



## Case Study: How Abiomed Reduced the Time, Expense, and Effort Associated with Sarbanes-Oxley Reporting

Sharon Kaiser, Chief Information Officer – Abiomed Corporation

Scott Goolik, Chief Technology Officer – SymSoft Corporation



Professional Solutions for Compliance Automation

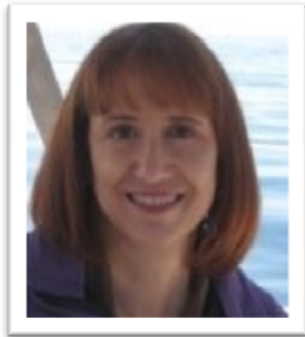
[www.ControlPanelGRC.com](http://www.ControlPanelGRC.com)

## Introducing

---



**Scott Goolik**  
Chief Technology Officer  
SymSoft



**Sharon Kaiser**  
CIO  
Abiomed

## What We'll Cover ...

---

- Exploring Abiomed's journey and challenges
- Defining key preventive and detective access controls
- Leveraging key controls over emergency access and SAP transports
- Evaluating how Abiomed helped ourselves through automation
- Wrap-up

## Who Is Abiomed?

- Publicly traded firm on New York Stock Exchange
- Medical Device manufacturer headquartered in Massachusetts with additional facility in Germany
- Over 350+ employees
- Experts in Pumping Blood for over 25 years
- World's smallest heart pumps for cardiologists and surgeons
- Over 200 patents or patents pending from over \$200m in R&D
- Over 12,000 patients supported in over 40 countries worldwide

- 2010 Impella® 2.5 >3500 patients and in over 450 hospitals in the U.S.
- 2009 Impella 5.0 available in U.S. for broad clinical use
- 2009 AB Portable™ driver FDA approved & first patient discharge
- 2008 Impella 2.5 FDA cleared in U.S. for broad clinical use
- 2005 Impella Available in Europe
- 2001 First AbioCor Artificial Heart patient
- 1992 First FDA approved VAD
- 1987 First heart recovery patient
- 1981 Abiomed Founded

## We Have a Story to Share

---

- We are a relatively small company but we are required to be SOX compliant
- It is important to us to be cost efficient, but effective
- Specifics of Abiomed's SAP Landscape:
  - One instance of SAP ECC 5.0
  - Over 350 users in the US, Canada and Europe
  - Utilize SAP FI/CO, MM, PP, SD, HR, QM, DMS, SM
- We recently re-evaluated how we want to define and manage our SOX compliance

## The Beginning

---

- Hired an outside auditing company for an initial SOX assessment
  - Looked at 139 different review items
  - Resultant gap analysis showed Abiomed was at risk in several areas
- Next step was to put together a project plan to:
  - Conduct business and financial risk assessment
  - Identify key controls for each major risk area
  - Create a control matrix for only the KEY controls and develop the associated test plan
- Result was 69 initial IT General Controls and 26 IT Application Controls

## Decision Made to Outsource Compliance Assistance

---

- Wanted Abiomed management to focus on core competencies
- Wanted a high level of control expertise and best practice input
- Wanted to provide ability for knowledge transfer to build Abiomed personnel experience and expertise
- Would only pay for hours expended
- Actual external auditors could rely more on testing conducted by independent third party with controls and information technology expertise
- Acted as a “Pre-Audit” to identify compliance gaps to be addressed before external auditors review

## Pre-Audit Approach

---

- External firm would provide:
  - Planning and assistance in Abiomed's SOX compliance efforts
  - Assistance to help management review and validate key controls and look for efficiencies in the overall SOX effort
  - Resources to perform actual key control testing
  - Reporting results and status updates, including tracking of test exceptions
  - Assistance to management to evaluate test exceptions and determine whether deficiencies represent significant deficiencies or material weaknesses

## Early Pre-Audit Results

---

- First audit identified 9 deficiencies, including:
  - Excessive access by IT in a key financial system
  - Authorizations were not reviewed and updated for a manager that changed jobs
  - Lack of consistent documentation for things like:
    - Remote or system access
    - Computer use policy sign-offs
    - Terminations checklists
- Although testing revealed no inappropriate actions were performed and access given was appropriate, gaps were identified where Abiomed was not managing to controlled processes for documentation

## Early Audit Lessons Learned

---



Caution

- Be diligent in what you define as a control – remember the goal is to identify risks associated with the accuracy and timeliness of financial reporting
  - Many were things that a good IT department should do as best practice
  - Focus on relevant controls for your organization
- Business and IT needed to organize and manage to defined policies
- New processes needed to be defined to handle things like personnel role changes and impact to authorizations
- Training was important for people to understand their role in SOX compliance

## Abiomed's Situation in Late 2009

---

- Original Abiomed roles were taken from generic SAP defined roles and needed to be customized to fit our specific business needs
- Risk management was identified as a high priority by Abiomed's Controller
- After years of bottoms-up SOX controls, we wanted to focus on more top-down, broader risk-based controls
  - Reduced our controls from 69 IT General Controls to 12 very key controls
- We turned our attention to evaluate affordable automation options that could help in three major areas
  - Cost Reduction and Efficiencies
  - Risks and Mitigation
  - Compliance & Reporting

