



# **Sustained Compliance Through Automation of Access Recertification and Attestation**

---

**A Discussion with ISACA-Atlanta Chapter Members**

**July 17, 2009**


# Agenda

---

- Introductions
- Effective IT controls for appropriate access
- Typical access recertification as manual process
- Drawbacks of manual process
- Typical access recertification as automated process
- Benefits of automated process
- Questions

## Introductions

---

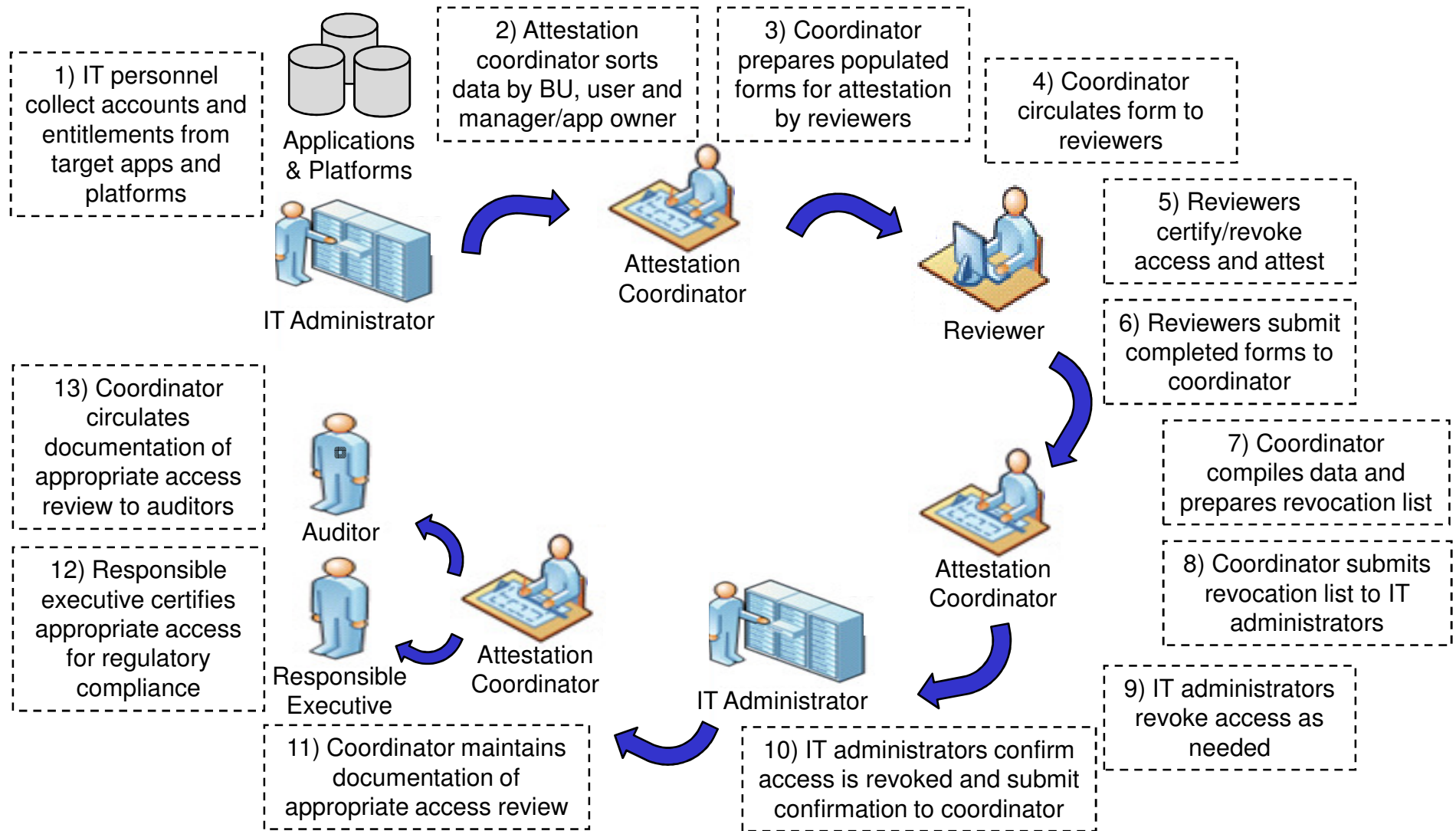
- Stoddard Manikin, CISM, CISSP  
Senior Delivery Manager  
Logic Trends, Inc.  
Atlanta, GA
- ISACA Atlanta chapter member 
- Logic Trends is a consulting and systems integration firm focused solely on Identity and Access Management (IAM)
- Founded in 2002, the Company has operations in Atlanta (HQ), Dallas, Tampa & Cleveland
- 170+ Identity & Access Management Engagements Completed

