SYMMETRY
Managed ERP & Cloud Hosting™

CONTENTS

Selecting a Solution

Defining Emergency Access Processes

Conclusion

Is Your SAP Emergency Access Process Cutting It?

The vast majority of organizations leveraging SAP as a business critical application have a requirement for some form of emergency access. Inevitably there will be situations where key IT resources, business users or even external consultants and software vendors require temporary enhanced authorizations to the SAP environment. It is absolutely essential to define a process that both satisfies the business need but more importantly is compliant and easily auditable.

Whether automated via a 3rd party solution or manual, there are key controls required to ensure this process is an asset to the organization and doesn't become an audit deficiency. This article will focus primarily on the selection and definition of a sound process and a few key items that if not in place can turn a good process bad. This is not intended to be a technical implementation guide.

Selecting a Solution

As with any business critical decision, it is imperative to take the time and evaluate potential solutions prior to jumping in. There is no doubt that standard SAP functionality can be used to develop a process that works, however, many of the items discussed later will not be conducive to a manual process. Not to mention the time and effort involved to sustain and audit this process would likely be recouped within your first year of implementing a 3rd party emergency access solution such as ControlPanelGRC's Emergency Access Manager (EAM).

ControlPanel GRC®

Key items to consider while performing your review to select a solution:

Overall return on investment – quantify time and effort spent assigning temporary access to Users, provisioning "emergency ID's" and most importantly auditing your process

■ Time and effort to implement – ControlPanelGRC's EAM solution installs and implements in under 2 weeks saving consulting dollars and time.

■ Ease of use – It shouldn't require a PhD in SAP to use or manage your emergency access process. Selecting a tool that requires little care and feeding, automated reporting and a streamlined workflow is key.

■ Flexibility – Not every organization is the same. Different organizational requirements can dictate a need for a greatly differentiated emergency access solution. ControlPanelGRC's EAM Solution contains a vast array of easily customizable options including the ability to use different approaches based on the specific scenario.

■ Auditability – One of the most critical success factors to an EAM solution is the ability to audit the tool. (i.e. who has access to activate, who are my Owners, are log reviews occurring, what transactions are being executed, etc.).

Overall there are a number of emergency access solutions that can be used. The majority of solutions contain similar functionalities, however, a few like ControlPanelGRC Emergency Access Manager have key differentiators that may go above and beyond in making a solution right for you.

Defining Emergency Access Processes

Regardless of your EAM solution selection, defining sound processes and controls are an integral piece of this exercise. Too often organizations get it wrong when developing their own emergency access processes or even during the implementation of a 3rd party product. There are key success factors that should be in place for any emergency access implementation, and forgetting these can ultimately lead to deficiencies.

1. Identifying the Need

Let's start by evaluating the overall need for emergency access. Unsurprisingly, different areas within the organization will require different access within SAP. To that same point, the ultimate goal of an emergency access solution is to provide a resource with access they would not normally have as part of their job. This need can ultimately stem from a number of different reasons, not limited to the ones specified below:

■ IT Support Resources may periodically require access to process functional transactions

■ Users otherwise limited to display authorizations need the ability to change data within SAP

■ Providing backup support for colleagues or supplementary support for a smaller department

■ Means to remediate Segregation of Duties (SOD's)

■ Granting access to SAP support personnel or consultants that may not otherwise regularly interface with your SAP system

Each of the reasons above may ultimately dictate the need for a different type of emergency access scenario. Defining and mapping these use cases for your organization is a necessary piece and facilitates the scope of your emergency access implementation.

2. Defining Scenarios

Next we need to review what type of access these various scenarios will require inside of SAP. There is a strong argument for still using access rights model within your emergency access solution, however, it is import not to be too restrictive so you avoid inhibiting your solution that is intended to be the answer for enhanced authorization requirements. As such, it is recommended to evaluate the needs and translate them into a tiered model similar to the following:

Exception Based Access

This type of emergency access scenario would generally be reserved for highly auditable items where additional visibility and control is required. This could be access to critical processes surrounding the modification of posting periods, administration of client settings and potentially user administration. Exception based access should ultimately be split into individually defined scenarios to further differentiate the process and enable more granular assignment.

Standard Emergency Support

In this scenario we would define individual business areas or job functions that may require additional access inside of SAP. The individual access that is granted to these scenarios can differ greatly by organization. As an example, we may have separate emergency access scenarios for Security Administration, ABAP Development, Configuration, Application (full functional access), etc. We could choose to become slightly more granular and create scenarios based on module area or even specific job functions. (Example: Order to Cash, Procure to Pay, etc.)

Critical Emergency Support

These are instances where more broad access similar to SAP_ALL will be required in an SAP system. In general there should be very few users that have the ability to activate this emergency access scenario, and there should be more stringent controls surrounding the use, monitoring and auditing.