## Abiomed's New Challenges

---

- As a small company, we were challenged to identify and manage excessive controls and SOD (segregation of duties) issues on a global basis – US and Europe
- Most of our IT general controls were managed manually and tested manually
- Information was available, but limited and difficult to access, making compliance reporting labor intensive, both for IT and for our business partners
- Our limited IT staff has to be knowledgeable of, and stay on top of, IT SOX controls on a daily basis
- A substantial amount of IT time is required, in a short period of time, to prepare for and support the SOX audits

## Example of Excessive Controls

---

- Initial SAP implementation had a role defined that allowed a wide variety of material movement codes
  - No one person was accountable for inventory accuracy
  - Many initiated transactions without understanding the implications to inventory
  - Limited visibility to review the transactions before they were executed
  - Finance was repeatedly making correcting adjustments to properly state inventory

## Project Approach

---

- Project initiated to restrict usage of movement codes
- Specific roles would be based on the job a person performed – quality inspector, shop floor clerk, shipping clerk, stock room, etc.
- One all-encompassing role became 17 distinct roles
- Each new role would allow a person to perform only what they needed for their job
- Extensive testing was conducted to verify security and product movement and inventory accuracy
- This was a very manual intensive effort that took over 3 months to research, design and test – would have been much easier with an automated tool

## Benefits of Resulting Role Segregation

---

- The project provided training so people would understand the system impact of each transaction
- Metrics were developed to monitor activity
- Controls have improved so significantly that Abiomed is now exempt from periodic physical inventory counts, providing a reduction in cost
- There are now increased efficiencies in daily inventory transactions, especially in shipping and receiving
  - For example, actual product movements were moved closer to the area of accountability.

## Factors Influencing our Need to Automate

---

- Difficult times always present opportunities
- We wanted to drive process improvements
- Automated processes are deemed more trustworthy than manual processes
- We wanted to automate repetitive tasks to drive efficiencies
- We wanted to reduce time spent by control owners, process owners, IT security, and administrative personnel
- We wanted to free up our staff to do more strategic activities through value added activities

## Goal 1 – Cost Reductions and Efficiencies

---

- Objectives:
  - Improve the efficiency, time and expense associated with audits
  - Automate data gathering, monitoring and reporting
  - Automate and streamline processes related to User/Role Maintenance and SAP Transports
- Challenges:
  - Some audit requests required data reconstruction
  - Audit test data requests had to be pulled manually and were highly labor intensive
  - Quarterly access reviews had to be compiled and distributed manually, requiring constant and repeated follow-up to obtain approvals

## Goal 2 – Risks and Mitigation

---

- Objectives:
  - Eliminate potential audit risks due to complex user access requirements
  - Consolidate data and processes
  - Provide more efficient and timely review of SAP emergency access and super roles
- Challenges:
  - Some functional owners didn't understand the content of the SOD reports or the purpose of their review
  - Change management transports required routing and approval from multiple business owners
  - Emergency access review was conducted monthly by manual review – too late to really question or prevent abuse

## Goal 3 – Compliance & Reporting

---

- Objectives:
  - Ensure Abiomed is meeting compliance requirements
  - Automate monitoring and reporting
  - Move to exception based reporting
  - Provide on-line, on-demand reporting and review capability
  - Provide more information, with higher value and less work
- Challenges:
  - Native compliance reporting in SAP difficult to obtain, usually requiring reformatting and manual compilation
  - Data was for the most part available, but hard to find, extract and report

## Solution Requirements

---

- We wanted one solution to meet all of our needs that integrated smoothly with SAP
  - Abiomed required:
    - SOD and sensitive authorization analysis
    - Tracking & reporting of actual system usage
    - Automated change request process via workflow, with audit trail
    - Automated workflows to optimize security administration
    - Temporary authorization and tracking to troubleshoot production issues
    - Automated execution and delivery of compliance reports
    - Central scheduling and monitoring of batch jobs

## What We'll Cover ...

---

- Exploring Abiomed's journey and challenges
- Defining key preventive and detective access controls
- Leveraging key controls over emergency access and SAP transports
- Evaluating how Abiomed helped ourselves through automation
- Wrap-up

## Stakeholder Involvement

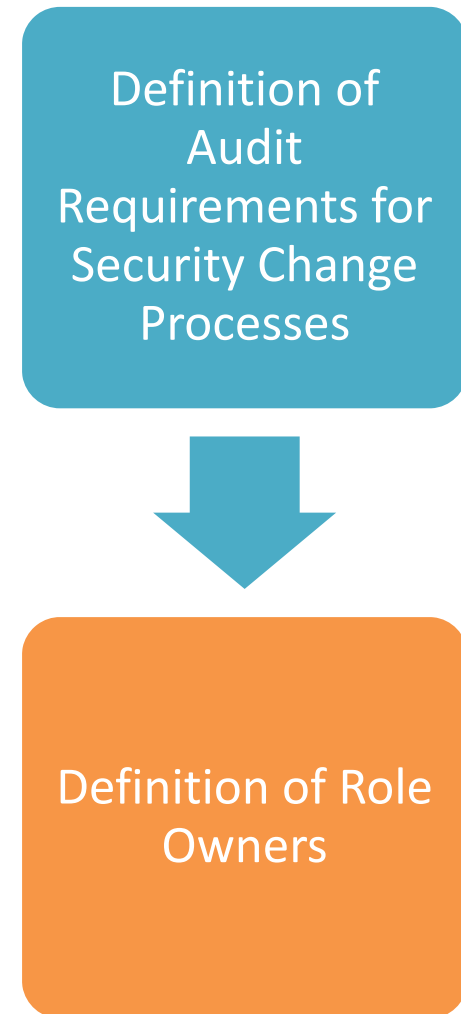
---

- Our internal auditors wanted stakeholders to be involved in approving security assignments
  - Role Owner Approvals required for all security changes
    - Who are our Role Owners?
  - Segregation of Duty checks required for both User and Role Changes
    - SOD Analysis for Role change must also consider Users assigned to the Role in Production
- Needed a process that could be audited at anytime without a huge amount of preparation by IT