## Effective IT Controls for Appropriate Access

---

- Effective controls that assure appropriate access to key systems and applications are typically the most challenging IT controls to implement and maintain
- When preventive controls break down, detective controls are crucial to safeguard the IT environment
- Access recertification and attestation is a critical part of effective detective access controls
- Manual recertification processes are costly, time-consuming, and sometimes ineffective
- Access recertification and attestation campaigns can be automated with vendor tools or with existing ITSM help desk solutions, leading to sustained compliance

# Typical Recertification Cycle as Manual Process



## Drawbacks to Manual Recertification Cycle

---

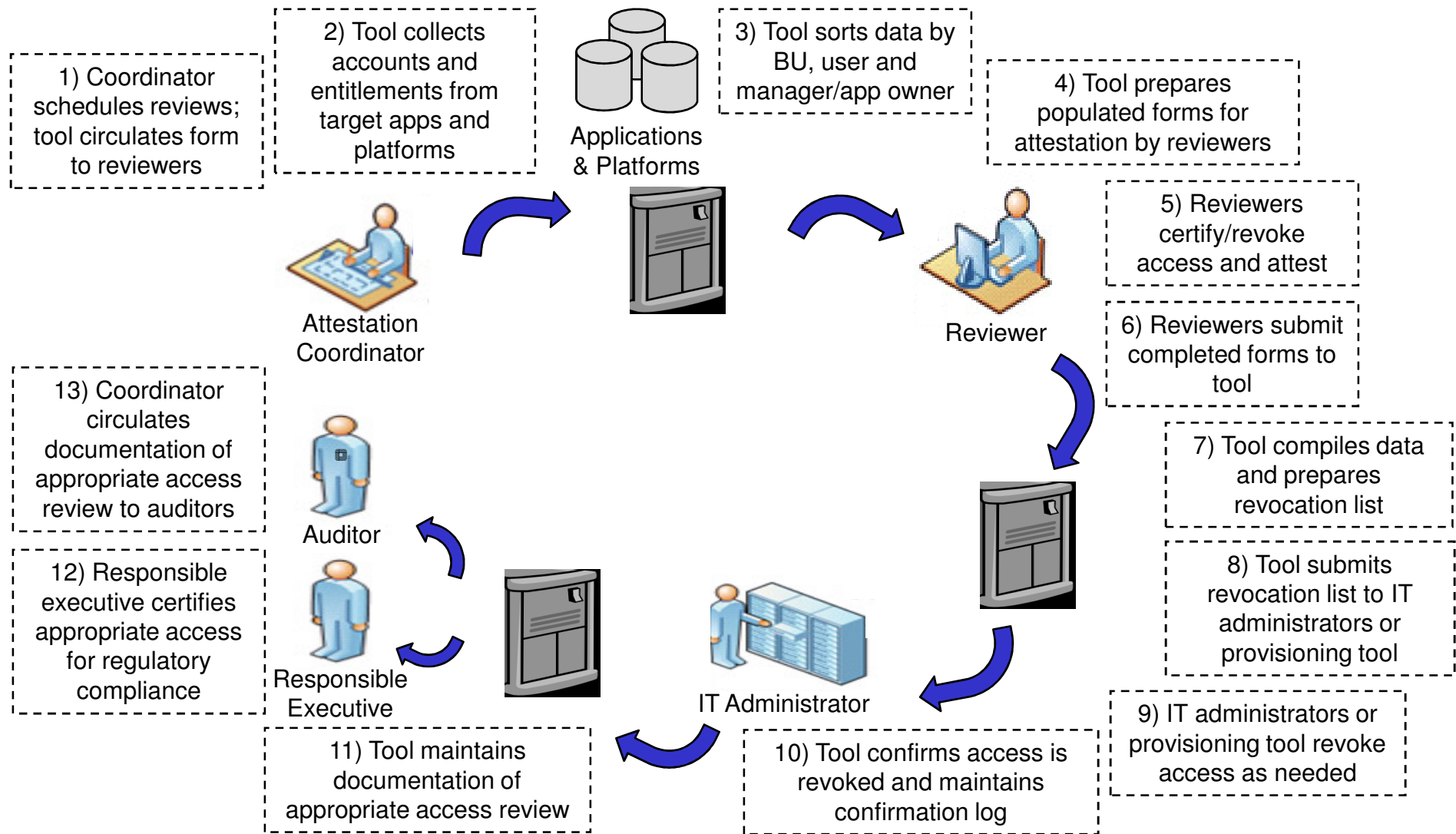
- Difficult to match user id's to actual users and approvers
- Entitlement descriptions difficult to interpret
- Susceptible to unintentional human errors (ex. SoD checks)
- Lacks reconciliation to validate requested changes are made
- May not address orphan or shared accounts
- Time consuming and expensive - preparers, approvers and auditors
- Significant time lag from inappropriate access granting vs. detection
- Reasonable for one-off reviews but typically unsustainable
- Could lead to weak or ineffective IT controls and/or non-compliance



