

Turnkey Consulting

GRC Benchmark April 2010

Introduction

There are a number of activities that combine to form an effective Governance, Risk and Compliance (GRC) strategy. At Turnkey Consulting we are helping our clients to embed these activities into their processes and to raise the profile for management of security and risk in their organisations.

Launched in summer 2009, our GRC benchmark sets the standard for SAP® security best practice with data gathered from over 100 organisations using SAP to support strategic business processes.

The benchmark data for all the respondents has been analysed and plotted on our maturity models for the following key areas:

- Adequacy of Segregation of Duty Controls
- User Provisioning and Administration
- SAP Security Settings
- Authorisation Change Management
- Application Security Design
- SAP Security Architecture
- Security Design for IT Support Services
- SAP Development Lifecycle and Change Management Processes

Overall we found that while many organisations have been investing in improving their processes, relatively few have automated their compliance efforts. Often there is an overhead associated with increasing control over processes. Automation of those controls can reverse that trend, improve the efficiency of the control and ensure continuous compliance.

Section 1: Adequacy of Segregation of Duties (SoD) Controls

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

Our benchmark has revealed that 74% of respondents maintain an SoD matrix for their SAP applications. The majority of organisations with an established SoD Matrix have also configured the matrix to suit the specific requirements of their business and regularly review the matrix for suitability. Furthermore, the same organisations maintain mitigating controls to manage SoD risks that they cannot remediate via security.

53% of our respondents have automated their SoD monitoring, with the remainder relying on manual processes to identify SoD issues within their SAP applications.

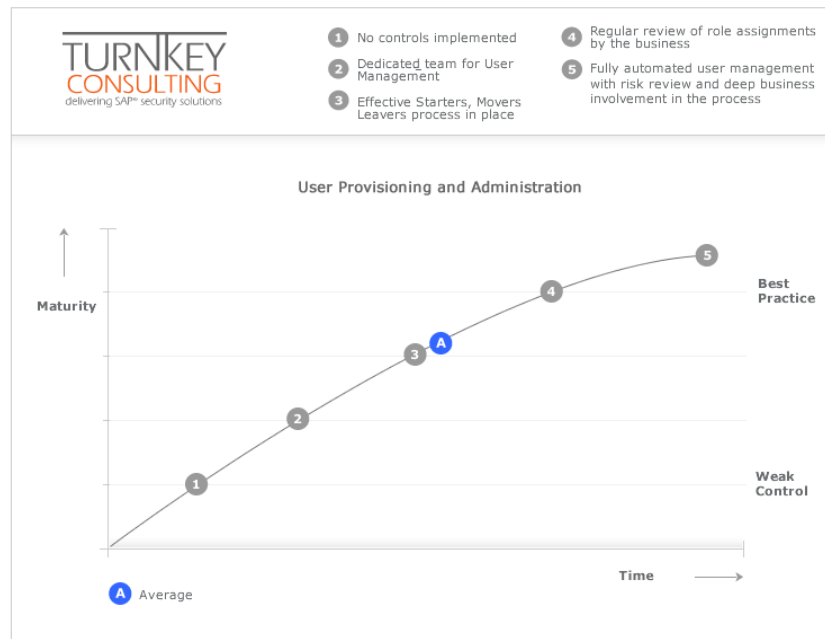
Recommendations:

It is recommended practice to maintain a matrix of SOD risks and fully document compensating controls. Each risk should be owned by a business user who is responsible for either ensuring the business processes are separated as required or that the mitigating controls are in place and working.

Many companies implement automated tools to assist in maintaining the control environment around the segregation of incompatible duties. Ideally these products should allow for full analysis of roles and users across platforms. Ownership should be documented together with the control procedures in place.

Section 2: User Provisioning and Administration

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

The large majority of respondents have a dedicated team responsible for user administration, with formal approvals driving the Starters, Movers and Leavers process. Once users have been created, only 59% of organisations taking part in our survey perform regular reviews of user mapping in conjunction with business role owners.

Half of the organisations polled automate some or all of the user administration, with a similar proportion incorporating SoD review in the user management process.

Recommendations:

The user administration process is a key risk area; this is recognised with many organisations investing in their Starter, Movers and Leavers processes. Increase in control in this area often leads to additional administrative overhead.

