



INFO:

The purpose of this infographic is to outline a simple step by step approach to implementing effective risk management within your organisation. According to ISO 31000 risk management refers to a "coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives."

BUSINESS OBJECTIVES / OUTCOMES

- More effective strategic and operational planning: alignment of objectives and risks across the organisation
- Greater confidence in decision making: proactive achievement of operational and strategic objectives
- Early warning system (visibility and reporting of significant risks): Avoid surprises
- Proactive management of risk and opportunity: long-term sustainability
- Cost effective internal controls and control strategy: systematic and consistent approach
- Evidence of a structured / formalised approach in decision making: resulting in confidence and business resilience
- Regulatory compliance: license to trade and director protection
- Greater stakeholder confidence: Reputation management, & capability

ALIGNING PEOPLE, PROCESSES AND SYSTEMS FOR EFFECTIVE RISK MANAGEMENT

PEOPLE



Buy-in, tone from the top, commitment to effective GRC

PROCESSES



Best practice GRC process (i.e. COSO, ISO31000)

SYSTEMS



User-friendly, non-intrusive, accurate and real time reporting, better decision making

STEPS



1 TONE FROM THE TOP AND BUY-IN FOR EFFECTIVE GOVERNANCE PROCESSES

- Ethical and effective leadership promoting good governance, sustainable performance and value-creation for the organisation.
- Change management and education
- Establish risk management roles and responsibilities: board, exco, risk / audit committee, risk officer, business unit risk champions, risk owners, system champion

PREPARATION

2 RISK MANAGEMENT POLICY AND FRAMEWORK

- Map your risk management policy to the COSO / ISO31000 framework
- Document your risk management plan
- Risk identification and assessment: existing registers, interviews, workshops, surveys, past experience, competitor analysis, market trends, research, scenarios etc.

3 PROJECT MOBILISATION

- Project charter
- Project scope
- Confirm IT minimum requirements
- Project plan
- Key stakeholders (project sponsor, project manager, system champion, risk champion/s)

PROJECT MANAGEMENT

4 SYSTEM INSTALLATION

- Minimum IT requirements verification and sign-off by Client IT
- Installation of your configured BarnOwl SQL server database
- Installation and testing of 'rich' client and web-based Lite client with Active Directory synchronisation
- Installation of offline and testing (where applicable)

TECHNICAL INSTALLATION

5 BUSINESS DISCOVERY AND INFORMATION GATHERING

- Review the risk management policy, methodology and framework (based on COSO / ISO31000)
- Risk parameters: risk ratings (impact and likelihood), Control ratings (adequacy and effectiveness), tolerance, appetite, risk model, risk categories / sub categories
- Organisational structure > weighting / impact thresholds, permissions (users and groups)
- Objectives>Risks>Contributing factors>Controls>KPIs, KRIs, KCIs (targets and thresholds)> Action Plans
- Incident types with relevant attributes (loss events, forensic, tip offs, health & safety, gifts, conflict of interest etc.)
- Risk reports

BUSINESS DISCOVERY AND CONFIGURATION

6 SYSTEM CONFIGURATION

- Configure risk parameters and risk model
- Setup organisational structure (hierarchical org structure by strategic, business and business activity unit)
- Setup process structure
- Setup / import users and configure unit permissions (group / user roles)

7 REPORT IDENTIFICATION AND CONFIGURATION

- Select standard reports from the system
- Configure additional reports with system report builder
- Business Intelligence dashboard design (if applicable)

8 DATA MIGRATION

- Client to format existing Excel registers into BarnOwl import format
- Import existing risk registers from Excel into risk library or organisational structure directly
- Import existing incident registers from Excel into the system

DATA MIGRATION

9 SUPER USER TRAINING

- System admin training (maintenance of parameters and permissions, risk library, organisational structure)
- System champion training (Objective and Risk identification>Risk assessment> Control identification and assessment, KRI identification >Action plans> Reporting> Monitoring)
- Risk management advanced training (advanced features, setup of voting templates, report design, aggregated reporting etc.)

TRAINING

10 USER TRAINING

- Business risk champion training (Risk register maintenance, action plans, unit reporting)
- General users (owners) training (complete action plans online, risk & control self-assessment voting and complete checklists online)

11 USER ACCEPTANCE TESTING (UAT)

- Super user acceptance testing with limited data set (full system functionality)
- Super user acceptance testing with full data set (full system functionality)
- User acceptance testing for risk champions (basic system functionality)
- User acceptance testing for general users (owners) (limited system functionality such as action plans, voting, checklists)

TECHNICAL INSTALLATION

12 GO LIVE AND SIGN OFF

- Roll out
- Ongoing monitoring
- Ongoing change management and communication

GO LIVE

SYSTEM OBJECTIVES



EASE OF USE



SAVE TIME



FLEXIBLE



ACCESSIBLE



REAL TIME



INTEGRITY OF DATA

- GRC reporting at the click of a button: simple, aggregated, trends, business intelligence
- Embed GRC and facilitate a culture of risk and control within the organisation
- Drive accountability and responsibility for GRC
- Proactive monitoring of your risk, compliance and audit universe
- Early warning monitoring of the achievement of your strategy