SAP Access Control Extended with Greenlight

Greenlight Access Violation Management (AVM) automates access risk monitoring requirements. AVM is the only solution that provides 100% transparency into the actual risks in SAP ERP which materialize by users with SOD access plus summarizes the information into a dashboard that shows the Financial Exposure of those risks.

## Automated Controls and Financial Exposure of Access Risks

Customers can quickly identify potential SOD risks in ERP. However, during the analysis and the follow on cycle of cleaning up users' access, users will be identified where access cannot be removed leaving SODs in the business environment. For those users, controls to monitor the SOD risks must be identified and implemented.

For all SAP customers who are planning to implement an SOD reporting solution, providing transparency to actual SOD violations with AVM can fast track a customer to SOD compliance by moving from theoretical risk reporting to actual SOD exception reporting. This transparency is facilitated by automating compensating controls to correlate SOD events transacted in SAP ERP, and binding those events to the users providing 100% transparency to provide required mitigation. Without automation of the mitigation control, business owners are tasked with reviewing several reports and correlating data across those reports to see if the same user performed SOD transactions. The business owner then needs to provide proof for each control period that the manual activities were performed. At the time of review the business owner may have found that there were no SOD exceptions for that period or may have found several exceptions. Regardless of the findings, the business owner must do all the manual activities, document findings for exceptions found and keep proof for any upcoming audit. This is an onerous task that many times is ignored due to the level of effort required to do manual reporting and monitoring.

Business Benefits of access management automation include:

- Reduce the cost of compliance

WWW.GREENLIGHTCORP.COM

- o Removes manual activities required by all key stakeholders in the organization.
  - ▪ Notifies the business when there is an exception vs. business owners reviewing reports on a manual basis to identify if there is an exception
  - ▪ Provides audit and compliance personnel with an independent system of record that can be viewed on-line at any time to determine business review is being completed
  - ▪ Provides management with confidence that exceptions are identified, investigated and exception cases are closed
- Decrease the risk profile of an organization
  - o Provides an enterprise view that associates real dollars to access risks that enables the business to focus on access violations which pose the highest risk to the organization
- Increase scope of audit while reducing time/resources required
  - o By integrating critical business applications to GRC, non-ERP systems can be monitored through automation vs. adding more manual activities per system
- Provide ROI to the business through GRC
  - o Allows business owners to focus on day to day business activities.
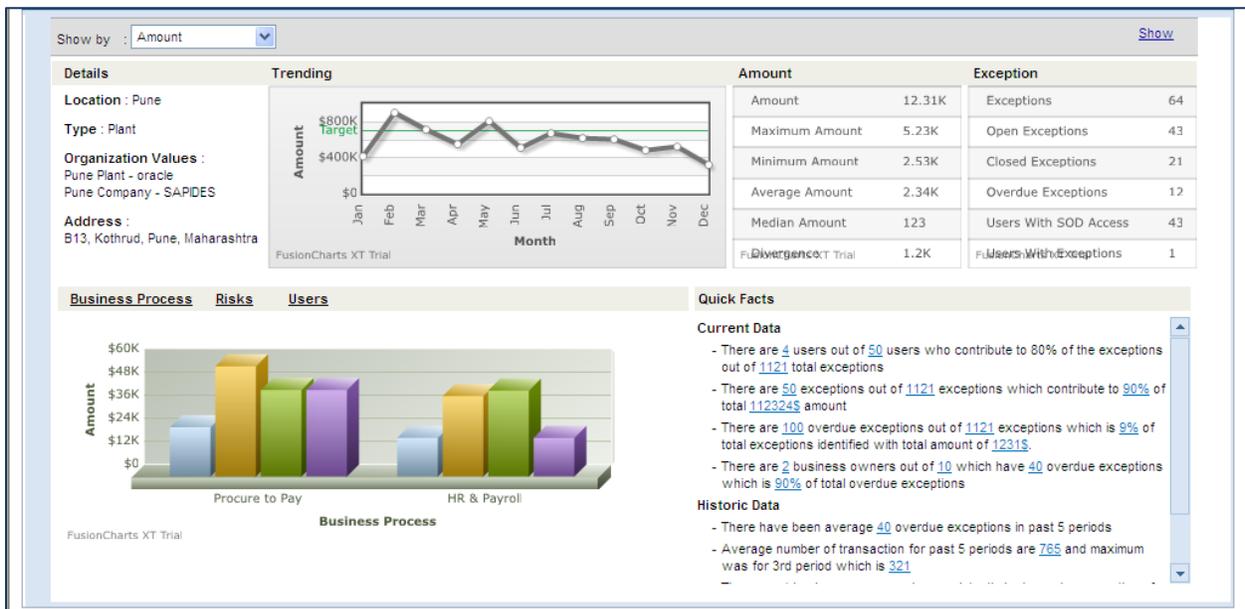
Together, SAP Access Control and Access Violation Management provides business stakeholders with visibility into the actual bottom-line or financial impact that risk has on the organization. This is a unique differentiator that shows
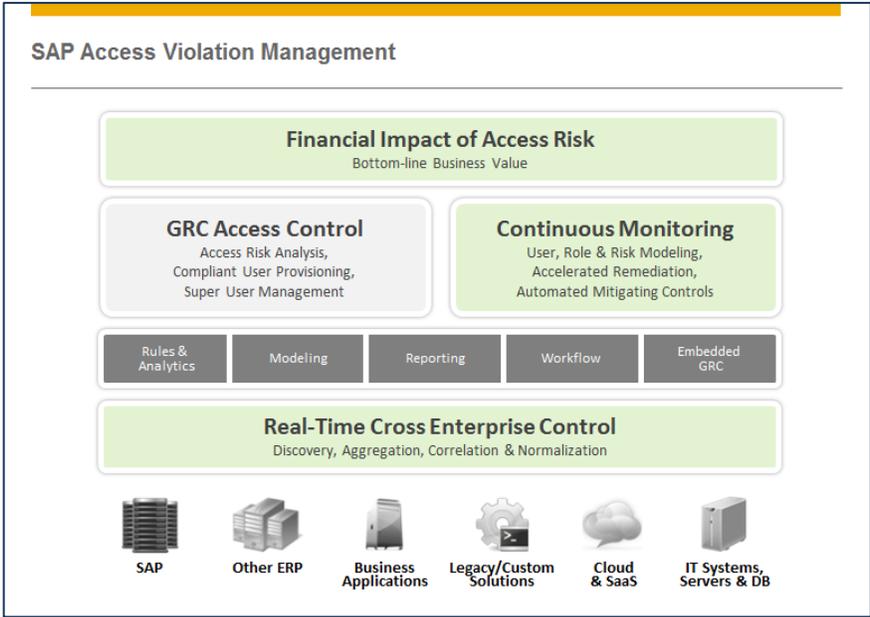
Greenlight TECHNOLOGIES