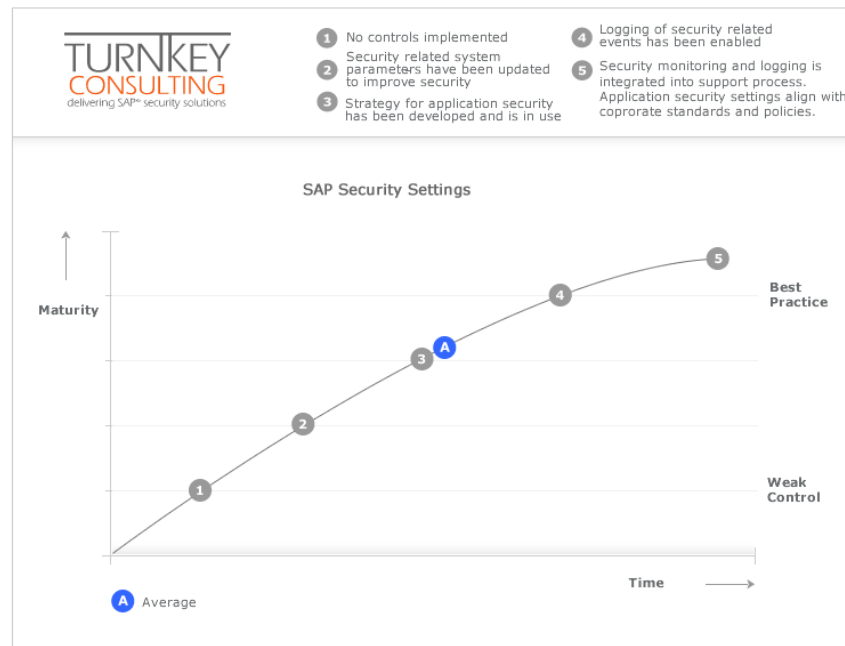
Access creep through role allocation over time is one of the primary causes of users gaining access to excess authorisations and conflicting functions.

Segregation of Duties monitoring should be incorporated within the user provisioning process to ensure that exceptions are caught before the access is granted.

Using automated tools to manage user provisioning can help improve controls via enforcing approvals and SoD checks before users are set up in any system.

Section 3: SAP Security Settings

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

Analysis of our results shows that 81% of our respondents have changed their security related parameters from the SAP defaults to match their corporate security requirements.

70% of organisations who participated in the benchmark have a defined security policy in place which drives their application security. A similar percentage of respondents regularly review their security settings to ensure compliance with corporate standards.

Only 55% of companies record security logs. Even fewer have a process in place to analyse the logs and respond when a threat or vulnerability is identified.

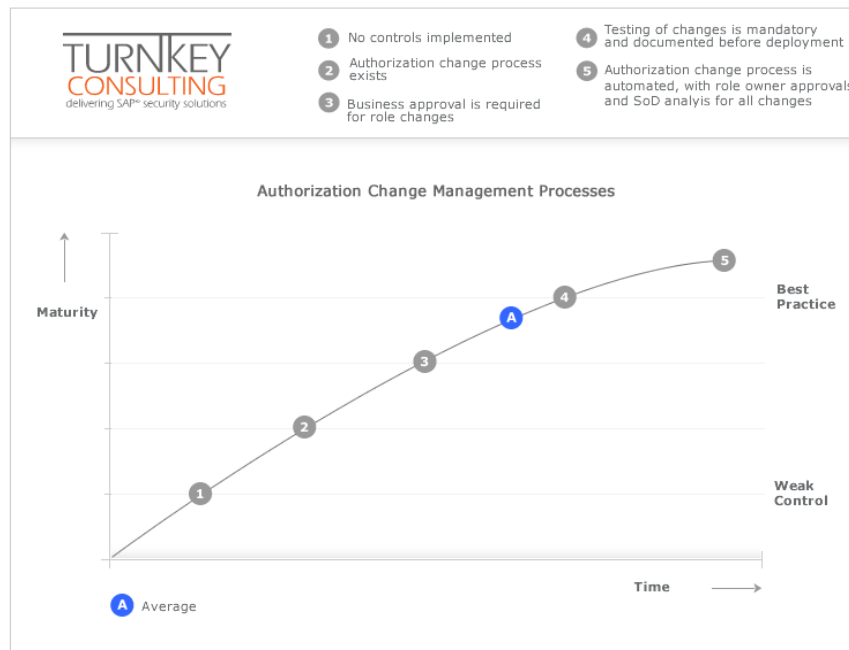
Recommendations:

The security policy should define the infrastructure and application security approach. The maintenance of security related parameters is recommended to provide increased level of control over the SAP defaults. Policies implemented in SAP should be derived from corporate application security policies to ensure consistency of approach across the enterprise.