Now that the individual scenarios are defined, there are a number of attributes that must be evaluated. Some of the below items may or may not be available given the selected emergency access solution. *(Any feature noted below is standard functionality in the ControlPanelGRC EAM tool).*

■ Who are the specific users within the organization that require one of the aforementioned scenarios?
   Note: It's quite common to initially roll out an emergency access solution to only IT support staff and later expand into the business.

■ What type of documentation will we require upon activation of the emergency access session?

■ Does a specific emergency access scenario require approval prior to the activation or would this scenario be considered "pre-approved" for those users enabled to use it?
   Example: We may provide our key SAP basis resources the ability to activate the emergency access scenario that allows client administration, however, each attempt to activate may route a workflow request to the owner for review and approval prior to activation.

■ Is there any additional logging outside of the transactions/reports executed, standard SAP change logging or table change login required for a given scenario
   Example: By default it is fairly standard to monitor which transactions/reports are executive during a session along with SAP change documents and table/view changes. Do we want to go even further and harvest SAP statistical records or system log entries?
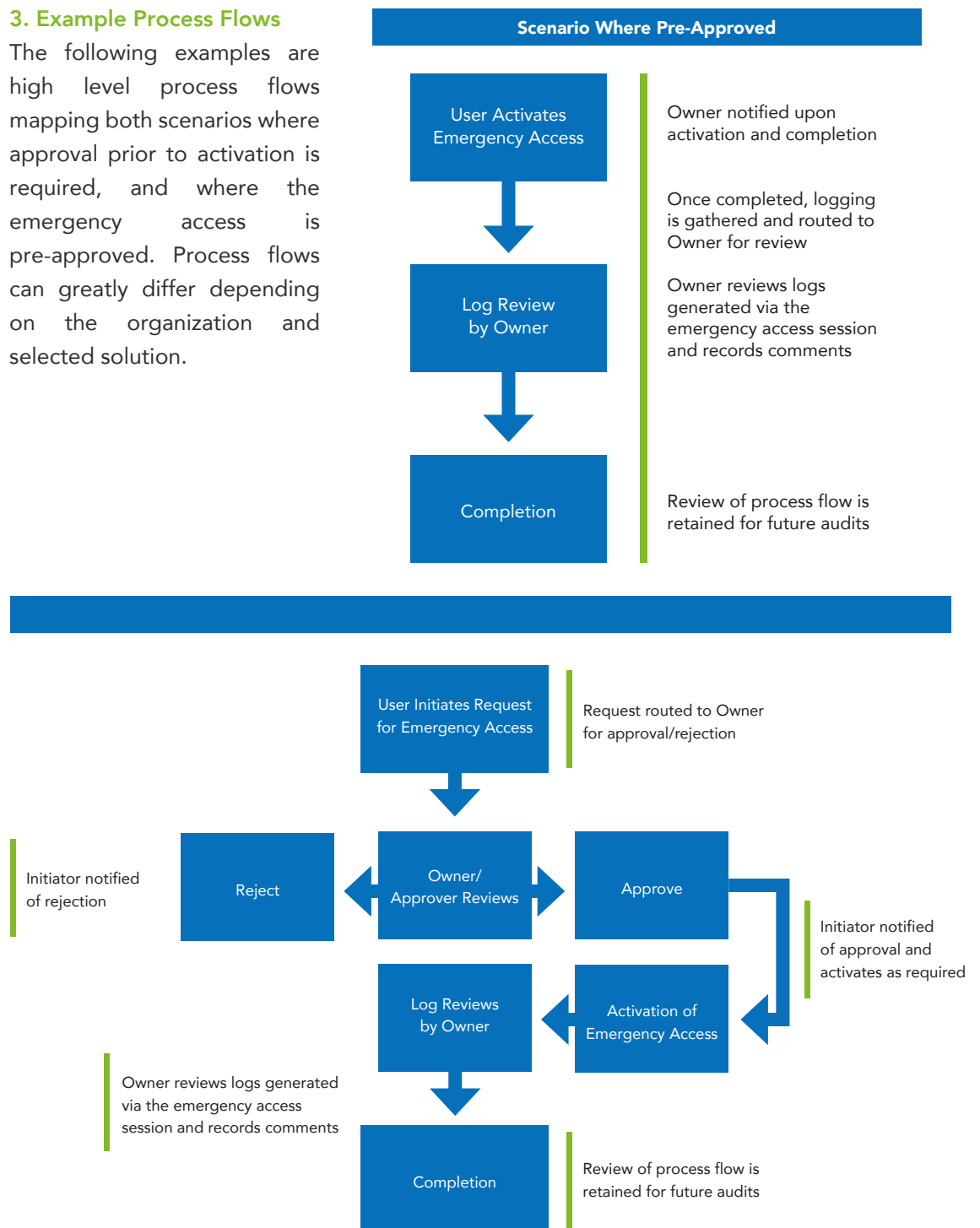
- Does a given emergency access scenario require a time limit?
  Example: By default an emergency access session is only active during that physical log on to SAP, however, is this critical enough that we should be limiting the users to 60 minutes with a certain amount of allotted extensions?