270 S. Main St., Flemington, NJ 08822
T +1-908-782-5700 F +1-908-782-5763
E info@greenlightcorp.com

WWW.GREENLIGHTCORP.COM

true benefit in business terms instead of just as an output for audit and compliance. Summarizing the actual SOD risks into a financial exposure view by company, division, and/or geographical location provides the transparency to business owners, compliance and management of exactly what impact the access risks pose to the company. This allows the business to prioritize where to start or where to focus their efforts based on the likelihood and impact of access risk.

Enterprise Access Risk Governance

The joint SAP Greenlight solution allows the ability to expand the strategic investment in GRC to enable an enterprise-wide approach to continuous access controls monitoring across all business processes regardless of the target applications. This provides the only solution for leveraging an organizations strategic vision of using SAP GRC by extending the business value derived from SAP Access Control to other ERP applications, best in class business applications, custom or legacy solutions and cloud-based offerings.

Greenlight enables the access governance processes for all enterprise systems to operate in the same manner as they would for SAP. The integration and the underlying complexity of the different systems will be transparent and all enterprise systems can be included in your standard processes, such as periodic scans, preventative controls for simulation and compliant provisioning, and workflow approvals.

For example, Procurement activities can be carried out in Ariba while all other activities such as Supplier Maintenance, Receiving Goods and Accounts Payable all are conducted out of SAP or potentially even other best of breed solutions. This means that your Procure to Pay business process spans multiple applications and may not be reviewed completely from start to finish in order to monitor for errors or fraudulent activity which could result in cash leaks, overpayments, double payments, etc. A few example risks we help our customers with today include:

- Create a fictitious vendor and initiate purchases to that vendor
- Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor
- Approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order
- Reconcile Purchase Order Amount or Contract Amount variance exceptions and send payment to Vendor

Business Planning and Consolidation can be used for everything from General Accounting and Journal Maintenance to Periodic Consolidation and Planning or Budgeting. Given the sensitivity of these activities there are single system critical access risks to be monitored natively in BPC as well as cross system risks with SAP or any other ERP General Accounting module. A few examples include:

- Ability to edit journals and post the same journals
- Ability to post or un-post journals and run report for the same
- Edit Dimension under ACTUAL & BUDGET
- AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access combined with the ability to modify ECCS hierarchy and reporting output

AVM allows companies to extend SAP Access Control functionality across business applications for real-time risk analysis and compliant provisioning. This provides the ability to embed compliance into day to day processes and gives end users and stakeholders a unified, consistent and efficient approach to manage access compliance including access requests, automated mitigation controls and periodic user access reviews.

Access Violation Management is sold by SAP as SAP Access Violation Management by Greenlight

Greenlight
TECHNOLOGIES

270 S. Main St., Flemington, NJ 08822
T +1-908-782-5700 F +1-908-782-5763
E info@greenlightcorp.com