Logging should be enabled and monitoring should be in place to identify security issues when they occur. Extraction of SAP logs to existing log processing tools can expedite the process.

Section 4: Authorisation Change Management

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

75% of respondents have processes in place to manage role changes and have resources dedicated to making these changes.

The majority of organisations who took part in the survey require business involvement in the change process, however only 65% require business ownership of roles.

50% of respondents perform SoD review as part of the role management process and only 47% require testing to be performed on changes before they are promoted to production.

Recommendation:

Business ownership of roles is vital to ensure that role contents and allocation to users supports the business processes and intended usage of SAP.

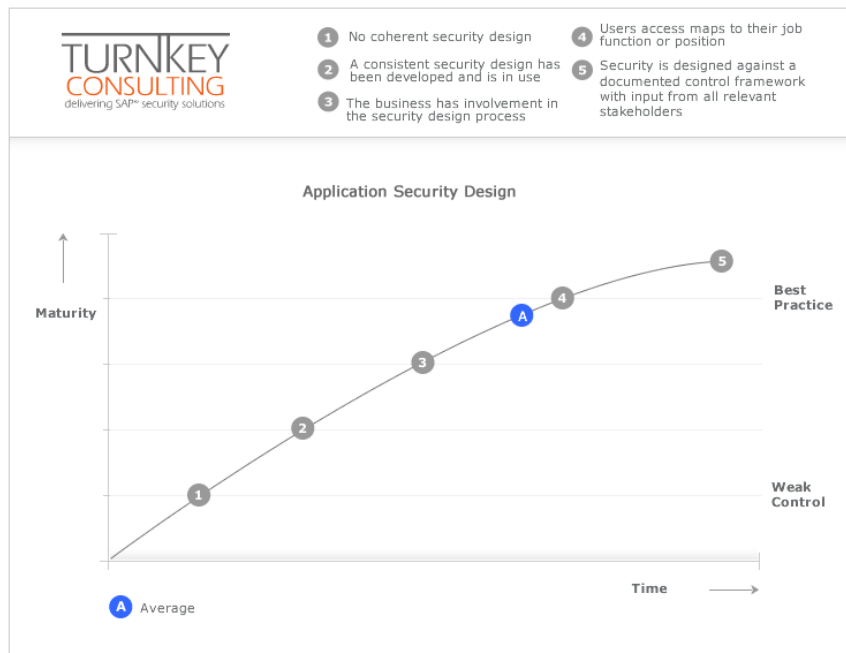
SoD review should be performed as part of the change management process to ensure that SoDs are not introduced by making what may appear to be minor changes.

Testing of all changes should be mandatory before they are promoted to production and should be a key part of the change management process.

Where the change process can be automated with appropriate checks and approvals, improvements in control will drive improvements in quality of service delivery.

Section 5: Application Security Design

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

The majority of organisations who took part in the benchmark have defined and documented authorisation designs. 65% of respondents have based their design on processes agreed with the business and can clearly map users access to their jobs or positions.

Only 39% of organisations have a risk register for their SAP application security, with a similar number being able to reconcile their control framework with preventative controls enforced by their SAP security design. Even fewer respondents believed that the business understands security.