## Definition of Role Owners

---

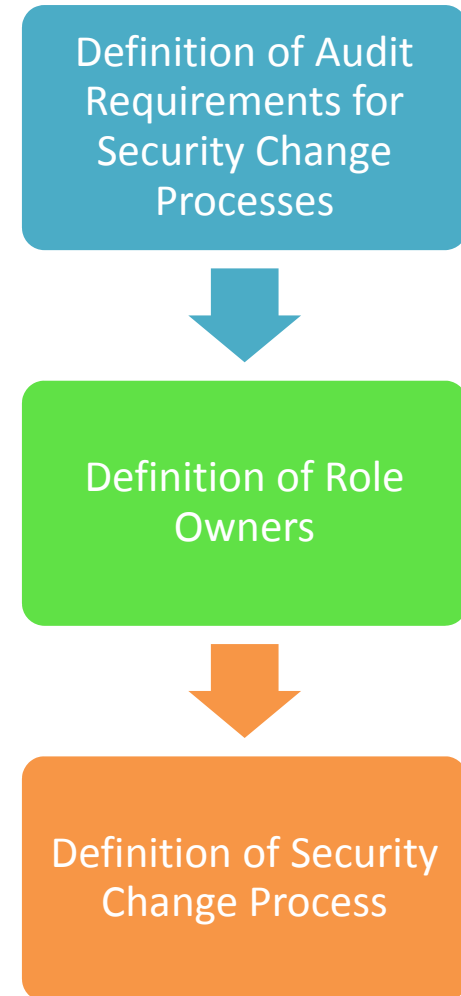
- Role Owners are responsible for approving assignment and definition changes to Roles
- Global Role Owners are responsible for the Transactions that are available in Roles
  - Derived Roles – US “Master” Roles with European versions that are linked
- Local Role Owners are responsible for the assignment of Roles to Users
  - Managers at each location better know the local employees for approval
- Role Owners defined as Department Heads
  - VP of Manufacturing, VP of HR, VP of Finance, etc.



## Definition of Security Change Process

---

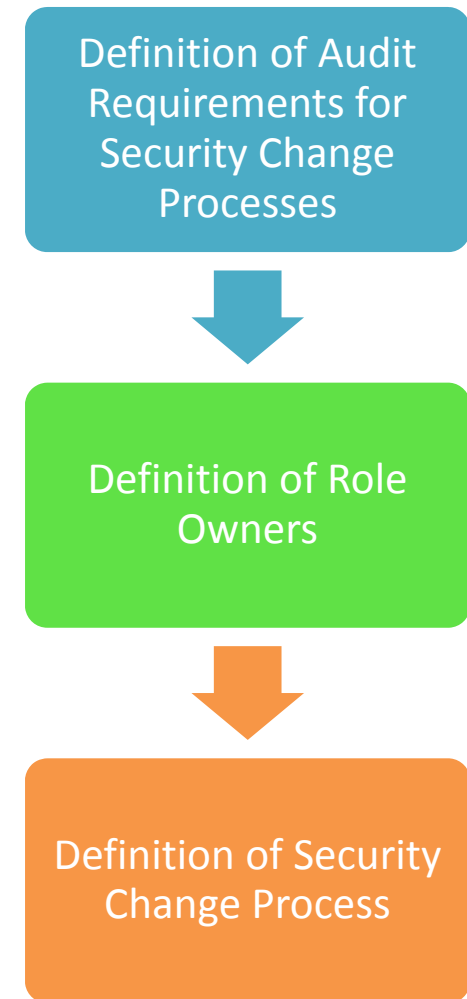
- Request Initiation Scenarios
  - Help Desk receives call and creates request
  - IT Support personnel creates request
  - Employee is hired and automatically provisioned to “default” Roles
- Request must be approved by Role Owners
  - Segregation of Duty checks are automatically executed during approval
  - Role Owner makes final decision on assignment of SOD Risks



## Definition of Security Change Process (cont.)

---

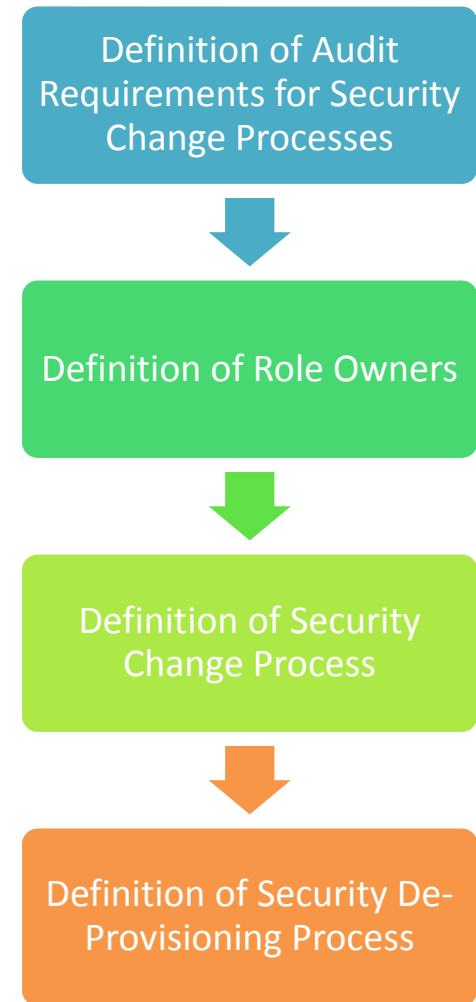
- Request forwarded to Security for review and processing
  - Automatic provisioning of User changes
    - Changes processed timely for our European locations
  - Manual implementation of Role changes
    - Integrated Transport Management for Role changes
- Communication back to requester that the change is complete



