www.pwc.be/erp

Governance, risk & compliance technology for organisations running SAP

Trends, analysis & insights on the Belgian market

pwc

Trends, analysis & insights on the Belgian market

- Introduction and context
- Introduction to GRC technology
- Belgian survey participants
- Key conclusions

Introduction and context

- Our SAP practice aims to help our clients implement, control and improve their ERP solutions
- PwC conducted a global study on GRC technology. Our Belgian firm complemented this with a survey of key SAP users in Belgium
- The Belgian survey contains insight from 50 companies that run SAP ERP systems
- This document shows how our SAP clients are managing risk, compliance and controls through GRC technology

50 companies

8 industries

Global study – Belgian survey

Introduction to GRC technology
Transforming the security & control environment

During the 1990's and early 2000's organisations delivered large scale business transformation through moving towards single source ERP systems

Over the next years organisations will drive significant improvement in security and controls by pulling together all security, control and compliance activity into one, dynamic and robust technology system

...reducing the cost of compliance and driving insight, visibility and accountability around risk, security, and controls throughout the organisation

Introduction to GRC technology
Key drivers behind increased investment in GRC

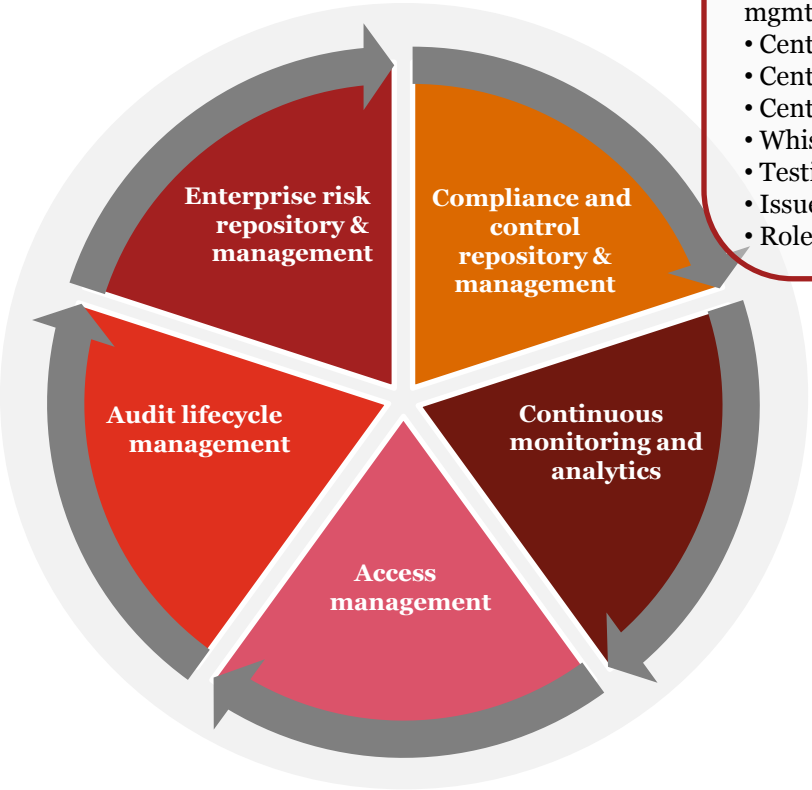
- Increased regulatory requirements - Demand for more assurance, subject to pressure to reduce cost
- Emergence of business control functions - Demand for technology to provide support
- Global shared service and control centres - Transparency and accountability for controls
- Business transformation & SAP consolidation programme - Protecting investment
- Increased maturity and consolidation in GRC technologies - Enhanced quality and capability
- Demand for better management information - Appetite for visibility and insight

Boards and senior management are demanding greater insight & visibility into the effectiveness of controls and compliance across the organisation

…GRC technology is seen as a key enabler

Introduction to GRC technology

Key components

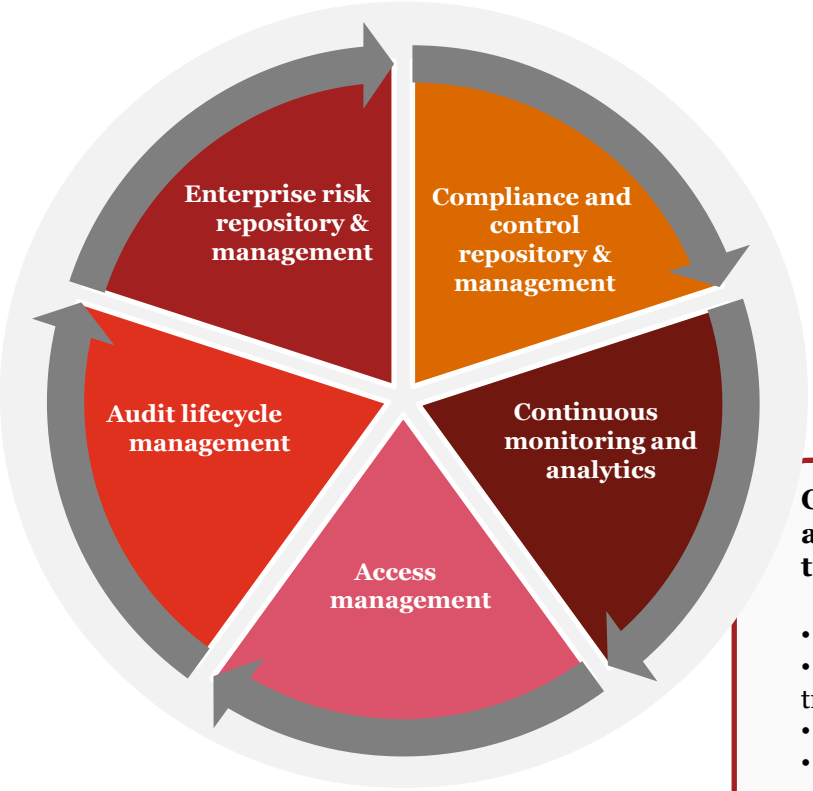


Document and manage the company's overall compliance and control framework(s), which includes:

- Support multiple compliance framework(s)
- Centralised organisation structure and hierarchy
- Policy, process and procedure definition and mgmt.
- Centralised control repository
- Centralised test and assessment libraries
- Centralised planning
- Whistleblower mechanisms (Ad-hoc issue Mgmt)
- Testing evidence repository
- Issue and remediation management
- Role-based access controls and security

Introduction to GRC technology

Key components

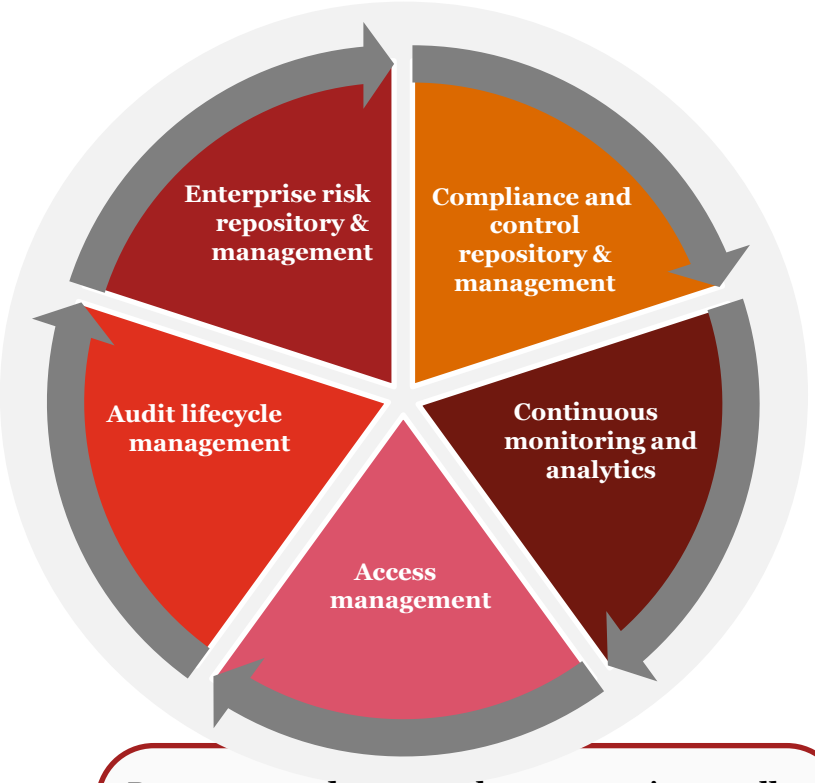


Continuous monitoring and analysis of controls, data and transactions, which includes:

- Continuous control monitoring
- Continuous data monitoring (master & transactional)
- Continuous risk monitoring
- Automated business rule framework
- Exception-based monitoring
- Data analytics capabilities
- Exception and issue-tracking platform
- Role-based access controls and Security

Introduction to GRC technology

Key components

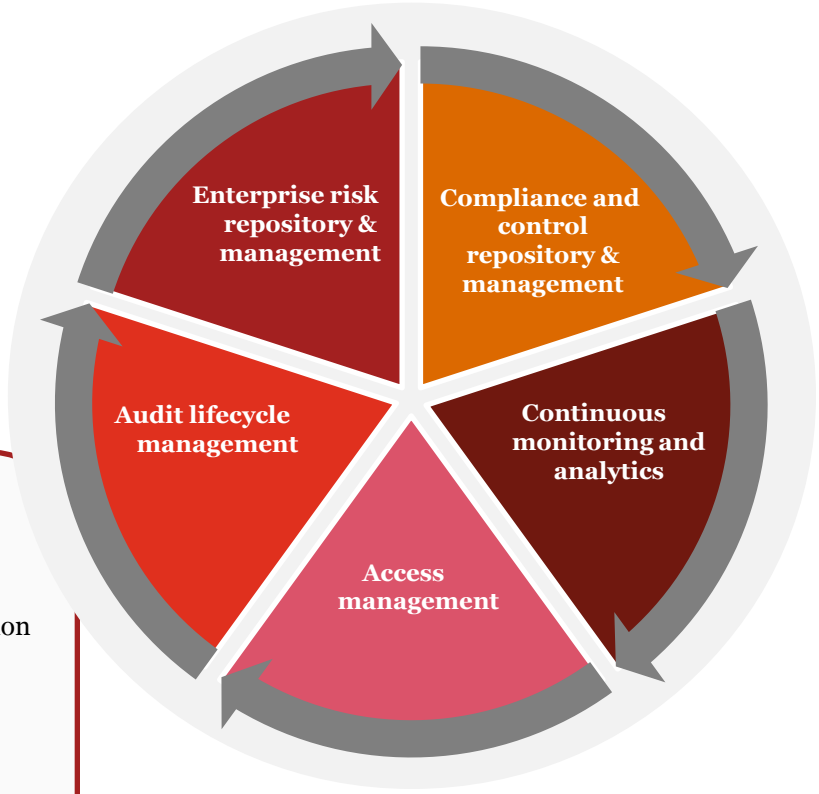


Document and manage the company's overall SAP security framework, which includes:

- Sensitive access risks and controls
- Segregation of Duties risks and controls
- Continuous access monitoring
- Super-user access Mgmt
- Security in user provisioning & Role management
- Role-based access controls and Security

