudulently receive a second salary by setting up a dataset for a fictitious employee using his own account details.

➢ Know-how drain
   e.g. Due to the illegal disclosure of development plans for a Bosch global product innovation a third party manufacturer pirated products causing a loss of competitive advantage for Bosch

➢ Disruption to processes as well as compliance and legal risks
   e.g. An associate obtained access to sensitive data about his colleagues due to a lack of suitable authorization controls.
Project – AIM - Components

BOSCH - GRC

Central Directive AIM
- IT role development
- Approval workflow
- Controls

Requirements for IT role development
Definition of workflows
Criteria critical authorizations
Requirements for controls

Information for risk assessment

APOLLO
- IT role meta data
- Implementation of IT role

AIM workflow
- Assignment of IT role to user
- User authorizations

RB-AIS
- Approvals

GRC 10.0 - BRM
AIM – Single Unified Access across Bosch

Through AIM we manage
• 2,000,000 SAP Licenses,
• 2,000,000 Derived Roles,
• 2000 Role templates,
• 3000 Job Functions.

.........Across 285 locations/26 + BU’s
GRC @ BOSCH

- IT-role development workbench based on SAP GRC AC 10.0
- Available for SAP- & non-SAP-products
- Central IT & SAP role catalogue
- Workflow features for
  - Creation, change and localization of IT & SAP roles
  - Change of role-related data
- Automated criticality check with SoD Analysis before delivery
- Data exchange with AIM-Workflow on role related data
- Supports implementation of authorization concepts

KEY FEATURES

- Search Functionality: Possible to search within the IT-role catalogue using different criteria as
  - Landscape
  - Process
  - Subprocess
  - Transaction Code
  - ...

- Reports: Different Reports are available to get information about the authorization concept as
  - List Action in Roles
  - Master to Derived Role Relationship
  - Single to Composite Role Relationship
  - Role Library (Dash Board)
Critical Achievements - AIM

1. Availability of Customizable Rule-set
2. Organization framework aligning to the Governance & Compliance
3. Adaptable process/module wise SAP roles
4. HR Security centrally managed through internal policies
5. Customized Web based tutorials and assessments for stakeholders
Critical Achievements - AIM

6. Central Methodology to implement across multiple Business & Geography

7. Cross System SoD analysis

8. Instant reporting of the users violation available in different SAP systems

9. Migration from non standard tools to GRC –BRM & CUP/IdM

10. Systematic review & reporting of the Internal controls
AIM – Benefits Realized

- Reduction in time to get new users on board with over 92% of requests being automated
- Availability of comprehensive SoD Rule sets in central library and hence 0% SoD Violation
- Compliance with IT Governance Standards of US & Europe
- Workflow approval and risk analysis simulation built into role management and user provisioning
- Improved reporting for compliance managers, top-level management, and external stakeholders/auditors
- Mitigation Risk responses put in place and monitored for effectiveness over time
- Identify and manage risks to the business for inputs to audit projects
Few Tips for GRC Initiative Success!

- Create integrated GRC dept. structure*
- Get Senior Management involved
- Prepare & execute annual GRC plan
- Integrate controls into application configuration
- Continuously monitor control environment
- Tighten controls on information security
- Focus on providing assurance & value addition to CXOs
Critical Success factors - AIM

• **Organization framework aligning to the Governance & Compliance**
  – Setup of the full fledged authorization concept involving many stakeholders like, Master of Data, Process Experts, Key users, Data Security Partners etc.
  – Setup of the well defined processes with effective approval protocols for the Role management, User provisioning & Risk mitigation.

• **Portable process based module wise SAP roles template**
  – Adaptable to heterogeneous businesses.
  – Readily available SAP template roles from all the SAP modules which can be used directly for any business with minimum customizing.

• **HR core security managed thru the template architecture centrally**
  – Unlike the stand alone systems for managing HR core, it is executed thru the central HR core template with limited localization allowed to the Business units catered thru a single SAP system.

• **Customized Web based trainings for all the relevant areas**
  – Web based trainings are prepared by the professionals who has the understanding of the processes. This is available different levels followed by the evaluation.
Critical Success factors - AIM

• **Methodology to implement Access controls across multiple Business & Geography**
  – Master Business Access control template is defined which could fit any line of business with local delta developments required. E.g. CIN, IFRS etc.

• **Cross System SoD analysis**
  – Since Bosch users have access to many SAP systems, cross system check is mandatory. Currently this is executed as a detective method with defined measures. The process of making it as preventive is on thru GRC.

• **Instant reporting of the users available in different SAP systems**
  – Customized report fetching the user & system matrix at any point of time. Since Bosch has more than 90 SAP instances, this would be the key factor during the User exit process thru which we are compliant with the audit standards.

• **Migration from non standard tools to GRC –BRM & CUP/IdM**
  – Strength in analysing and migrating / replicating the workflow definitions from the legacy tool or manual archival into GRC role management & User management tools configuration.

• **Systematic review & reporting of the Internal controls**
  – Redundant activities like SAP Licence management, Quarterly user access review etc will benefit the organization for Benchmarking and also to stay Compliant with audits.
Thank You