## Definition of Security De-Provisioning Process

---

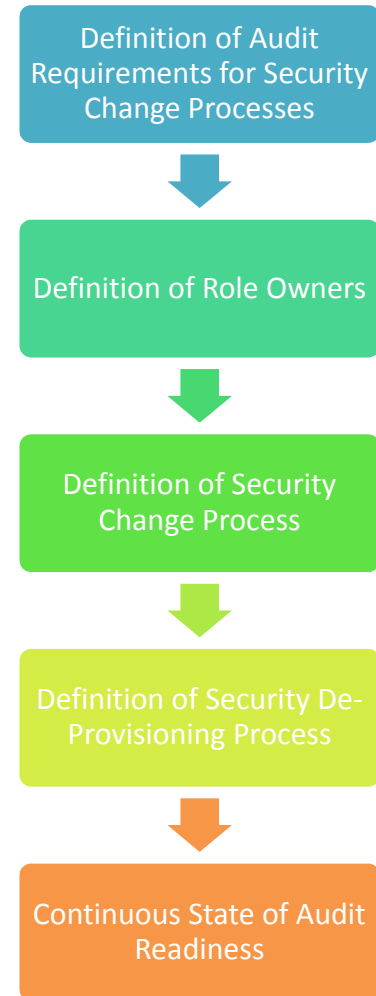
- All Employee Logons are tied to Employee Master Records in SAP ERP HCM
  - Nightly process identifies terminated employees and compares to current Logons
  - Automatic de-provisioning for terminated logons
- Non-Employee Logons are addressed with Detective Access Controls



## Continuous State of Audit Readiness

---

- We are always ready for the auditors!
- All approvals are captured in our workflow
- Auditors identify User or Role change sample and we can easily provide supporting documentation



## Authorizations Monitoring

---

- Our auditors wanted us to monitor authorizations on a periodic basis to ensure ...
  - Segregation of Duty issues are in check and not expanding
  - Sensitive Authorizations are properly assigned to appropriate individuals
  - Powerful Roles and Profiles are properly assigned to appropriate system logons and not available to normal dialog users
  - Inactive Users and non-Employee logons are being monitored
  - User access is current and reasonable

## Our Internal Auditors Have Defined a Number of Risks ...

- SOD, Sensitive Authorizations, Powerful Roles and Profiles, Valid Users, etc.
- We are a lean and mean shop, so manually running, compiling and reviewing these reports wasn't a viable option
  - Our security team defines reporting processes to mitigate potential risks
    - Needed to be easy to understand – we don't have a master's in SAP security!
  - Reports are automatically executed on a monthly basis and pushed to Control Owners



## Report Review Bolsters Readiness

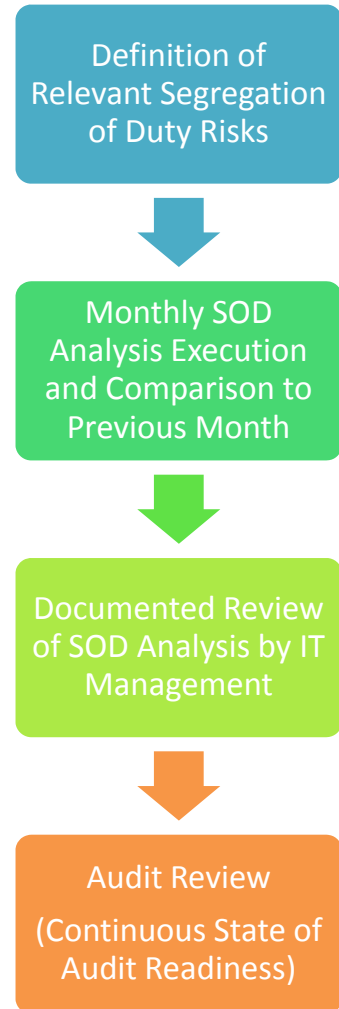
- Most reports are routed to IT Management for review in documented workflow
  - Occasional follow-up may be required with managers of other departments
  - Any exceptions are noted in workflow
- This puts us in a state of continuous audit readiness!
  - Auditors can review the control execution and related sign-offs in workflow at anytime