Introduction to GRC technology

Key components



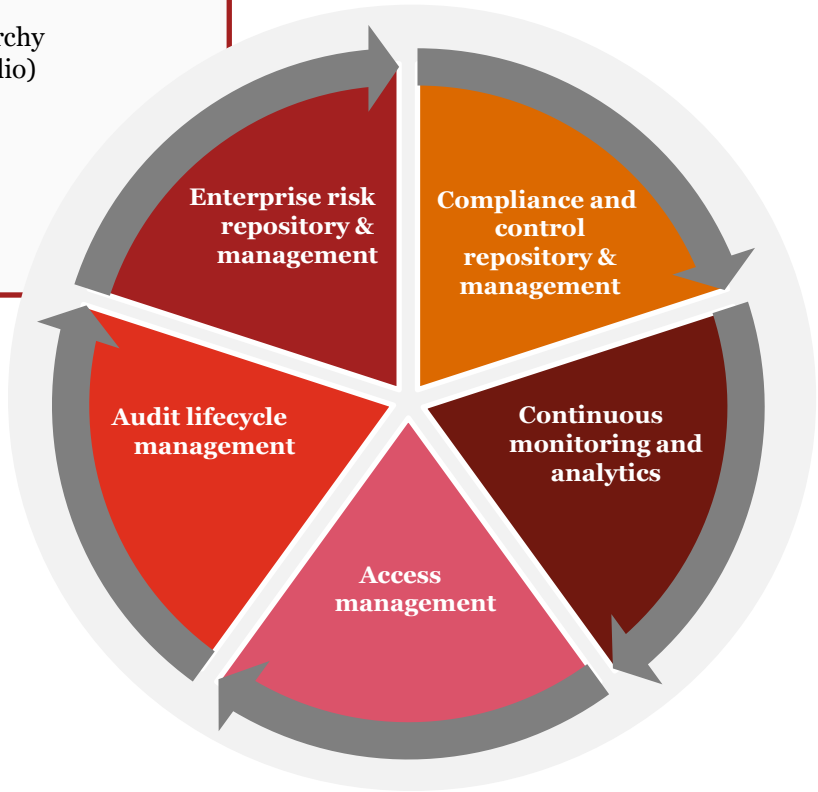
End-to-end management of the audit lifecycle, which includes:

- Audit scoping & scheduling
- Organise work papers & documentation
- Support all types of audits, including internal audits, operational audits, IT audits, quality audits, etc.
- Manage audit work plans
- Risk Management monitoring efforts including but not limited to independent reviews, RCSAs, and surveys to oversee and monitor compliance and risk management activities
- Role-based access controls and Security

Introduction to GRC technology
Key components

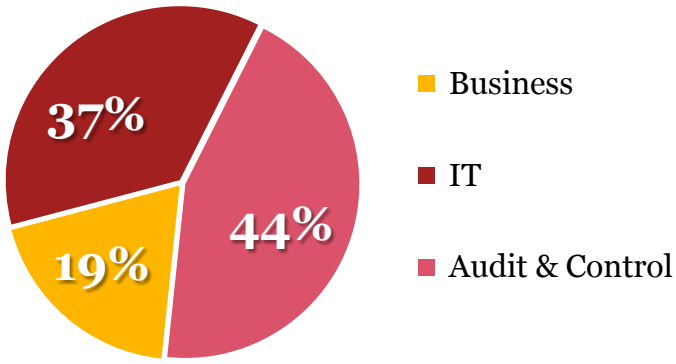
Document and manage the company's overall enterprise risk framework(s), which includes:

- Risk Framework (Risk Profile, Risk Appetite, Risk Tolerances, Strategy, Objectives, etc.)
- Centralised organisation structure and hierarchy
- Risk Repository & Classification (Risk portfolio)
- Risk assessment processes
- Risk Correlation & Simulation
- Response plans library & Incident Mgmt
- Loss metrics and event collection Mgmt
- Consolidated risk Heatmap & risk exposure
- Role-based access controls and Security

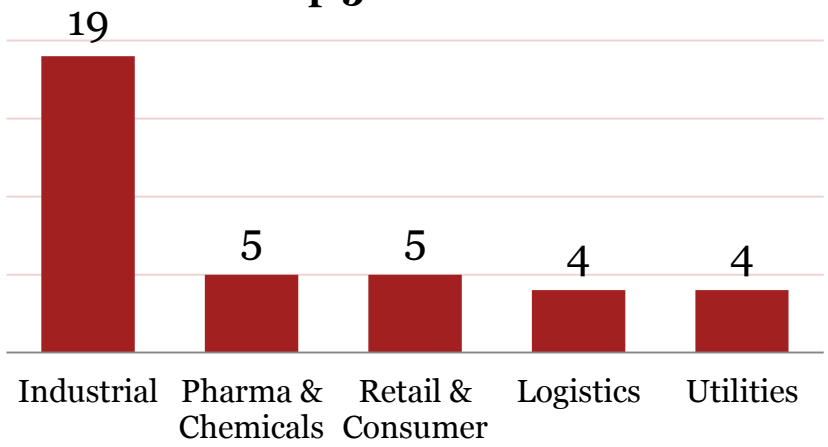


Belgian survey participants

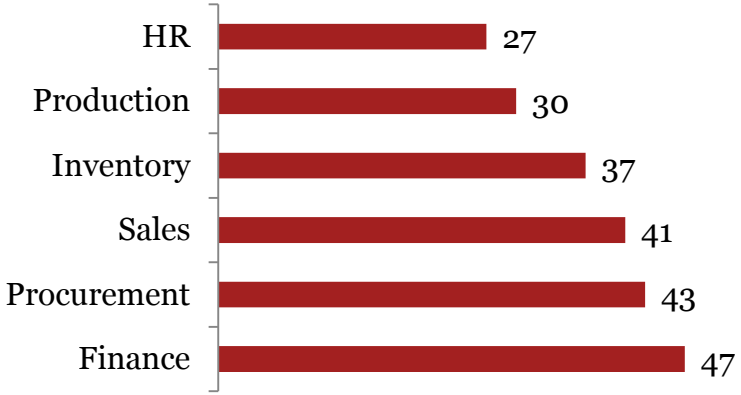
Responding department



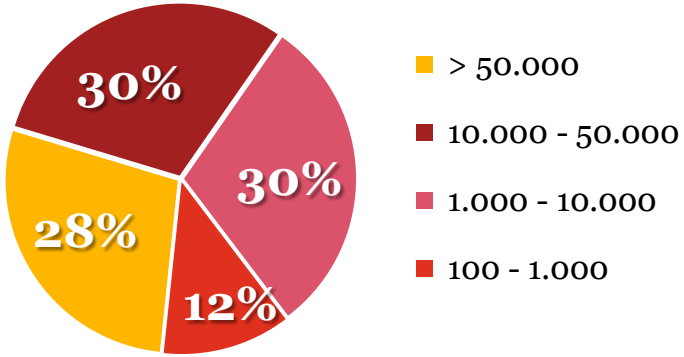
Top 5 industries



SAP supported processes



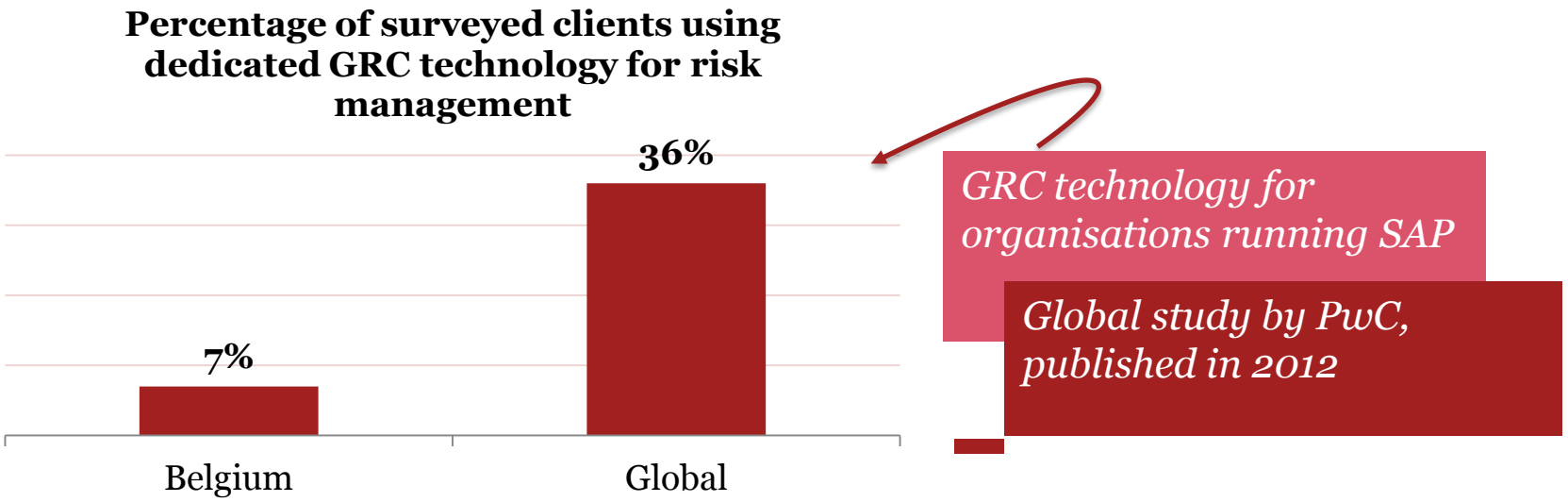
Number of employees



Key conclusions
Risk management

*Only **7%** of Belgian companies are using dedicated technology for risk management purposes, as compared to **36%** of companies globally*

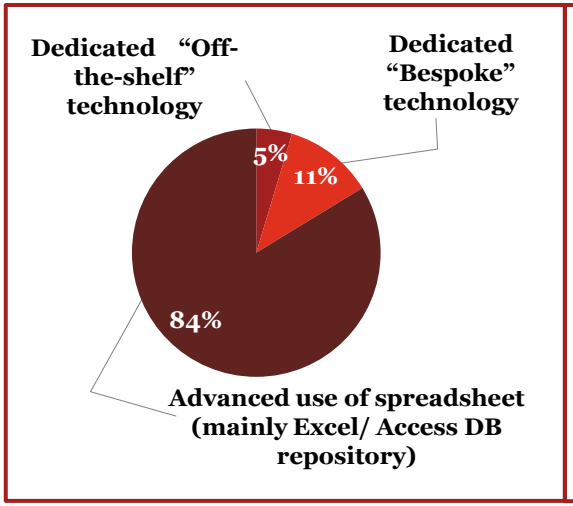
Of the 7% most companies are using custom in-house developed applications



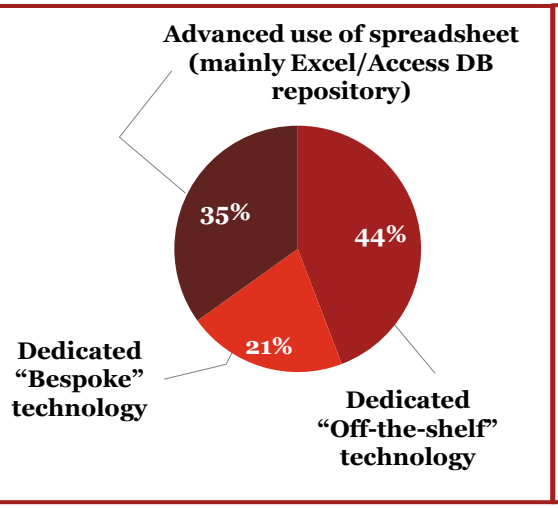
Key conclusions
Internal control management