# Manual SoD Review

<b>SOD MATRIX</b> SYSTEM LEVEL/ROLE ACCESS	Technician Non User	Technician User	Subcontractor	Subcontractor Supervisor	Field Technician Supervisor	Field Manager	Scheduler	Dispatcher	Dispatcher with Inventory	Dispatch Manager	Dispatch Manager with Inventory	Warehouse	Warehouse Manager	Payroll/Back Office	Escalation	Call Center	Management	Workforce Provisioning	Answers User	Dashboard Reports User	Inventory Transaction
Technician Non User	Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Technician User	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Subcontractor	Not Allowed	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Subcontractor Supervisor	Not Allowed	Not Allowed	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Field Technician Supervisor	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Field Manager	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Scheduler	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Dispatcher	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Dispatcher with Inventory	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Dispatch Manager	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Dispatch Manager with Inventory	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Answers User	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Dashboard Reports User	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Inventory Transaction	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
<b>Legend :</b>																					
Allowed	Allowed																				
Not Allowed	Not Allowed																				

# Typical Recertification Cycle as Automated Process





## Sample Automated Recertification Screen 1

Screen 1 – Reviewer views open certifications, verifies subordinates work for them, and reviews access

### Certification Details

[Back](#)

**Certification:** Nursing Cert

**Business Unit:** Nursing

**Period:** 01/31/2008

**Incremental:**

**Number of Users:** 638

**Created By:** rbackadmin

**Creation Date:** 01/29/2008

**Last Updated By:**

**Last Update Date:**

**Completed(%):**

[Back to Certifications List](#)

Page: [1](#) [2](#) [3](#) [4](#) [5](#) [64](#) [Next>>](#)

1 - 10 of 638 Records - Display

Status	User ID	Last Name ▲	First Name	Phone	E Mail	Comments	Employee Verification	Action
		<input type="text"/>	<input type="text"/>		<input type="text"/>			<a href="#">Filter</a>
New	E50178	A Stallone	A Sylvester				Choose... ▼	[ Review Access ]
New	E43171	A Schwarzenegger	J Arnold				Choose... ▼	[ Review Access ]
New	E50199	A Willis	E Bruce				Choose... ▼	[ Review Access ]



# Sample Automated Recertification Screen 2

Step 2 – Reviewer certifies the subordinate’s accounts and entitlements

My Certifications > Nursing Cert > Willis, Bruce

Views: All Entitlements

**Access Details** Back

User: Willis, Bruce

[Back to Users List](#)

Roles (None) | Entitlements (1 entitlement)