## Segregation of Duties (SOD)

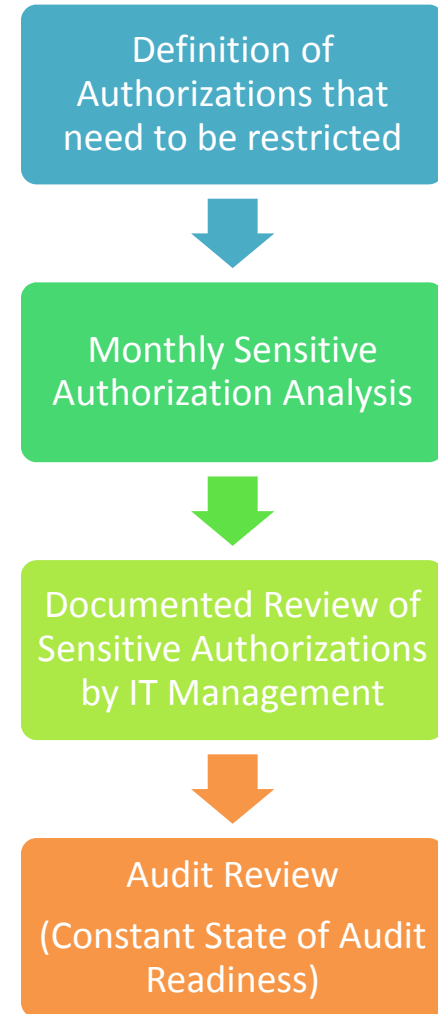
---

- Internal Auditors validated which SOD risks were of importance in our business
  - Emphasis placed on procurement and financial processes
- Risk analysis are executed on the first of each month and compiled as a “delta” analysis to detail changes from the previous period
  - Saves time by spelling out new risks



## Sensitive Authorization

- Internal Auditors identified specific Authorizations that they did not want to see assigned to end-users or IT support personnel
  - Ability to maintain configuration, workbench objects, number ranges, Roles or Profiles, client settings
- Sensitive Authorization analysis is executed on a monthly basis
- IT Management review ensures that any exceptions are addressed in a timely basis
  - Clear definitions of Risk – easy to understand



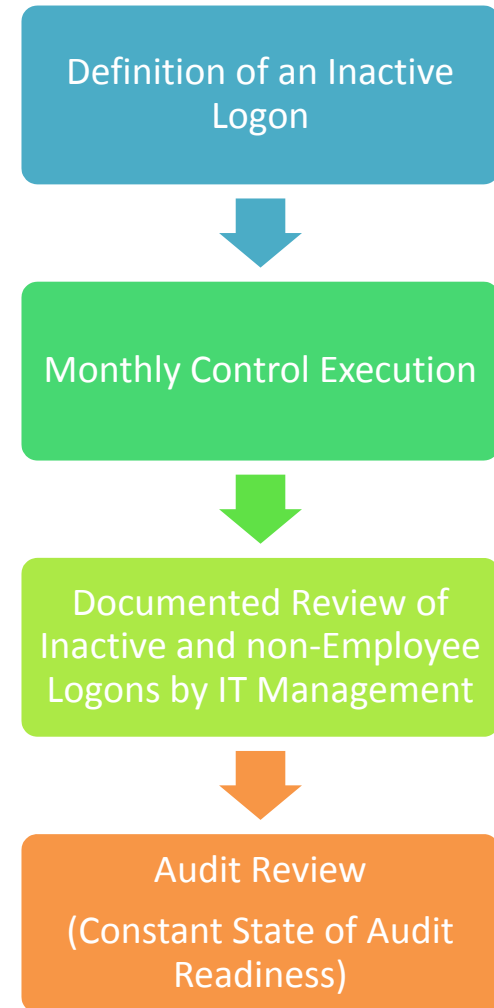
## Sensitive Roles and Profiles

- Internal Auditors identified specific Roles and Profiles that should be assigned to limited personnel
  - SAP\_ALL, SAP\_NEW, other powerful Roles
- Sensitive Role and Profile analysis is executed on a monthly basis
- Reports are routed to IT management for review in documented workflow



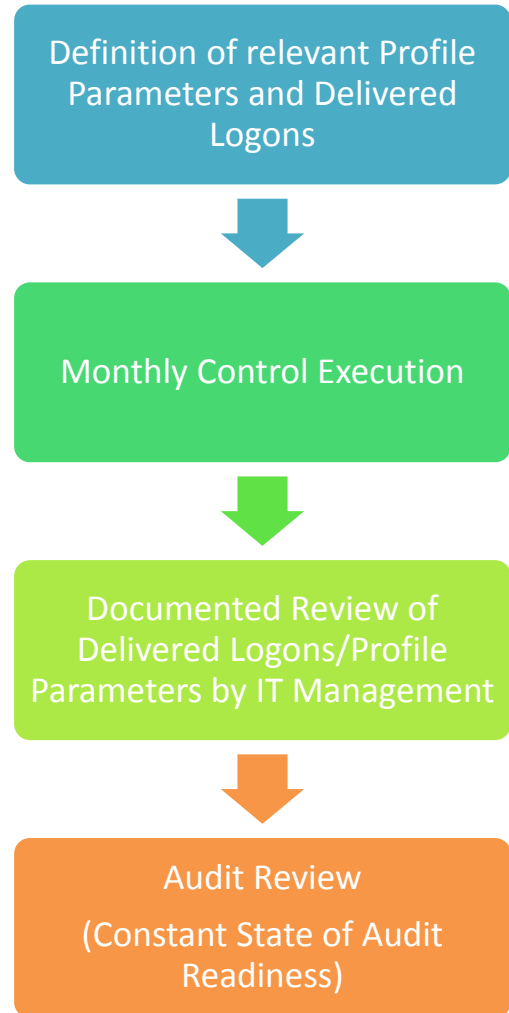
## Inactive and non-Employee Logon Review