Numbers from PwC's global GRC survey

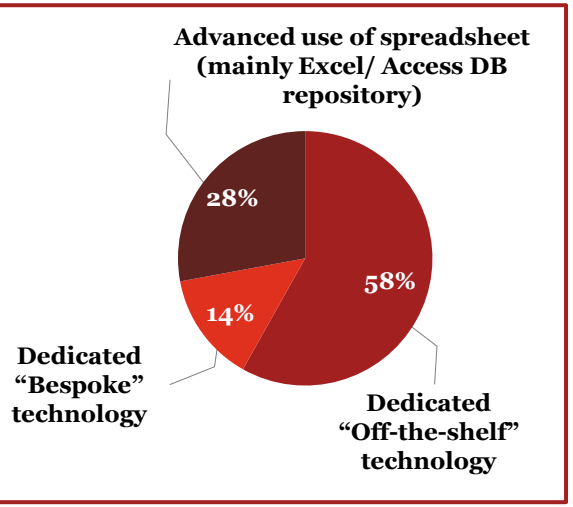
Year 2005



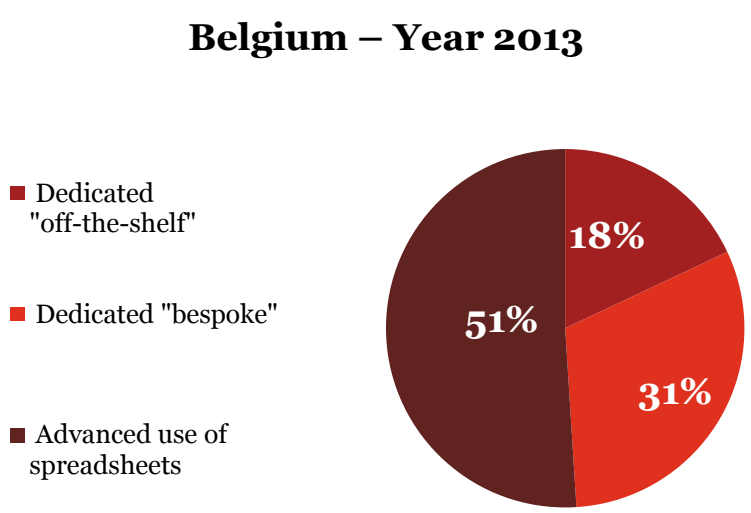
Year 2010



Year 2011



Key conclusions
Internal control management

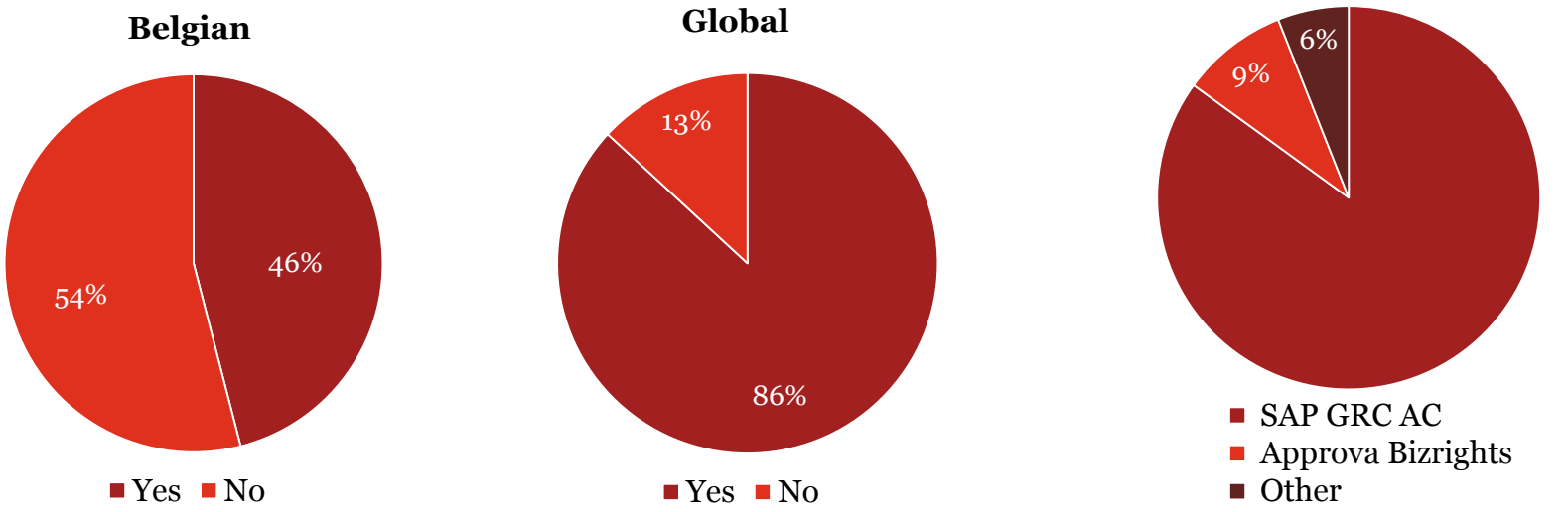


Belgian companies mostly use MS Office applications and consequently our survey shows:

- increased cost to maintain internal control frameworks;
- limited use of automated functionality such as workflows and dashboards; and
- current solutions do not scale well over large organisations.

Key conclusions
User access management

Percentage of organisations that own dedicated GRC technology for user access management



*Due to inherent complexity of security in SAP, nearly **90%** of global surveyed clients use dedicated GRC technology to manage user access. Currently, **46%** of Belgian surveyed clients follow this trend and consequently more than half of respondents do not have a transparent view of their authorisations.*

Trends, analysis & insights on the Belgian market

- GRC technology benchmark 2013
  - Enterprise risk repository & management
  - Compliance and control repository & management
  - Continuous monitoring and analytics
  - Access Management
  - Audit lifecycle management

Key focus areas

1. **Enterprise risk repository & management**
2. **Compliance and control repository & management**
3. **Continuous monitoring & analytics**
4. **Access management**
5. **Audit lifecycle management**

Key focus areas

1. **Enterprise risk repository & management**
2. Compliance and control repository & management
3. Continuous monitoring & analytics
4. Access management
5. Audit lifecycle management

GRC technology benchmark 2013

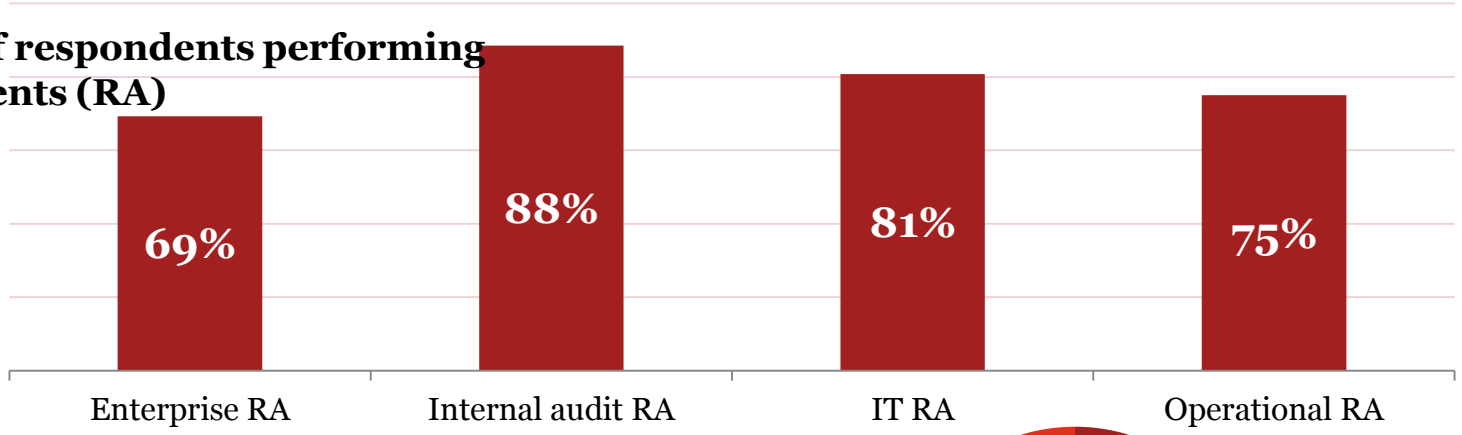
1 Enterprise risk repository & management

Conclusions

- *The vast majority of clients are still using a wide range of spreadsheets (e.g. Excel) to document and maintain their enterprise risk repository*
- *Organisations have generally adopted a sequential and phased approach when deploying the GRC Risk Management technology, focussing on core functionality first*
- *Most of the risk events managed within the GRC technology fall under the "financial" and "compliance" risk categories*
- *Risk management is still viewed as a compliance exercise and is typically performed with an annual frequency. Very few organisations have designed more sophisticated risk analysis processes by introducing additional dimension(s) such as risk velocity, risk reaction, etc.*
- *The majority of organisations respond to risks through the creation and/or assignment of existing controls (financial, operational, etc.). In most cases, the quantitative evaluation of residual risk exposure is still a manual, non-standardised and non-automated process.*

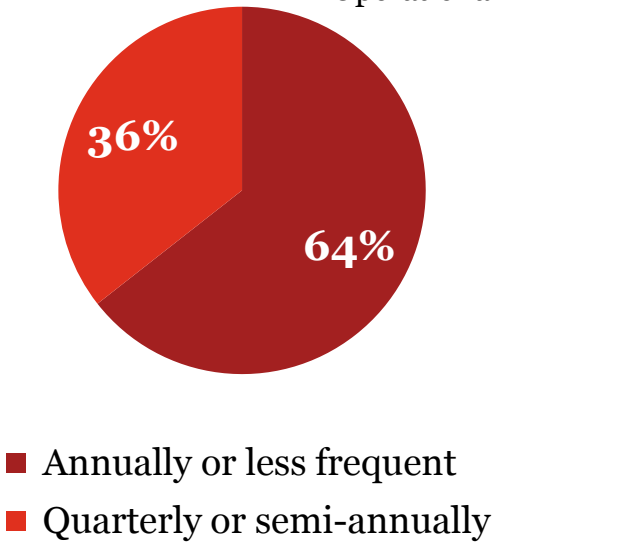
Enterprise risk repository & management

Percentage of respondents performing risk assessments (RA)



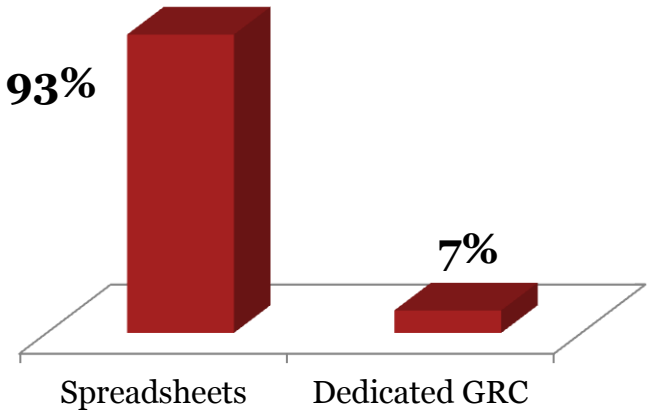
Most companies perform various types of risk assessments. However, this is still viewed as a compliance exercise. Risk assessments are typically performed with an annual frequency.

Current risk assessments are generally performed using a two dimensional approach (probability and impact) to estimate inherent risk levels. Few organisations have designed more sophisticated risk analysis processes by introducing additional dimension(s) such as risk velocity, risk reaction, etc.