Recommendations:

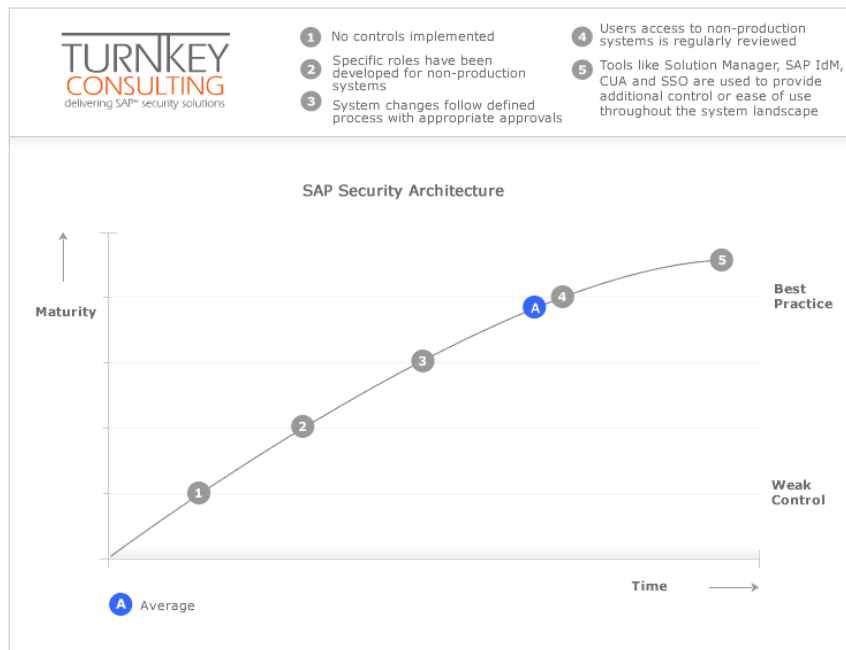
Business processes and risk frameworks are foundations of a security design. It is the role of SAP security to allow users to perform business process activities within the bounds of acceptable risk.

The risk framework or register should stipulate what restrictions are deemed to be important for the business processes operated by the organisation.

The business should be involved at all stages of security definition to ensure that the technical build meets their requirements. The security build should adequately reflect what users need to be able to do within SAP and should logically map to the jobs that users perform.

Section 6: SAP Security Architecture

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

The large majority of respondents have a multi-tier architecture supported by clear, documented change processes. In general, developments and customizations require management approval before they are deployed into the production environment/s

50% of organisations who took part in the benchmark use Solution Manager to help manage their environments, with a similar percentage using CUA and SSO to simplify user management and access to multiple systems.

Our results show that non-production access reviews are performed by 52% of respondents.

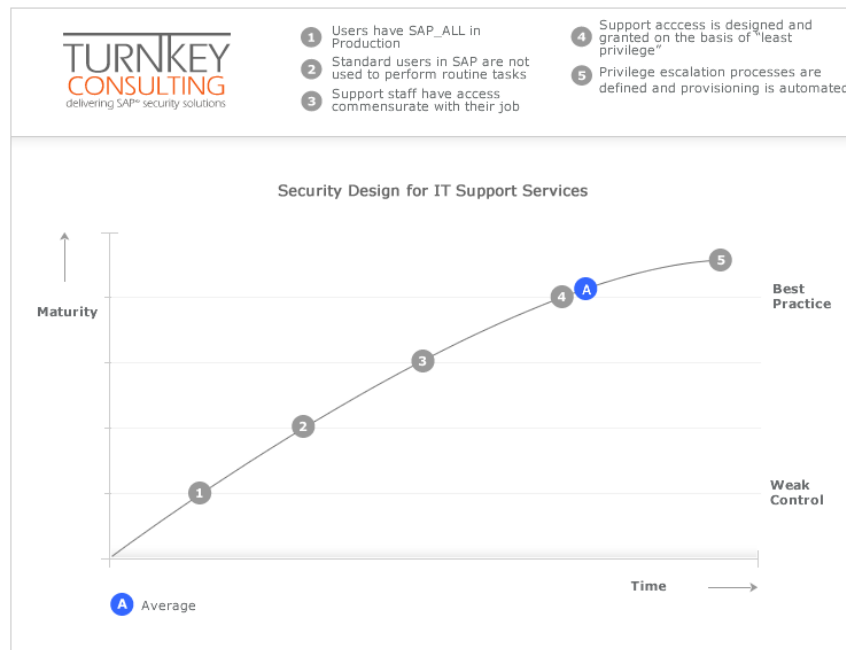
Recommendations:

As landscapes are growing increasingly complex, use of tools like Solution Manager can improve support and reduce the workload on system administrators. Self-Service Security Optimization can be run from within Solution Manager and can be used to highlight issues with security in connected systems and push out alerts where problems have been detected.