- Review of all logons that have not accessed the system in over 30 days and all logons not tied to an Employee in SAP ERP HCM
- Reports are executed and routed to IT Management for review by our individual locations
  - Exceptions are noted and submitted as requests to security team



## Review of Delivered Logons and Security Related Profile Parameters

- Review of Delivered SAP Logons to verify that default passwords do not exist
- Review of Profile Parameters to ensure that they are in line with Auditor recommendations and have not changed
  - Exceptions are noted and submitted as requests to security team



## Periodic User and Role Certification Process

---

- Internal Auditors determined that we need to review Users and Roles on a quarterly basis
  - Wanted Role Owner sign-off on:
    - Current Roles and assignments
      - Making sure Users are still with the company and didn't change Positions
    - Changes to Roles or Users during the reporting period
    - Current Segregation of Duties analysis
  - Needed to be able to easily audit the process
    - Verification of timely sign-offs
    - Verification of processing of related requests

## Periodic User and Role Certification Process (cont.)

---

- Lack of IT staff made the generation and distribution of quarterly reports a challenge
  - Download User and Role data, Transaction Execution Logs, change docs, and SOD analysis from SAP system
  - Map the User/Role/Transaction data into a usable format
- We implemented an automated process
  - Generates reports in a usable format
  - Pushes reports to Role owners via workflow
  - Collects feedback from Role owners

```
graph TD; A[Definition of Periodic User and Role Certification Requirements] --> B[Definition of processes to generate and distribute certification reports];
```

Definition of Periodic User and Role Certification Requirements

Definition of processes to generate and distribute certification reports

## Periodic User and Role Certification Process (cont.)

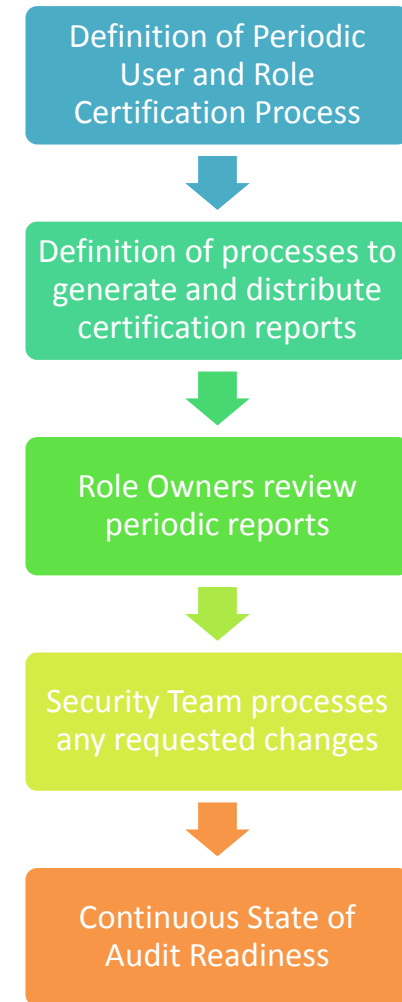
---

- Role owners receive reports via workflow, review, and sign-off to certify analysis
  - Matrix-based mapping of Roles detailing User and Transaction assignments
  - Validation that changes during the reporting period were approved
  - Validation of segregation of duty risks for “owned” business process



## Periodic User and Role Certification Process (cont.)

- Changes are requested via documented workflow
  - User terminations
  - Role removal from Users due to responsibility changes
- Security Team receives requests via Workflow and processes any changes
  - All changes and sign-offs are always available for audit review



## What We'll Cover ...

---

- Exploring Abiomed's journey and challenges
- Defining key preventive and detective access controls
- Leveraging key controls over emergency access and SAP transports
- Evaluating how Abiomed helped ourselves through automation
- Wrap-up

## Key Controls Over Emergency Access

---

- Internal Auditors wanted IT support personnel to have display-only access in Production
  - Creates challenges as IT support occasionally needs to make changes in Production
- Internal Auditors preferred that we did not use generic logons
  - Better tracking of changes processed
  - Ability to easily see executed SOD Risks
- Internal Auditors wanted an IT Management sign-off after emergency access session was complete
  - Noting executed Transactions/changes

## Key Controls Over Emergency Access (cont.)

---

- Definition of Emergency Access Process
  - We grant emergency access to non-HR change functionality in Production on a pre-approved basis
  - We grant emergency “SAP\_ALMOST” access in our Quality System on a pre-approved basis
  - Provisioning is done via an automated solution
- We use workflow to route details from emergency sessions to IT Management
  - Provides info on what was executed and changed
  - Records IT Management sign-off

```
graph TD; A[Definition of Audit Requirements for Emergency Access] --> B[Definition of Emergency Access Processes];
```

Definition of Audit Requirements for Emergency Access

Definition of Emergency Access Processes

## Key Controls Over Emergency Access (cont.)

- IT Support User activates emergency access
  - User processes whatever Transactions are necessary
- Monitoring jobs identify executed Transactions and changes pushing output in workflow to IT Management
  - Includes a review of Change Documents and Statistical Records
- IT Management signs-off on changes processed during emergency session
  - Checks for reasonableness of changes
- Auditors can review the process and/or documentation at any time