Enterprise risk repository & management

Technology used for risk management activities



Only 7% of surveyed clients use dedicated GRC technology to document and manage their enterprise risk framework(s).
All others use spreadsheets.

The vast majority of clients are still using a wide range of spreadsheets (e.g. Excel) to document and maintain their enterprise risk repository.

Risk management is not anchored in formal enterprise-wide technology systems, leading to inefficiency and increased costs.

A “siloed” and non-centralised approach to risk management processes usually requires much more efforts for data analysis and consolidation.

Enterprise risk repository & management

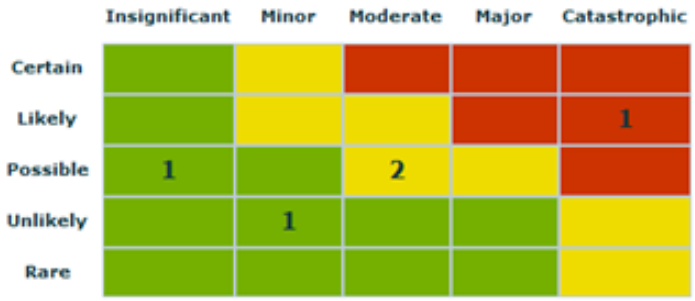
Of the surveyed clients having a dedicated GRC solution:

Nearly all have only implemented "core" functionalities such as:

- *Central risk repository*
- *Standard risk assessment process*
- *Basic workflow & reporting*

Responding to (or treating) risks is a critical step in the overall risk management process. The majority of organisations respond to risks through the creation and/or assignment of existing controls (financial, operational, etc.).

Example of a risk heat-map in SAP GRC Risk Management, functionality which is not yet frequently implemented:



In most cases, the quantitative evaluation of residual risk exposure is still a manual, non-standardised and non-automated process. Only a few organisations have defined and implemented an automated process to convert control evaluations (design and operating effectiveness) into risk response completeness and effectiveness ratings.

Enterprise risk repository & management

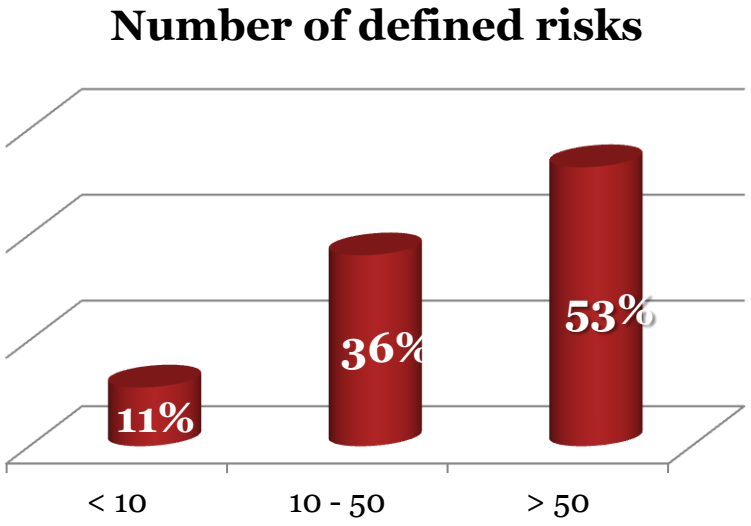
Organisations have generally adopted a sequential and phased approach when deploying GRC risk management technology:

- Phase 1 consists of organisations implementing "core" functionalities in order to enable existing risk management processes (mainly migrating existing data and processes from spreadsheets to a new technology solution). The key objective of phase 1 was centralising master data (harmonised risk repository) and performing risk assessments, because this has a low complexity level and can be completed in less than 1 year.
- Phase 2 is about incorporating new functionalities (such as heat maps, risk simulation, early risk detection through Key Risk Indicators, etc.) into the overall enterprise risk management environment.

***67%** of the surveyed clients having a dedicated GRC solution have implemented and customised the technology with the support of the vendor and/or external consultants.*

Enterprise risk repository & management

Of the surveyed clients having a dedicated GRC solution:



47% have defined less than 50 risks in their respective risk repositories. Interrelationship between risks are typically not defined.

GRC tools provide a central repository to define all potential risks and risk events identified as applicable to the organisation.

47% of surveyed clients have considered less than 50 risks. Most of the defined risks fall in the financial and compliance risk categories.

Risks do not occur in silos and the occurrence of one risk should have an influence on one or more other risks. Defining “influence factors” and risk interrelationships is an important step in order to move towards risk scenario management and assess, in a quantitative manner, the overall “cross” risk exposure to the organisation.

Key focus areas

1 Enterprise risk repository & management

2 Compliance and control repository & management

3 Continuous monitoring & analytics

4 Access management

5 Audit lifecycle management

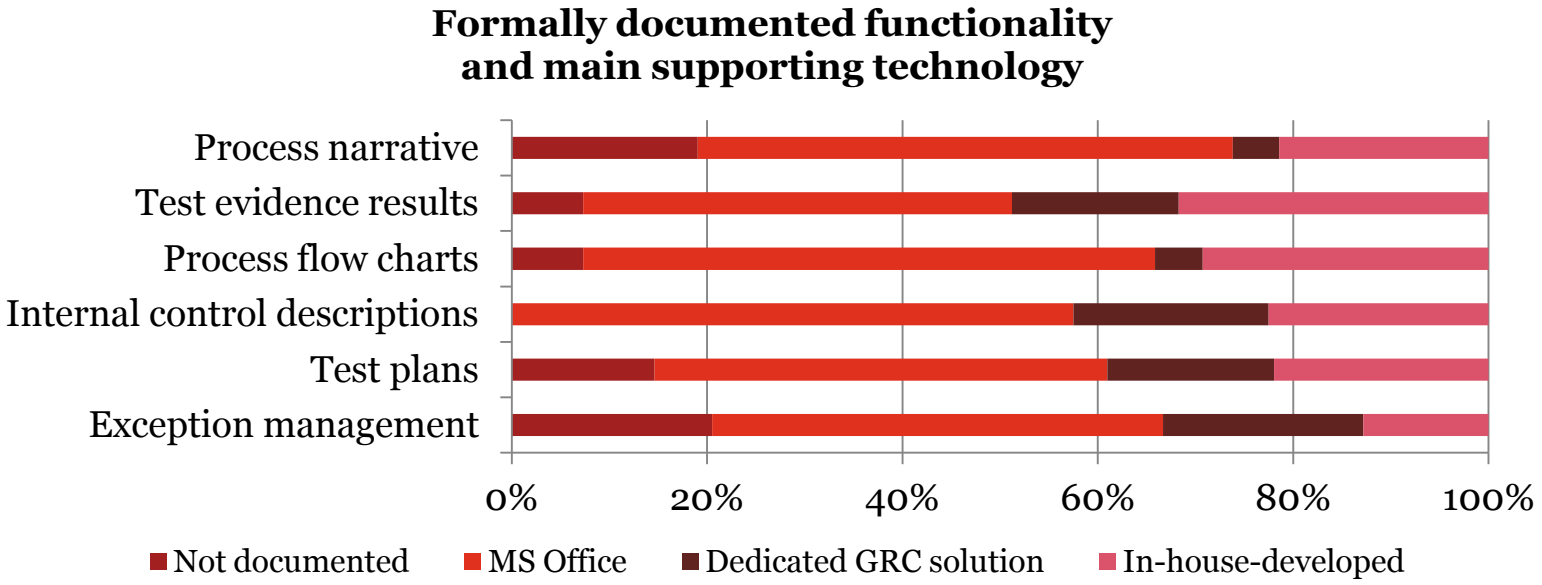
GRC technology benchmark 2013

2 Compliance and control repository & management

Conclusions

- *The vast majority of clients are still using a wide range of spreadsheets to document and maintain their enterprise control repository.*
- *The majority of organisations that are acquiring a GRC technology, are doing so with a primary objective of documenting and organising their existing control framework(s). Few organisations are already using GRC technology for specific activities such as continuous monitoring.*
- *Due to the increase in maturity of GRC technology, clients without dedicated GRC technology are directly investing in "off-the-shelf" GRC solutions rather than bespoke solutions. Client adoption of "off-the-shelf" GRC technology has significantly increased compared to previous years.*
- *An increase in regulatory compliance requirements has led organisations to consider consolidating their internal control repository into a single centralised "multi- compliance" framework.*
- *Few technology vendors offer a continuous monitoring platform which is embedded within the compliance and control framework .*

Compliance and control repository & management



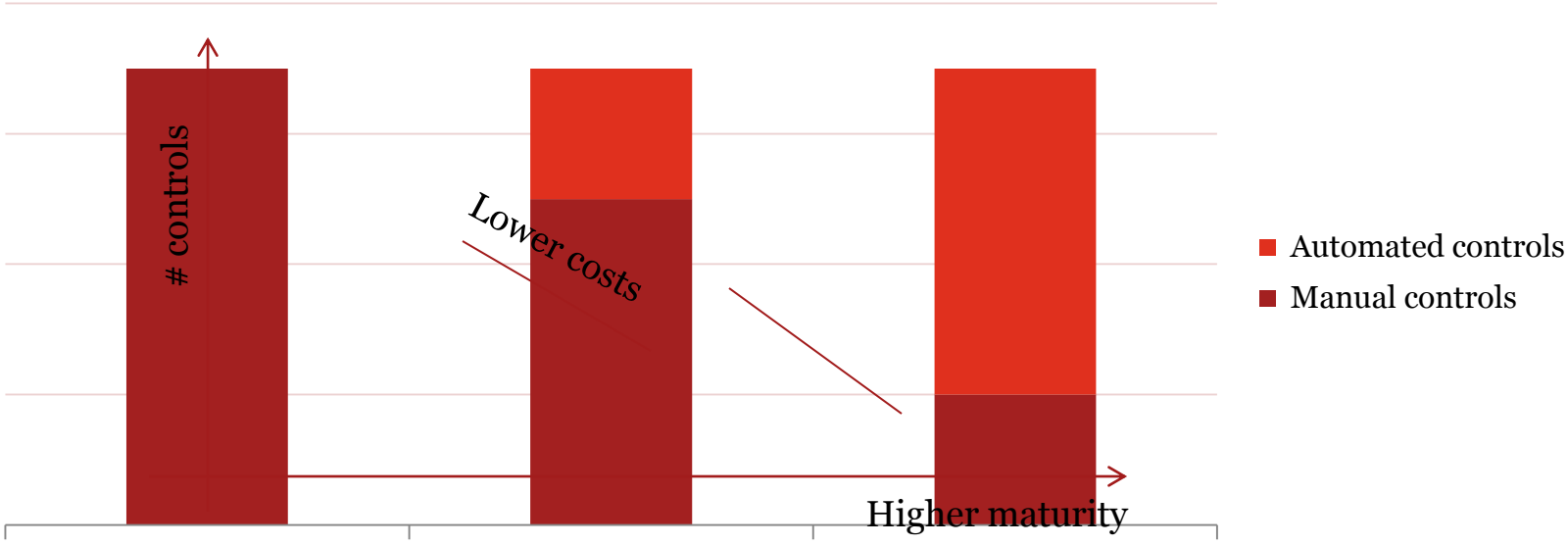
The vast majority of surveyed clients has formally documented their controls and related management activities. Most of them are still using spreadsheets to support this. However, agreement exists on the fact that these solutions lack functionality and technical robustness leading to increased cost of usage and maintenance.

Currently, the primary objective of companies acquiring GRC technology is to centrally document and organise their existing control framework(s).