Certify	Revoke	Name	Namespace	Endpoint	Attributes	Comments																																																												
<input type="radio"/>	<input type="radio"/>	E17005	ECLIPSYS Namespace	ECL	<table border="1"> <tr><th colspan="4">Disciplines :</th></tr> <tr> <th>Certify</th> <th>Revoke</th> <th>Attribute Value</th> <th>Comments</th> </tr> <tr> <td><input type="radio"/></td> <td><input type="radio"/></td> <td>Nursing</td> <td></td> </tr> <tr><th colspan="4">Task Role :</th></tr> <tr> <th>Certify</th> <th>Revoke</th> <th>Attribute Value</th> <th>Comments</th> </tr> <tr> <td><input type="radio"/></td> <td><input type="radio"/></td> <td>RN</td> <td></td> </tr> <tr><th colspan="4">Organization Role :</th></tr> <tr> <th>Certify</th> <th>Revoke</th> <th>Attribute Value</th> <th>Comments</th> </tr> <tr> <td><input type="radio"/></td> <td><input type="radio"/></td> <td>Diabetes Ed</td> <td></td> </tr> <tr><th colspan="4">Occupation :</th></tr> <tr> <th>Certify</th> <th>Revoke</th> <th>Attribute Value</th> <th>Comments</th> </tr> <tr> <td><input type="radio"/></td> <td><input type="radio"/></td> <td>RN</td> <td></td> </tr> <tr><th colspan="4">Order Role :</th></tr> <tr> <th>Certify</th> <th>Revoke</th> <th>Attribute Value</th> <th>Comments</th> </tr> <tr> <td><input type="radio"/></td> <td><input type="radio"/></td> <td>Registered Nurse</td> <td></td> </tr> </table>	Disciplines :				Certify	Revoke	Attribute Value	Comments	<input type="radio"/>	<input type="radio"/>	Nursing		Task Role :				Certify	Revoke	Attribute Value	Comments	<input type="radio"/>	<input type="radio"/>	RN		Organization Role :				Certify	Revoke	Attribute Value	Comments	<input type="radio"/>	<input type="radio"/>	Diabetes Ed		Occupation :				Certify	Revoke	Attribute Value	Comments	<input type="radio"/>	<input type="radio"/>	RN		Order Role :				Certify	Revoke	Attribute Value	Comments	<input type="radio"/>	<input type="radio"/>	Registered Nurse		
Disciplines :																																																																		
Certify	Revoke	Attribute Value	Comments																																																															
<input type="radio"/>	<input type="radio"/>	Nursing																																																																
Task Role :																																																																		
Certify	Revoke	Attribute Value	Comments																																																															
<input type="radio"/>	<input type="radio"/>	RN																																																																
Organization Role :																																																																		
Certify	Revoke	Attribute Value	Comments																																																															
<input type="radio"/>	<input type="radio"/>	Diabetes Ed																																																																
Occupation :																																																																		
Certify	Revoke	Attribute Value	Comments																																																															
<input type="radio"/>	<input type="radio"/>	RN																																																																
Order Role :																																																																		
Certify	Revoke	Attribute Value	Comments																																																															
<input type="radio"/>	<input type="radio"/>	Registered Nurse																																																																