- What type of log review is required? Should we require only a passive email log review or will we require a documented review in workflow?

3. Example Process Flows

The following examples are high level process flows mapping both scenarios where approval prior to activation is required, and where the emergency access is pre-approved. Process flows can greatly differ depending on the organization and selected solution.


Scenario Where Pre-Approved

User Activates Emergency Access → Owner notified upon activation and completion

Once completed, logging is gathered and routed to Owner for review

Log Review by Owner → Owner reviews logs generated via the emergency access session and records comments

Completion → Review of process flow is retained for future audits

User Initiates Request for Emergency Access → Request routed to Owner for approval/rejection

Reject ← Owner/Approver Reviews → Approve

Initiator notified of rejection

Initiator notified of approval and activates as required

Log Reviews by Owner ← Activation of Emergency Access

Owner reviews logs generated via the emergency access session and records comments

Completion → Review of process flow is retained for future audits

Is Your SAP Emergency Access Process Cutting It?

4. Auditing the Process

An emergency access process is not complete without developing a plan for auditing the process. Many organizations stop defining their process once they have achieved their main goal of granting the SAP Users their enhanced authorizations. Far too many organizations end up with audit deficiencies because they miss critical steps in defining their emergency access solution.
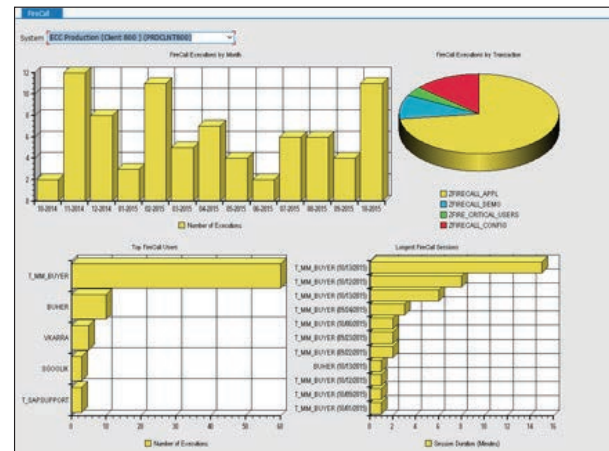
Example Graphical Dashboard from ControlPanelGRC Emergency Access Manager

Below is a list of requirements when it comes to emergency access in SAP:

■ Similar to standard SAP Security, a periodic reaffirmation of authorizations available to your emergency access scenarios is required.
The frequency of this review can differ between organizations, however, should occur at least on an annual basis.

■ Review of Users that are able to activate each emergency access scenario for appropriateness.
Resources frequently move throughout the organization or come and go. As such, a periodic review of users with access to each emergency access scenario should be reviewed periodically and adjusted accordingly. Assuming the solution contains built-in reporting that can facilitate a quick and painless review, this should be something that can be performed on a quarterly basis.

■ Review of owners/reviewers who are approving and reviewing emergency access logs.
Similar to the item above, it is imperative to perform a periodic review of these owners. There should be no reason this review cannot coincide with the control above.

■ Review of users with high volume and frequency of emergency access execution.
This is frequently overlooked, however, can be a good resource for identifying issues with the current SAP security design requiring users to rely too heavily upon emergency access to perform their job. This can also help point out users that ultimately are not following the designed process, and only leveraging emergency access when required.

■ Periodic monitoring of the emergency access log reviews to ensure appropriate and timely reviews are being performed.
Over the last year this has become a more prevalent topic and untimely reviews of

For more information, please contact our Business Development Department at:

www.SymmetryCorp.com

salesinfo@symmetrycorp.com

888-796-2677

———————

Symmetry

400 South Executive Drive

Brookfield, WI 53005

Is Your SAP Emergency Access Process Cutting It?

of emergency access logs have resulted in audit findings. With that said, it is critical that these logs be reviewed as close to generation as possible. (Generally speaking 1 to 2 weeks after creation). The more time that surpasses between the log generation and review the more this can become a rubber stamp, and the more likely it becomes that an inappropriate action generated during emergency access is missed.

Conclusion

Management of emergency access within SAP is an integral process that ultimately starts with the selection of a solution. Whether through SAP standard or a 3rd party solution such as ControlPanelGRC Emergency Access Manager, if done properly your emergency access solution can become an incredibly beneficial asset. Automation can alleviate the potential for human error and ultimately free up SAP security and basis resources to perform more value-add activities within the organization. There are a number of procedural decisions and considerations that need to be made in order to facilitate the roll out of a scalable, sustainable and auditable solution.

It is essential to spend the time in the beginning to identify the needs for emergency access through the definition of use cases, construction of the various scenarios and ultimately ensuring your process is auditable. ∎