Compliance and control repository & management

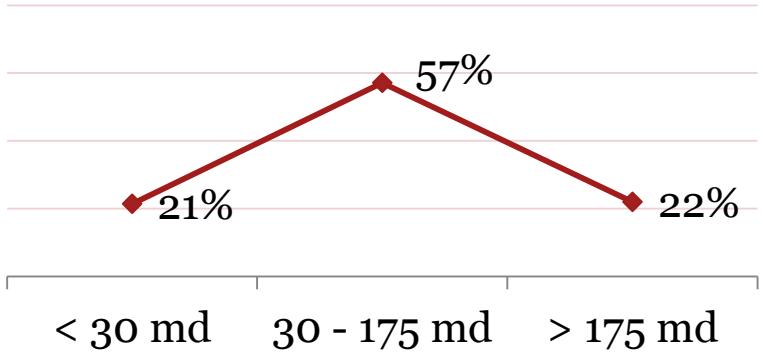
88% of the surveyed clients agrees that their tool has improved their internal control environment and is generating savings (cost) and efficiency (time) when managing internal control processes and activities. However, only 5% is currently leveraging GRC technology to increase reliance on automated controls.

Control automation results in less manual labour and lower costs and offers more granularity, improved consistency and higher control frequency.



Compliance and control repository & management

***94%** of surveyed clients required customisation in order to fit business requirements and implemented the technology with the support of the vendor and/or external consultants.*



Standard core functionality of dedicated GRC solutions includes:

- Master data repository: e.g. risk, business process & control repository, organisation hierarchy
- Configuration such as standard workflow, end-user interface
- Testing activities
- Security such as role & authorisation definition (usually by leveraging security model provided by the vendor)

*On average, the Belgian companies in our survey have spent **30 to 175 man-days** to implement core functionality.*

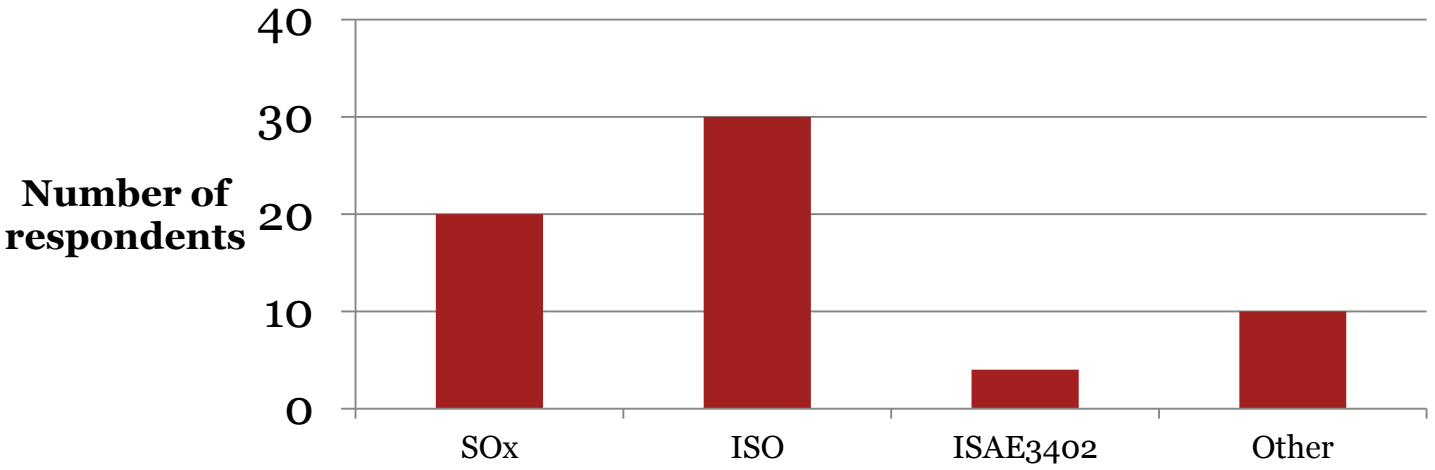
Compliance and control repository & management

The acquisition of GRC technology to manage compliance and control activities is mainly driven by a “reactive” compliance (pressure from compliance/ regulatory requirements).

A significant number of organisations have defined and implemented internal principles and frameworks for control management.

More and more, organisations are looking to manage all their existing compliance and control framework(s) in one single technology platform.

Compliance regulations managed in a GRC platform by respondents:



Compliance and control repository & management

How can GRC technology enable a “multi-compliance framework”?

A

One technology. *Using a **single software platform** to improve efficiency and effectiveness in managing all compliance activities (compliance initiative agnostic framework). The multiple-compliance framework enables you to implement a **variety of compliance initiatives**, such as financial compliance (SOx) operational compliance (COBIT, ISO 17799: 2005) or others as needed.*

B

Shared master data. *Using common and **centralised master data** to reduce **redundancy.** Ability to implement one or more compliance initiatives and document their requirements (possibility to also group compliance initiatives).*

C

Flexible attribute per regulation. *Ability to maintain **compliance-specific attributes** of organisation, risks, processes, subprocess and control if required (**allowing a flexible way to share data** across multiple compliance frameworks).*

D

Authorisation & accountability. *Ability to **specify compliance-specific authorisation model**. Users with compliance-specific roles can edit the data for a particular compliance framework, but can only see data from other compliance frameworks. Users with a cross-compliance role can edit data for all compliance frameworks, e.g. cross-compliance tester, cross-compliance policy owner, etc.*

E

Reporting & dashboards. *Using **shared evaluations** across multiple compliance initiatives and define **common compliance processes** and **reporting**. Ability to implement “shared” testing and assessments across compliance initiatives and leverage evaluation results across multiple framework (testing optimisation). When scheduling testing activities, you will have the possibility to indicate if you want to share the test results across multiple regulations.*

Key focus areas

1 Enterprise risk repository & management

2 Compliance and control repository & management

3 Continuous monitoring & analytics

4 Access management

5 Audit lifecycle management

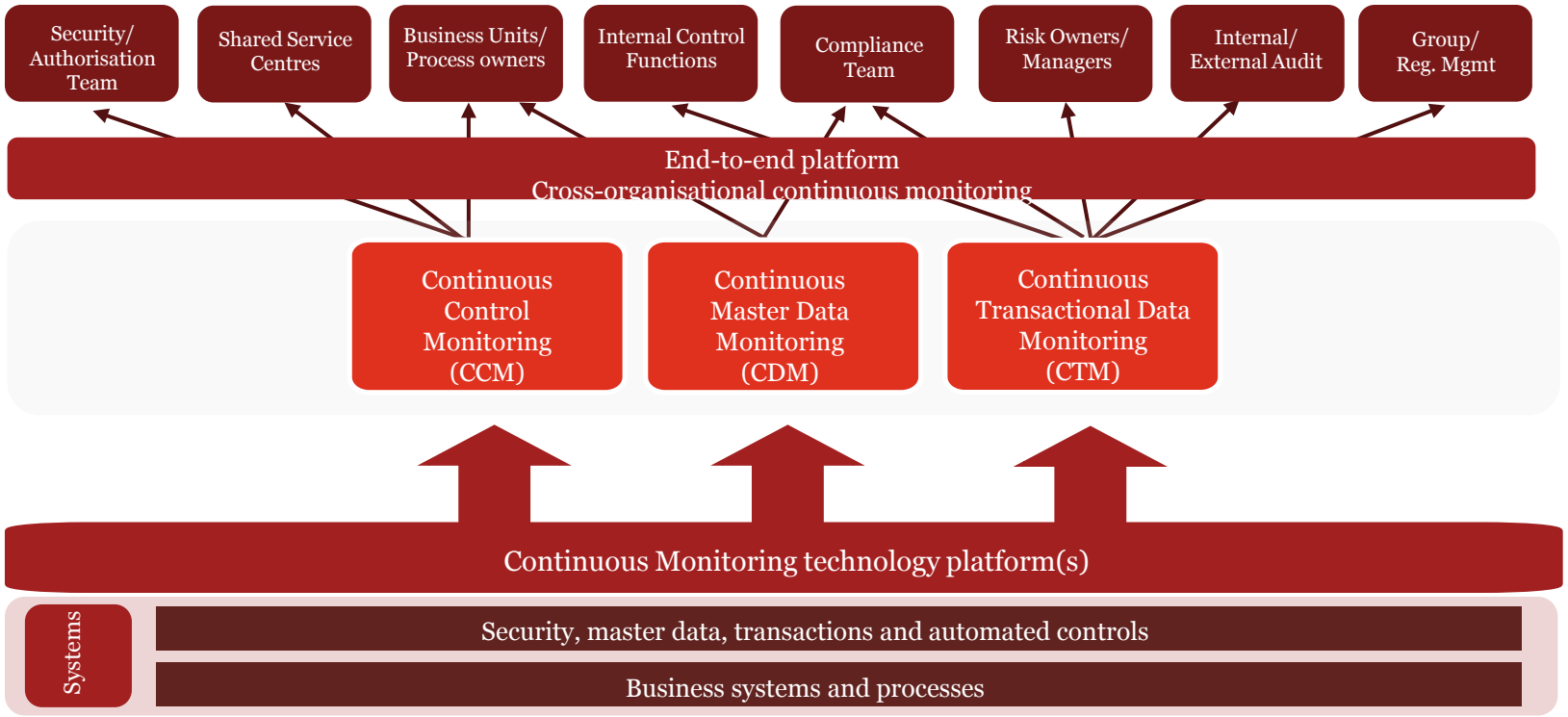
3 Continuous monitoring and analytics

Conclusions

- *Continuous monitoring (CM) technology is still maturing. Few organisations are currently using a Continuous Monitoring (CM) solution as part of their routine compliance activity. The use of CM technology is always very targeted (one SAP instance, one market, one company, etc.) and limited (specific financial processes, specific types of continuous monitoring mechanism, etc.).*
- *Organisations are initially developing automated rules to monitor critical configurations, before rolling out the CM technology for data monitoring (master and transactional data).*
- *Most of the organisations that are implementing CM have defined a sequential and gradual deployment by "waves" in order to make sure that the "element of change" around people & process can be effectively managed, governed & embedded.*