## Key Controls Over Change Management (SAP Transports)

---

- Internal Auditors required that we document all changes
  - Includes testing/validation details
- Internal Auditors required that our business owners have a sign-off in the change management process
  - Ensures business involvement in testing
  - Increases awareness of system changes
- Internal Auditors required that our IT Management have final sign-off
  - Ensures proper documentation
  - Visibility and prioritization of all SAP changes

## Key Controls Over Change Management (SAP Transports)

---

- Created a “Change Review Board” (CRB)
  - Represents top management from all major departments (approximately 10 people)
  - All CRB members are notified of pending changes, but only 3 sign-offs are required
- Implemented workflow-based process to manage all change documentation and approvals
  - Once changes are approved in workflow, they are automatically selected for import into the Production System

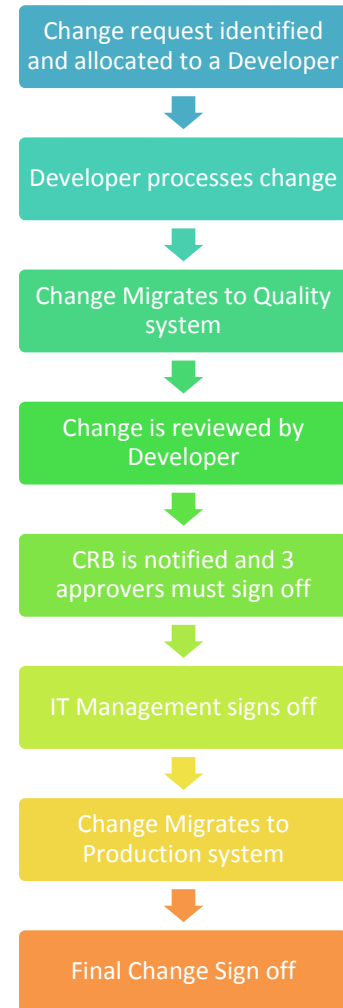
```
graph TD; A[Definition of Audit Requirements for Transport Management] --> B[Definition of Transport Management Processes];
```

Definition of Audit Requirements for Transport Management

Definition of Transport Management Processes

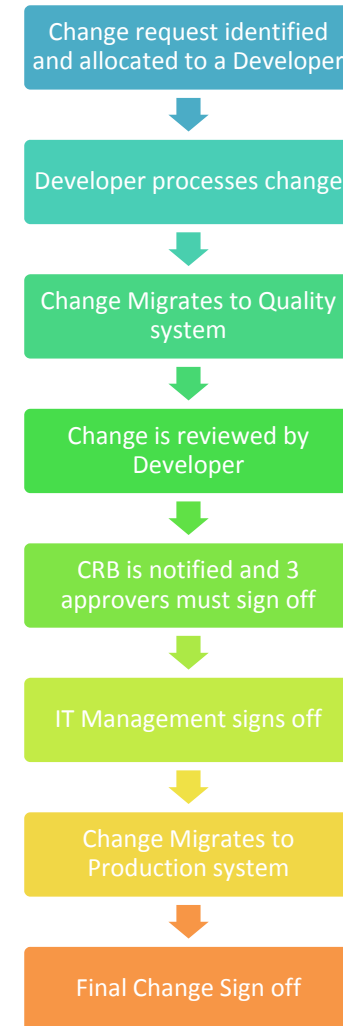
# Key Controls Over Change Management (SAP Transports)

- Transport Change Management Process
  - Change request identified and allocated to a Developer
  - Developer processes the change
    - Configuration or Development changes are completed and released via Transport into workflow
  - Workflow automation imports change into Quality system
  - Developer verifies migration into Quality system and notifies users to begin testing
  - CRB is notified of pending changes and approves or returns to Developer (if necessary)



# Key Controls Over Change Management (SAP Transports)

- Transport Change Management Process (cont.)
  - IT Management reviews change
    - Validates documentation is complete
  - Workflow automation imports change into Production system
  - Final sign off provides verification that change is functioning properly
- Continuous state of audit readiness!
  - Auditors can provide a sample of changes from import history
  - We can easily pull all documentation and approvals related to the change



## What We'll Cover ...

---

- Exploring Abiomed's journey and challenges
- Defining key preventive and detective access controls
- Leveraging key controls over emergency access and SAP transports
- Evaluating how Abiomed helped ourselves through automation
- Wrap-up

## Answering Goal 1 – Cost Reduction and Efficiencies

---

- Automated processing of change request transports for review and approval
  - Abiomed has a specific requirement that 3 functional owners must review and approve any transport to production
- Configurable workflow to route requests to appropriate parties for review and approval
- Extensive change request tracking and reporting that allows easy access to details for our auditors
- Acceleration of day-to-day SAP security administration via workflow and automatic provisioning

## Return on Investment – Specific Results

---

- Reduced the time, expense, and distractions associated with manual audits
  - Actual 50% reduction in time spent by third-party pre-auditors
  - Reduction in internal staff time spent supporting ad hoc requests from external audit and in analyzing SOD issues
- Significantly reduced time spent on compiling, distributing and following-up on Abiomed quarterly SOD reports
  - One week prep time condensed to two hour review time by IT resource
  - Review and approval by 7 functional owners received within one week time period versus 5 months with paper process
    - Workflow distribution
    - Electronic approval documented and captured

