

## SAP Access Control with Winterhawk

At Winterhawk, we have extensive experience delivering SAP Access Control to our customers with our accelerated deployment model. For more information, please contact us at [info@winterhawk.com](mailto:info@winterhawk.com)

More information on SAP Access Control can also be found [here](#).

## About Winterhawk

Winterhawk is the leading global SAP Security, GRC, Cyber and Data Privacy consulting practice. Supporting more than 2 million users worldwide, we are proud to be innovative, independent and cost-effective. Our services are complemented with domain expertise, software content, accelerators and toolkits that provide fast, efficient and expert implementation and support services.



# HOW TO BUILD A BUSINESS CASE: SAP ACCESS CONTROL

Winterhawk has designed this guide to equip you with the key financial and non-financial benefits of SAP Access Control which can be used when compiling your business case.

## What is SAP GRC Access Control?

Your business is accountable for the data it holds and who has access to it. SAP Access Control allows your organisation to automatically detect, manage and prevent access risk violations and reduce unauthorised access to company data and information.

Additionally, it allows for self-service driven processes to access request submission and workflow configured authorisations. Automatic reviews of user access, role authorisation and risk violations can also be used using the solution.

## SAP GRC Access Control is split into five key processes:

### 1. Analyse risk

- Comprehensive, predefined rule set available to analyse risk
- Ability to perform cross-system analysis for enterprise applications in real time or offline mode, to automatically remediate against access risk violations such as segregation of duties & sensitive access – across SAP and non-SAP systems
- Identify, remediate and mitigate access risks
- Simulate changes to identify and prevent new risks

### 2. Manage access

- Self-service, automated access requests
- Workflow-driven approval process
- Embedded risk analysis simulations to “stay clean” with compliance checks and risk mitigation
- Automated provisioning

### 3. Maintain roles

- Define roles in business terms and align with business processes
- Analyse and optimise business roles

#### 4. Certify authorisations

- Automated user-access reviews
- Certification of role content and assignment to users
- Automate review of mitigating control assignments

#### 5. Monitor Privileges

- Emergency Access management
- Review user and role transaction usage details
- Proactive notification of conflicting or sensitive usage & actions
- Dashboard and reporting



### Building a business case

#### Cost Avoidance

When it comes to security, business cases are often based around cost avoidance; for example, a store will invest in security and/or CCTV if the potential long-term cost of stolen inventory outweighs the cost of implementing CCTV & paying a security guard.

SAP Access Control helps organisations protect against internal, fraudulent & accidental data breaches and fraud and their associated costs (reputational as well as financial).

**Segregation of Duties** - a core audit requirement, designed so that a single point of compromise does not have significant impacts on the business. The risk being that if a single post is responsible for highly privileged actions and is not monitored or controlled, then compromise of that role could result in disastrous impacts to the organisation

**User and Role Privileges** - with the ability to easily identify who has access to which privileges and quickly understand the impacts of those privileges, the potential for data breaches and associated costs to the business (such as regulatory fines) are reduced.

**Rectifying Audit findings** - Audit findings need to be addressed and resolved at a cost to your business. With SAP Access Control these audit findings will be minimal and therefore costs to remediate will be avoided.

#### Cost Reduction

Do you employ a team of people to process user access requests across your SAP Landscape? Do they periodically audit users and roles to check for segregation of duty issues? Are you paying for security team members to assign emergency access late at night and over weekends to support projects and maintenance work? Do team members manually create security reports and dashboards for valuable management information? Do your security team spend time supporting planned or out of hours emergency access authorisations?

If the answer is “yes” to any of the above, in addition to a cost avoidance business case, there may also be a case on the basis of cost reduction.

Further examples of cost reduction opportunities with SAP Access Control which can be explored include:

- Automated user provisioning – eliminate the need for manual provisioning
- Remove the requirement for manual segregation of duty and sensitive access checks from within your security team
- Internal, manual audits and checks will be simplified and less resource intensive
- Automated access reports and dashboard will remove the need for manual creation

These scenarios can be worked out as a cost reduction and potential reduction in headcount / paid external resources or increased in resources availability to focus on value-added activities which cannot be automated, thereby driving up productivity.



#### Contact Us

For further information on implementation and support, or to discuss Winterhawk’s Rapid Deployment Services for SAP Access Control, please get in touch with Winterhawk: [info@winterhawk.com](mailto:info@winterhawk.com)