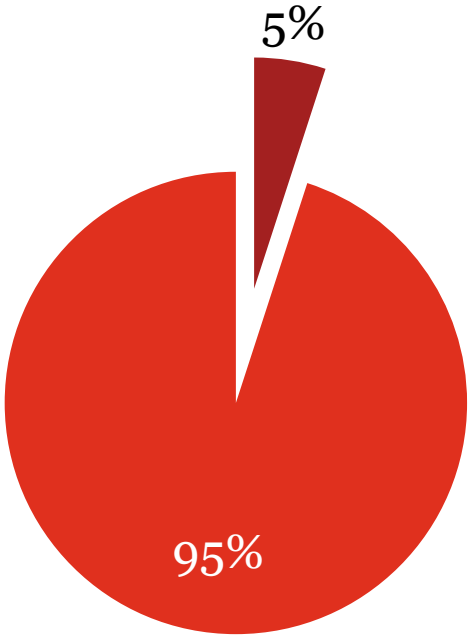
Continuous monitoring and analytics

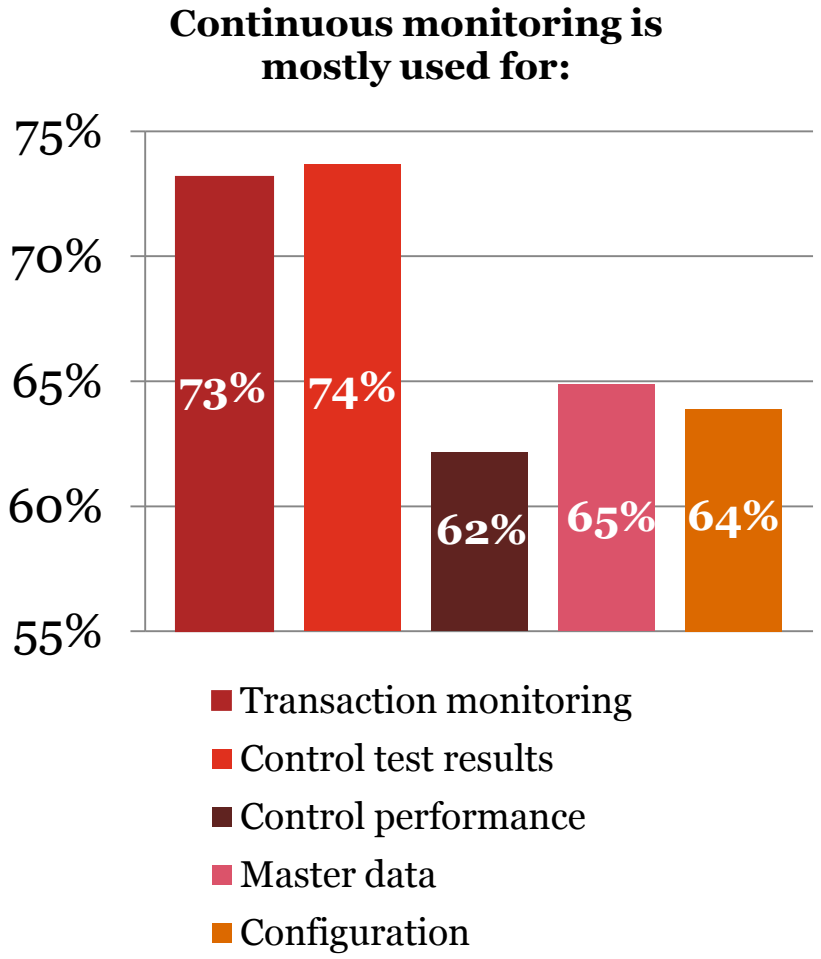
Continuous monitoring is a mechanism that enables organisations to get near real-time insight into behaviours across all SAP modules that deviate from established standards and/or ways of working.



Continuous monitoring and analytics

*Only **5%** of surveyed clients fully agree that their tool facilitates continuous monitoring of their internal control environment.*





Key focus areas

1 Enterprise risk repository & management

2 Compliance and control repository & management

3 Continuous monitoring & analytics

4 **Access management**

5 Audit lifecycle management

4 Information security & access related matters

Conclusions

- *More and more organisations are implementing a dedicated GRC access management technology. Also, organisations are looking to expand the coverage of GRC access management technology to non-core SAP platforms such as HR, CRM and BI.*
- *While the majority of surveyed clients are monitoring SoD risks, only few have defined sensitive access risks for business and SAP basis.*
- *Organisations are looking at GRC access management technology to support user provisioning processes across the underlying SAP landscape.*
- *Emergency access management continues to be a challenge for organisations.*
- *Organisations that have already invested in GRC Access management technology to support user provisioning processes, are now looking for integration with wider Identity management (IdM). This continues to be an aspiration.*

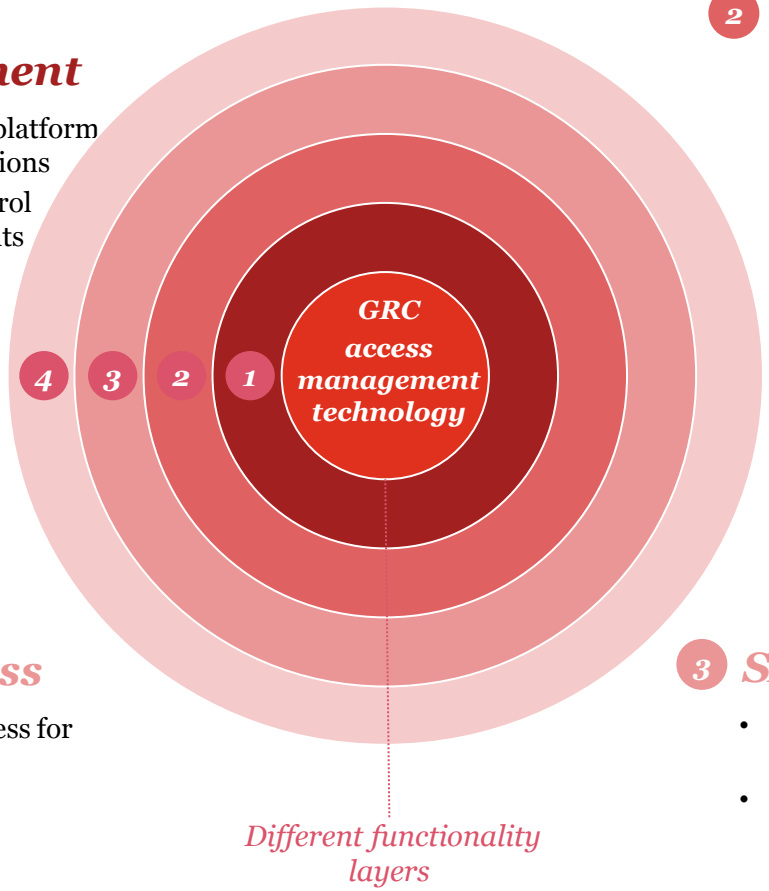
Information security & access related matters

1 SoD & sensitive access management

- Monitors real-time cross-platform SoD's and critical transactions
- Maintains mitigating control definitions and assignments

2 User provisioning

- Accelerates the request approval process for SAP and non-SAP systems
- Automatically provision roles to users in SAP and non-SAP systems



4 Emergency access

- Pre-define emergency access for approved users
- Activity monitoring for all emergency users

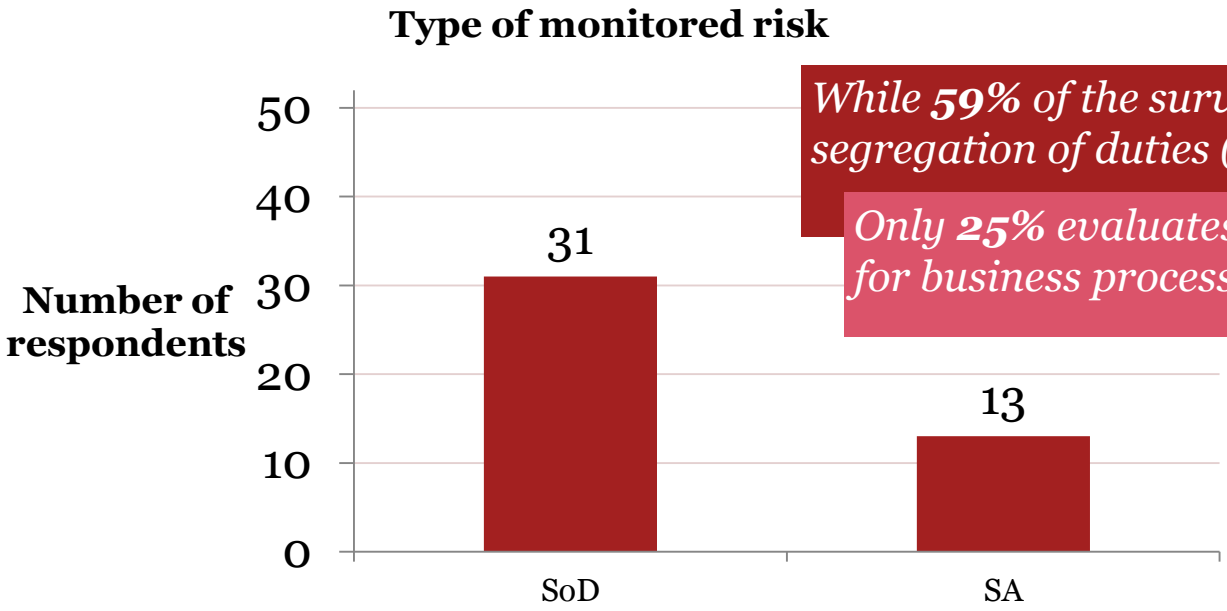
3 SAP role management

- Applies consistent and structured approach to building roles
- Documents role information, such as SoD analysis results and change history

Information security & access related matters

Typically, organisations initially use GRC access management solutions to monitor only segregation of duties (SoD) risks. However, a growing number of clients leverage their GRC solution to monitor sensitive access (SA) risks.

Mature organisations monitor both sensitive transactions (critical access) and sensitive authorisation objects (critical permission).



*While **59%** of the surveyed clients monitors segregation of duties (SoD) risks.*

*Only **25%** evaluates sensitive access risks for business processes and SAP Basis.*

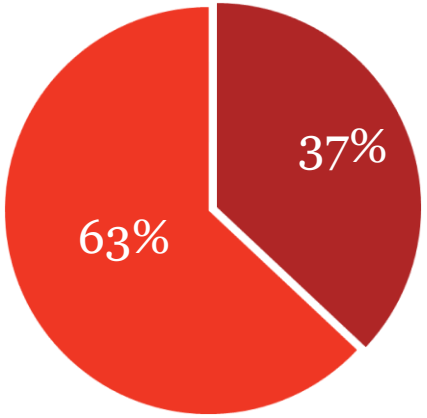
Information security & access related matters

Most organisations continue to rely on manual mitigating controls to respond to segregation of duties and sensitive access issues, rather then applying a structural solution through an SAP security authorisation redesign. Such manual mitigating controls tend to be costlier in the longer term than system based remediation.

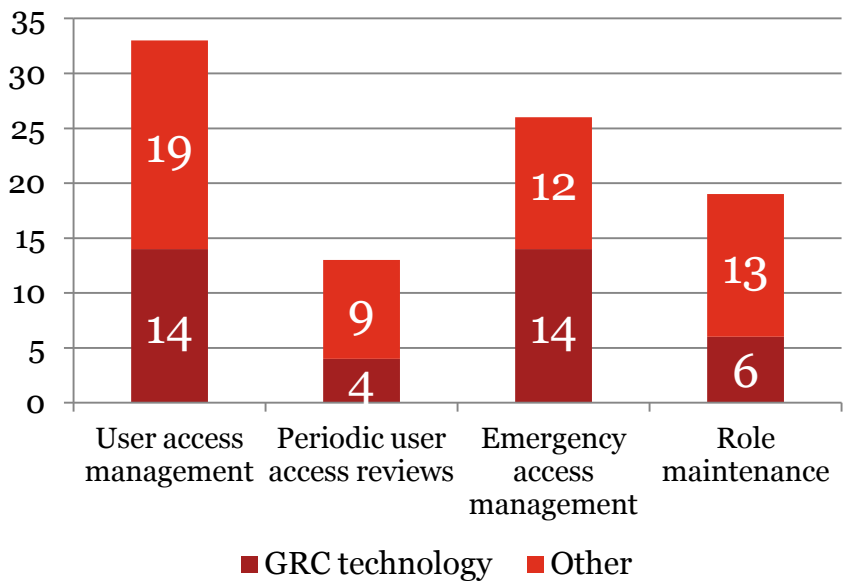
In addition to a redesign, organisation with a high number of access violations should consider rolling out GRC tool functionality to manage user access in a controlled manner, e.g. SAP emergency access management. Organisations invest in further GRC Access management solution (like emergency access management) to manage critical access, as this is cheaper and more effective in the long term.