## Answering Goal 2 – Risks and Mitigation

---

- Real-time risk analysis and mitigation of authorizations for SOD and sensitive authorization risks
- Pre-defined and customizable Rulebook to meet Abiomed's specific needs
- Automatic monitoring of transaction execution and alerts to compliance owners
- Integrated role management via workflows that provide risk analysis, owner approval and facilitated request processing
- Immediate notification for emergency access with activity monitoring and reporting

## Risk Mitigation – Specific Results

---

- Receive immediate notification of activation of Emergency Access (Firecall) activity
  - Previously, IT management team would meet monthly and review prior month's firecall activity
  - Reviews are now done upon close of emergency access and any questions and potential mitigation activities can be timely
- During audit preparation, the risk analysis identified user with the ability to create a sales order and the ability to change a customer's credit limit
  - Was able to address and mitigate before actual audit started

## Example of Risk Mitigation: SOD Initiative

---

- Joint initiative between Finance and IT; started fall 2010
- Goal to drive operational excellence through the evaluation, analysis and mitigation of Abiomed's Segregation of Duties risks
- Quarterly review and analysis verified Abiomed was in compliance, but the process could be improved
- Three key areas being addressed:
  - Risk identification and management
  - Role assignment optimization
  - Mitigating controls

## Risk Identification and Management

---

- Phase consisted of the following activities:
  - Analysis of actual key risks that have been executed to determine priorities to focus
  - Analysis of business rules to ensure completeness
  - Analysis of custom transactions to ensure they are accounted for
  - Development of an ongoing process to maintain rule sets to prevent them from getting stale
  - Development of an annual training program for functional owners to educate how to review and approve the SOD reports for their functional areas

## Role Assignment Optimization

---

- Phase consisted of the following activities:
  - Analysis of existing role assignments
  - Development of recommended changes to eliminate or reduce risks, including potential role redesigns
  - Development and documentation of testing processes to ensure new role assignments don't conflict with established rules
  - Manual validation to test a sampling of the risks
  - Review transaction usage and remove unused 'high risk' transactions from production roles

## Mitigating Controls

---

- Phase consisted of the following activities:
  - Validation that high risk areas are covered by mitigating controls
  - Validation that the mitigating controls are in place and managed
  - Validation that all known unmitigated risks are documented and approved

## Results of Initiative to Date

---

- Streamlined segregation of duties effort from a regulatory and good practices standpoint
- After analysis of 368 potential risks, identified 61 user role assignment changes and 36 role changes
- Defined and documented 7+ mitigating controls
- Simplified the processes going forward

## Answering Goal 3 – Compliance and Reporting

---

- Scheduling and automatic execution of predefined or custom compliance reports, routed to predefined users for review
  - Sensitive role and profile assignments
  - Mitigating control assignments
  - Invalid logon attempts or initial passwords
  - User and role changes over a time period
- Management of batch jobs providing central scheduling and monitoring of batch processes
  - Provides documentation and monitoring of batch jobs
  - Notifies appropriate owners of job success or failure, with the appropriate details

## Compliance & Reporting – Specific Results

---

- Receive reports that are required to support defined audit controls, either from an event trigger or via a time requirement
- For example, the first of each month, IT management receives the following reports for review and analysis:
  - System Environment Report
  - Critical Authorizations Report
  - Inactive Logons
  - Non-Employee Logons
  - Users with SAP\_ALL

## What We'll Cover ...

---

- Exploring Abiomed's journey and challenges
  - Defining key preventive and detective access controls
  - Leveraging key controls over emergency access and SAP transports
  - Evaluating how Abiomed helped ourselves through automation
- Wrap-up

## What Abiomed Learned

---

- There are reasonably priced GRC solutions on the market to meet a small company's requirements
  - First, identify your goals and what you actually need
  - Find the solution that fits your goals and don't overbuy
- Deployment was quick and painless – almost a non-event
  - Be prepared and plan the transition – change in processes? training requirements?
  - Understand what you are getting and determine what functionality you will use and how
- The controller and his team are all over risk mitigation – get the business involved and don't make this an IT solution only
- SOX Audits don't have to be quite so time consuming

## What You Can Look For

---

- Use a GRC tool for the process of configuring changes – from request, development, testing, approval and movement into production
- Tools that capture audit reporting information
- Tools that support your business processes with automated workflows
  - Automated workflows not only manage migration of those changes through the development cycle, but also document who made the request, who developed it, who tested it, the test results and when it was moved to production

## 7 Key Points to Take Home

---

- Don't tolerate energy sapping manual processes
- Understand management's need for GRC data
- Look for a solution that meets your needs and that is manageable for your company
- Seek to “embed compliance” – automate capture of audit data at the time of execution
- Enable ad hoc, on-demand audit reporting
- Look for tools that will streamline routine IT operations
- Embrace GRC – view it as a tool for innovation



---

**For Further Information Please Contact:**

Scott Goolik  
Chief Technology Officer, SymSoft Corporation  
[Scott.goolik@sym-corp.com](mailto:Scott.goolik@sym-corp.com)

Sharon Kaiser  
Chief Information Officer, Abiomed Corporation  
[skaiser@abiomed.com](mailto:skaiser@abiomed.com)

Heather Mickelson  
Manager of Client Relations, Symmetry Corporation  
414-732-2738  
[hmickelson@sym-corp.com](mailto:hmickelson@sym-corp.com)

---

ControlPanel GRC

Professional Solutions for Compliance Automation

[www.ControlPanelGRC.com](http://www.ControlPanelGRC.com)