Access creep is a particular problem in non-production systems so it is important that users are reviewed periodically. Strong controls in the production environment can be rendered obsolete by activities which are performed in the non-production environments and can find their way into production.

Section 7: Security Design for IT Support Services

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

Our benchmark has revealed that 90% of respondents have defined roles for support staff, with the majority of them restricted to their appropriate functions. 58% of respondents reported that their support team were able to process business transactions.

59% of organisations have procedures in place for privilege escalation, of which half of them use a tool for the automation of privilege escalation.

Out of all the respondents, 28% have users with SAP_ALL or similar access in production and 19% regularly use standard users like DDIC and SAP* for routine support purposes.

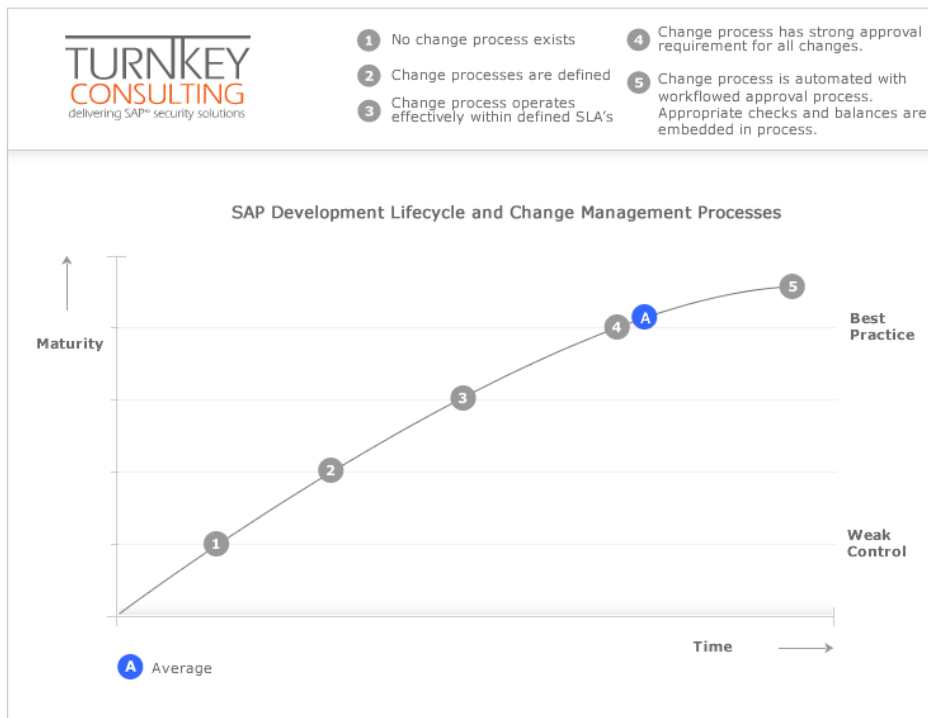
Recommendations:

Support users should have the minimum privileges required to perform their role. Outside of emergency situations, support users should not have the ability to process business transactions unless they have responsibility for those processes. The use of automated privilege escalation tools can strike the balance of restricting support users access for everyday tasks but also making available extended access for fire-fighting activities.

SAP_ALL type access should be removed from all users and replaced with more appropriate access aligned with users support activities. Standard users should also not be available unless specific circumstances mandate their use.

Section 8: SAP Development Lifecycle and Change Management Processes

Results:



The Turnkey Consulting maturity model is based purely on answers to our benchmark survey questionnaire.

Analysis:

88% of the respondents to our benchmark survey operate documented change processes which require strong approvals, are deemed effective and are adhered to by staff involved in the process.

66% of organisations have SLA's for their change management process that are measured and reported against.

At this point in time, only 48% of respondents use workflow approval functionality to streamline the approval process.

Recommendations:

Inadequate control in the change management process can lead to changes getting through to production that are inadequately tested and carry an associated operational risk. It is possible that malicious code could be transported or that controls within a particular transaction have been bypassed based on (mis)use of a user exit or enhancement point.

An effective approval process needs to incorporate adequate checks and balances to ensure the quality of the changes that are being sent to production. Streamlining the process by using workflow based approvals can help ensure that the additional control steps do not end up causing delays in the resolution of issues or deployment of new functionality.