***63%** of organisations with access violations defined manual mitigating controls as a response.*

These controls should be minimally used as they are more error-prone and increase total cost of ownership.



Information security & access related matters



Organisations have implemented formally documented processes for user access management and emergency access management as a reaction to compliance & regulatory requirements and audit findings.

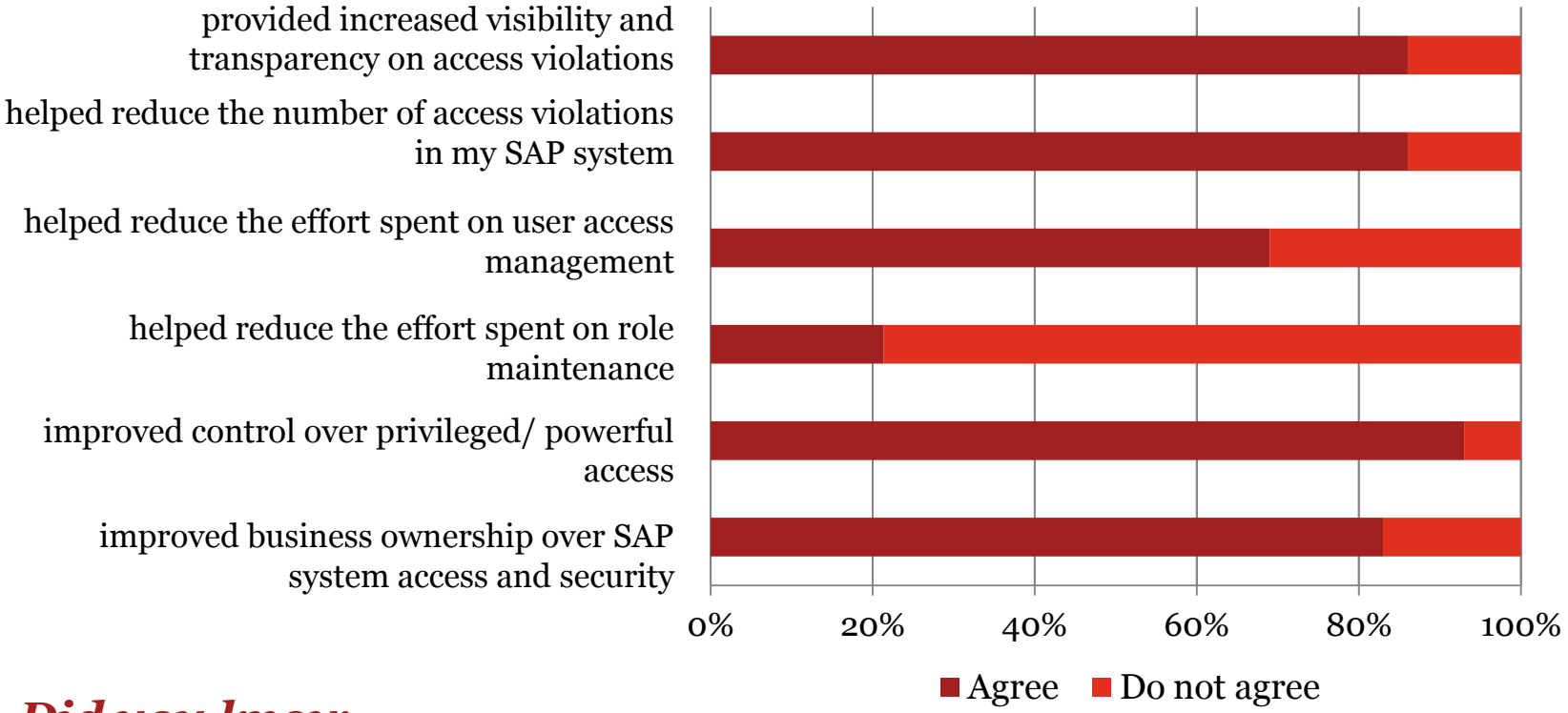
Dedicated GRC technology is widely used by organisations to manage user access and to monitor emergency access.

However, organisations continue to struggle to identify the right function to administer, support and maintain emergency access management technology as it requires a combination of IT, business and risk skills.

***37%** of the surveyed clients using dedicated GRC technology use SAP GRC Access Control for user access management and emergency access management.*

Information security & access related matters

My GRC tool…



Did you know…

SAP is now also offering a **Starter Edition of SAP GRC Access Control**. This edition costs approximately 1/3rd of the full suite price and supports the measuring, monitoring & reporting of access risks and administering & reporting of super user access.

Key focus areas

1 Enterprise risk repository & management

2 Compliance and control repository & management

3 Continuous monitoring & analytics

4 Access management

5 Audit lifecycle management

5 Audit lifecycle management

Conclusions

- *Internal Audit functions continue to use standalone Audit Management Systems (AMS). However, more and more GRC solutions contain a dedicated module with similar functionality.*
- *Next to audit file management and issue tracking, larger teams also tend to use dedicated functionality for audit scheduling, time management, monitoring stakeholder KPIs, etc.*
- *IA functions continue to apply caution when deciding to co-invest with the business in a GRC platform, in order to be able to safeguard their independence.*

Audit lifecycle management

How might Internal Audit functions interact with GRC technology for compliance and control repository & management?

- Greater visibility of management testing and monitoring activities: Internal Audit can review evidence of control execution/review performed by business units (single point of evidence repository)
- Independent testing can be performed by Internal Audit through the use of GRC technology. Ability to test operating effectiveness of control for targeted processes/organisation units.
- Injection of internal audit issues /findings in management evaluation activities.
- Improved visibility of risk exposures available “at the press of a button”.
- Full audit trail of risks, controls , exceptions and mitigations.
- Increased efficiency enabling re-allocation of audit effort to other (more strategic) priorities.
- Information enabling more risk-targeted audit activities based on exception data.

Audit lifecycle management

But….

- Increased visibility of risk exposures will require strategies on how to respond outside of annual audit planning.
- The debate continues around Internal Audit's independence. Should the Audit Management processes (and supporting technology, AMS) run on the same platform (using same master data, shared processes and planning mechanism) as the Risk/Compliance platforms . We have seen many clients that are not very keen on mixing AMS (Internal Audit) with other Risk & Compliance solutions for independence and complexity reasons…

How can PwC help?

How can PwC help?

- Accelerated implementation methodology for SAP GRC
- SAP authorisation quick-scan & (re)design
- SAP utilisation & monitoring metrics
- Why PwC?

PwC's accelerated implementing methodology (AIM) for SAP GRC

PwC AIM GRC

AIM GRC is an accelerated SAP GRC implementation package developed by PwC.

Our solution significantly reduces implementation time and can save up to 60% of cost.

PwC's market leading teams are supported by extensive experience, a proven methodology and proprietary accelerator tools.

AIM GRC is a 12 week accelerated implementation program.

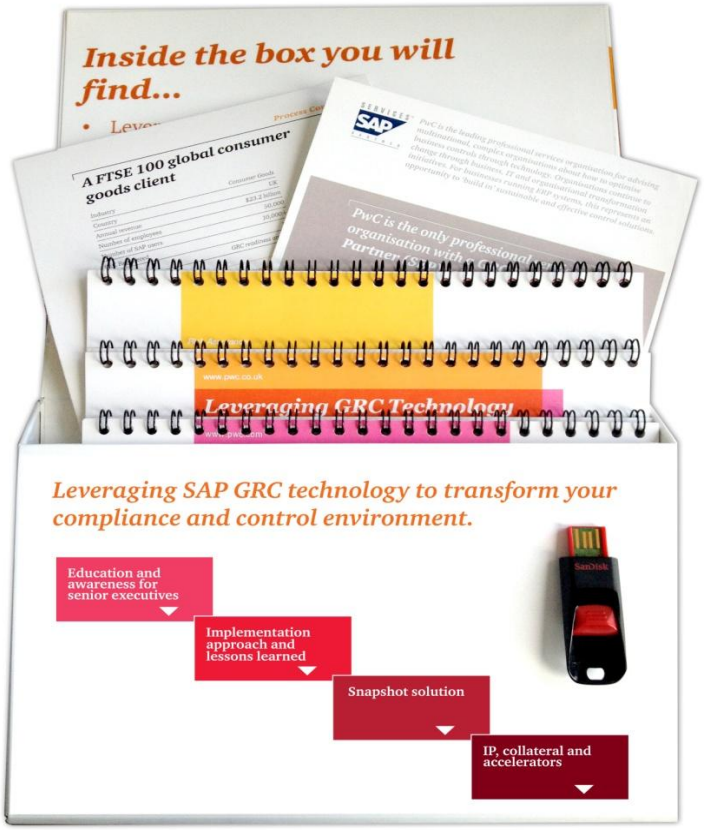
AIM GRC leverages significant collateral, intellectual property and accelerator products and tools that form the base implementation solution.

AIM GRC reduces the implementation cost of "core" functionality, allowing your organisation to rapidly migrate existing risk & control repositories. This provides the platform to evolve your solution as you require.

PwC AIM GRC

Our AIM capability is achievable through leveraging our extensive experience in full end to end SAP GRC implementations

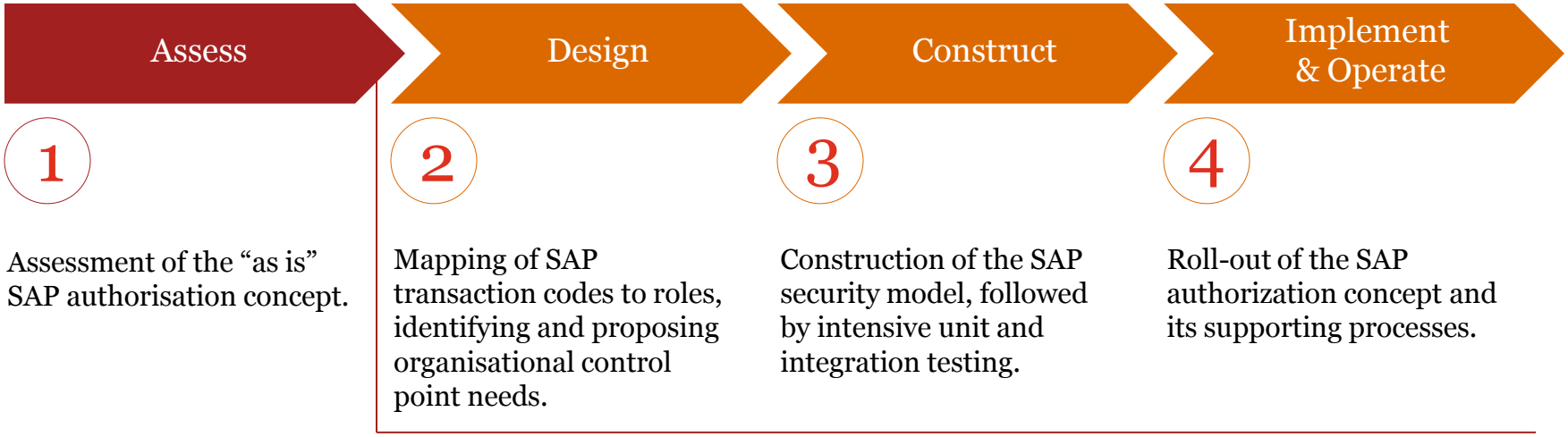
A summary of the SAP GRC technology value proposition, our services and supporting IP have been consolidated into PwC's "SAP GRC in a Box" solution



PwC's SAP authorisation quick-scan & (re)design

Our methodology
SAP security: Design to align

We follow a proven methodology to evaluate and design SAP security. During a SAP authorisation quick-scan, we focus on the "Assess" phase and identify possible next steps to help improve the maturity of the SAP authorisation concept.



The "as is" assessment covers the following aspects :

- Assess and compare how your individual business units are adopting existing controls.
- Benchmark how your security set-up measures against common standards.
- Implement PwC's User Activity Analysis tool to analyse your actual transactional usage.
- Map activity analysis output onto existing security design and identify areas for design remediation.
- Map security access controls design back to SAP security governance design.

SAP authorisation quick-scan
Scope & approach

Our authorisation quick-scan gives you insight in your authorisation concept by evaluation below elements while using our proprietary ACE (automated controls evaluator) tool:

- **SAP Basis** – Providing a clear overview of IT critical functionalities assigned to users across the system in the different areas of user provisioning, change management and operations. Additionally password settings and other typical security settings are reviewed.
- **SAP security** –Providing a summary of profiles and roles set-up within the system and an analysis of customised transactions available. Review of system usage per user and transaction over a period of time. Preferably run in combination with SAP Basis review.
- **Segregation of duties & sensitive access** – For a specific set of modules defined for your system an analysis is performed over some key functionalities in the area of sensitive access and segregation of duties.

Insights obtained through our quick-scan are an important input to decide on next steps to address potential challenges in the SAP authorisations domain.

SAP authorisation (re)design
Task based model with master/ derived or enabler design

We construct SAP authorisations through **task based roles**. This generates following benefits to our clients:

- **Flexible provisioning of roles to users**
  Task based roles are building blocks providing the flexibility to build SAP access at the user level. Transaction codes rarely duplicated between roles making it clear what functionality a role provides.
- **Low maintenance security design**
  Task based roles reduce the need for role maintenance they can be leveraged when assigning access to users with different jobs.
- **Reduction in SoD risk violations**
  SoDs are less likely to occur within a task. Use of task based roles therefore significantly reduces the risk of inherent SoDs in roles and provides the ability to minimise SOD conflicts at the user level through flexible provisioning.

Master/ derived design

- Traditional approach
- Only one role needed to give complete access to transaction codes and authorizations
- Able to assign different activities in different organizational areas (e.g. not "all or nothing" assignment)

Enabler design

- Four tier model with general, display/ reporting, functional and enabler/ control point roles
- Reduces the number of roles and authorizations
- Reduces complexity with "cross pollination" issues

PwC's SAP utilisation & monitoring metrics

Introduction
SAP utilisation & monitoring metrics

SAP aims to deliver an integrated system which provides you with timely, relevant and accurate information to monitor and manage your business.

Most information coming from SAP **focuses on final results** (financial & operational performance) and doesn't detail how users interact with the system and whether users are following business processes as prescribed.

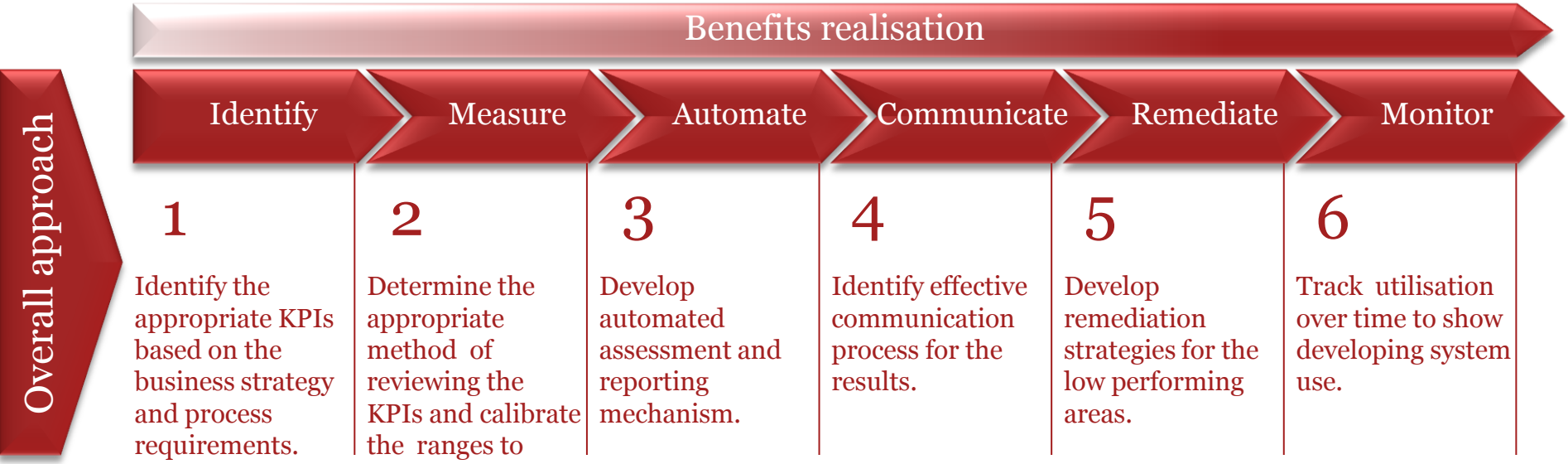
PwC's SAP Business Process Analytics (BPA) service offering allows you to measure your return on investment by:

- Delivering a customised set of relevant **key performance indicators** (KPIs) of system usage; and
- Providing a **sustainable mechanism** to continually assess system usage to drive cost reduction, process improvement and user satisfaction.

Classic reports	SAP utilisation reports
List of invoices without an approved purchase order (PO).	List of retrospective POs (i.e. the goods receipt or the invoice is processed before the PO was created).
List of newly created/changed vendors.	Percentage of incomplete vendor master data based on minimum required fields.
Listing of (manual) FI invoices processed.	Count & value of FI invoices expressed as a % of all FI and MM invoices processed.
Listing of processed journal entries.	Listing of back dated journals, i.e. those where the posting date is prior to the system entry date.

SAP utilisation & monitoring metriccs

Approach

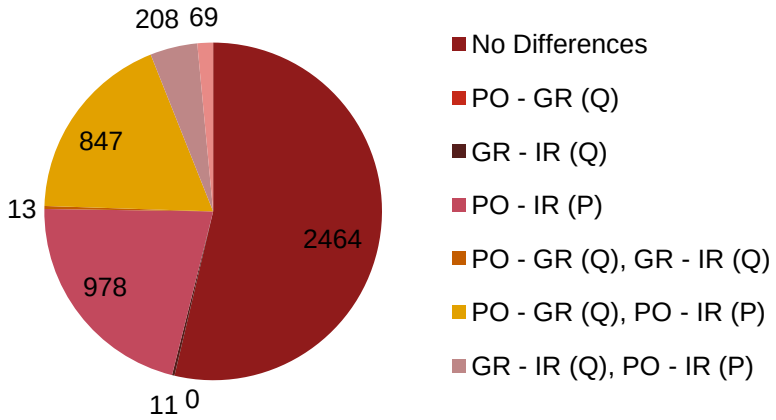


Key advantages:

- Flexible toolset, easy to adapt or develop new KPI's or dashboards.
- Queries are SQL based and can be integrated in different BI tools.
- No software license costs to start up project.
- Quick project start-up with real data results; ideal as proof of concept.

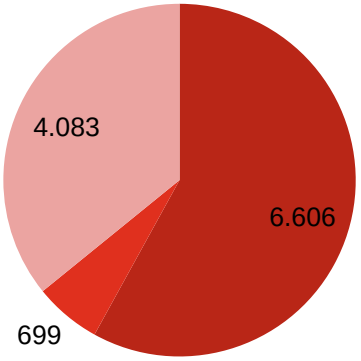
SAP business process analytics KPIs
Some examples

The 3-way match in the SAP MM module helps automate the checking of invoices. This graph shows how 3-way matching vs purchase order and goods receipt was applied for invoices, both in terms of quantity and price.

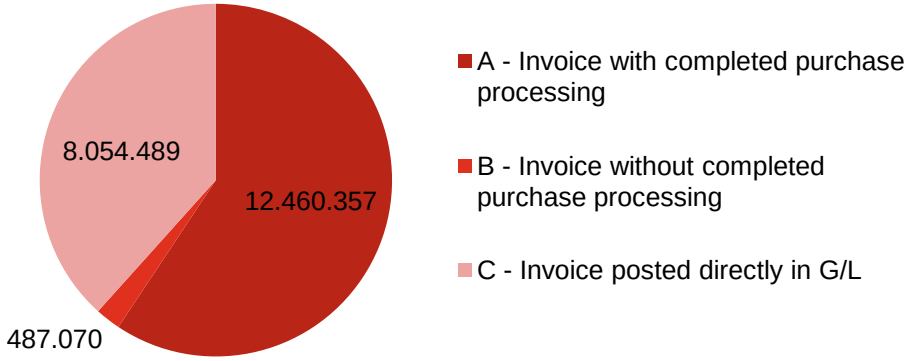


However, the number of invoices doesn't tell the full story. It's important to see how many line items are concerned and what amounts are involved

Line items



Amounts (EUR)



Why PwC?

A team of **200+ dedicated SAP GRC professionals** who have extensive experience in implementing SAP GRC solutions

Geographical presence in all key markets, providing experienced resource solutions and options in key locations

SAP GRC Special Expertise Partner (SEP) relationship with SAP

A market leading position as SAP GRC integrator and advisor. Our SAP GRC practice has a depth and breadth of implementation experience that is unmatched in the global market

By leveraging knowledge and lessons learned across other SAP GRC projects globally, our Centre of Excellence team will assist you throughout all phases of the implementation life cycle as required

We have assisted SAP with the detailed testing and validation of SAP GRC solutions, enabling you to gain better insight and understanding of how to get the best out of the solution

Why PwC?
Our global experience and credentials


Certificate

On account of its special expertise and successful cooperation,

PWC

has been appointed as a

SPECIAL EXPERTISE PARTNER

Enterprise Performance Management, Governance Risk & Compliance and Sustainability Solutions

Valid from January 14th to 31st December 2011

SAP UKI Ltd

Mark Hollyhead
Sales Director – PGA Solutions

Lizzy Squires
UKI Alliances Director

THE BEST-RUN BUSINESSES RUN SAP

SAP Global Partner

More than 15 GRC 10.0 PC implementations

+50 end to end GRC Access Control implementations (5.3 & 10.0)

Centre of Excellence team dedicated support and deep expertise

Business and system integrator capability

SEP status with SAP for GRC solutions

Collateral and accelerators to fast track implementation

Full GRC 10.0 experience covering Access Control, Process Control and Risk Management experience

Our SEP Status - The right experience and credentials for you

SAP have granted us Special Expertise Partner status for GRC due to our unrivalled experience of delivering successful integration projects.

This also gives you access to the right people in SAP for problem resolution.

Thank you

Ingvar Van Droogenbroeck
Partner
Office: +32 (0) 2 710 7204
Cell: +32 (0) 477 381 445
ingvar.van.droogenbroeck@pwc.be

Wim Rymen
Director
Office: +32 (0) 2 710 7238
Cell: +32 (0) 473 269 227
wim.rymen@pwc.be

Kris Wauters
Manager
Office: +32 (0) 2 710 4631
Cell: +32 (0) 499 558 949
kris.wauters@pwc.be