## Sample Automated Recertification Screen 3

Step 3 – Reviewer certifies the subordinate's accounts and entitlements

### User Certification

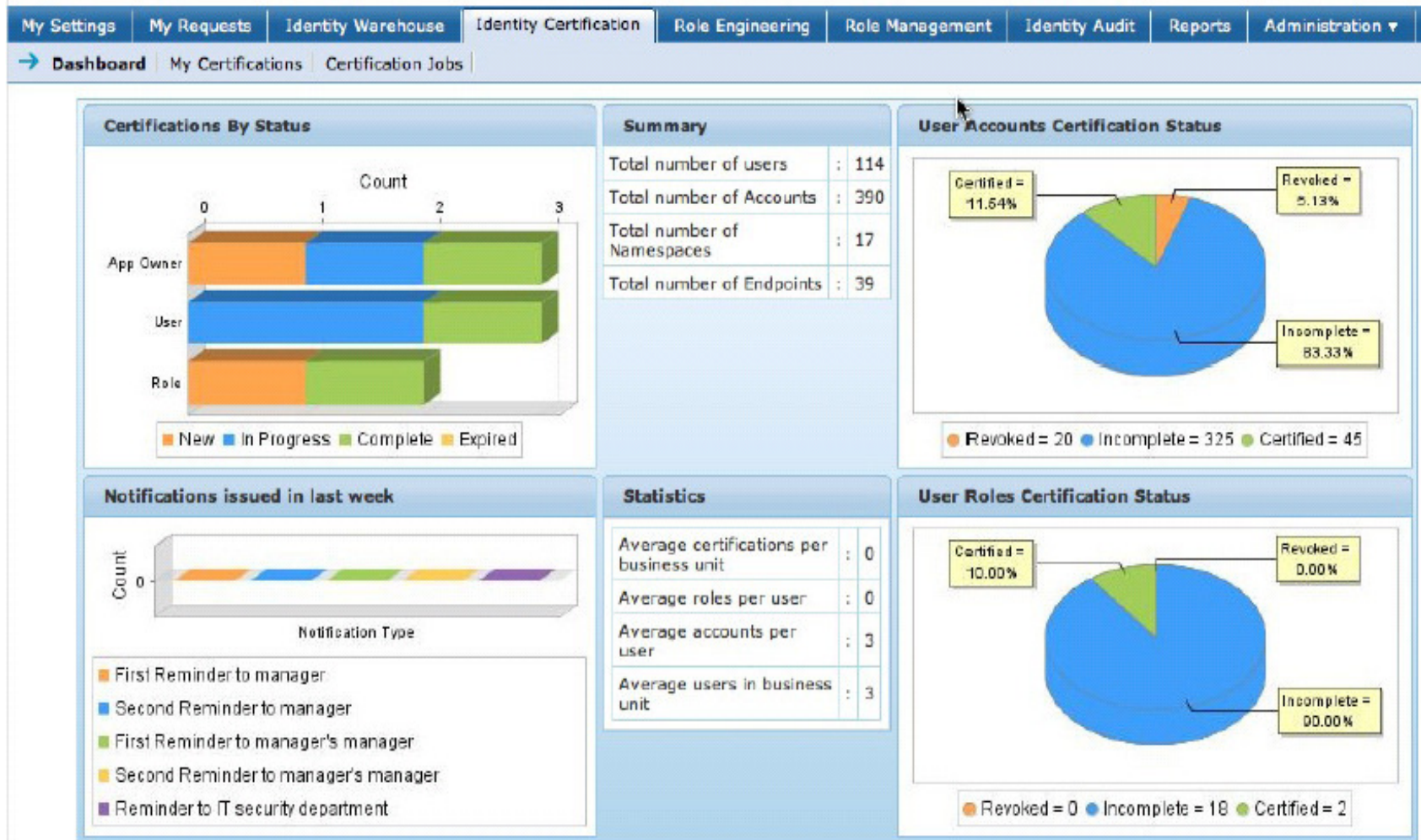
Organization: Stamford Branch

Status: 7 Users (1 Not Reviewed, 2 Reviewed, 1 Approved)  Hide reviewed privileges

UserName	PersonID	Org	Org Type	Country	Location	Susp. User	Susp. Conn.	Prop. Conn.	
- Willis, Bruce	82922230	Stamford Branch	Branches	US	Connecticut		8	1	Completed
Business Unit: Special Field: Version:9									
- Roles (4)									
Name	Description	Used By	Link Type	Audit Card Status	History	Remove All	Approve All	Comment	
BSTAMJ1	Sage Role	5/7 71%	Direct	*Suspect User-Role Connection By Privileges(Score:32 Status:Suspected);	Request to add 4/12/2007 5:25:20 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	no longer needs this	
BSTAMMGR	Sage Role	1/7 14%	Direct		Request to remove 4/12/2007 5:25:20 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
TSSTAMJ1	Sage Role	2/7 29%	Direct		Request to add 4/12/2007 5:25:20 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
STAMFORD	People working in Stamford Branch	7/7 100%	Direct	*Suspect User-Role Connection By Privileges(Score:37 Status:Suspected);	Request to approve 3/29/2007 5:53:20 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
+ Resources (6)									

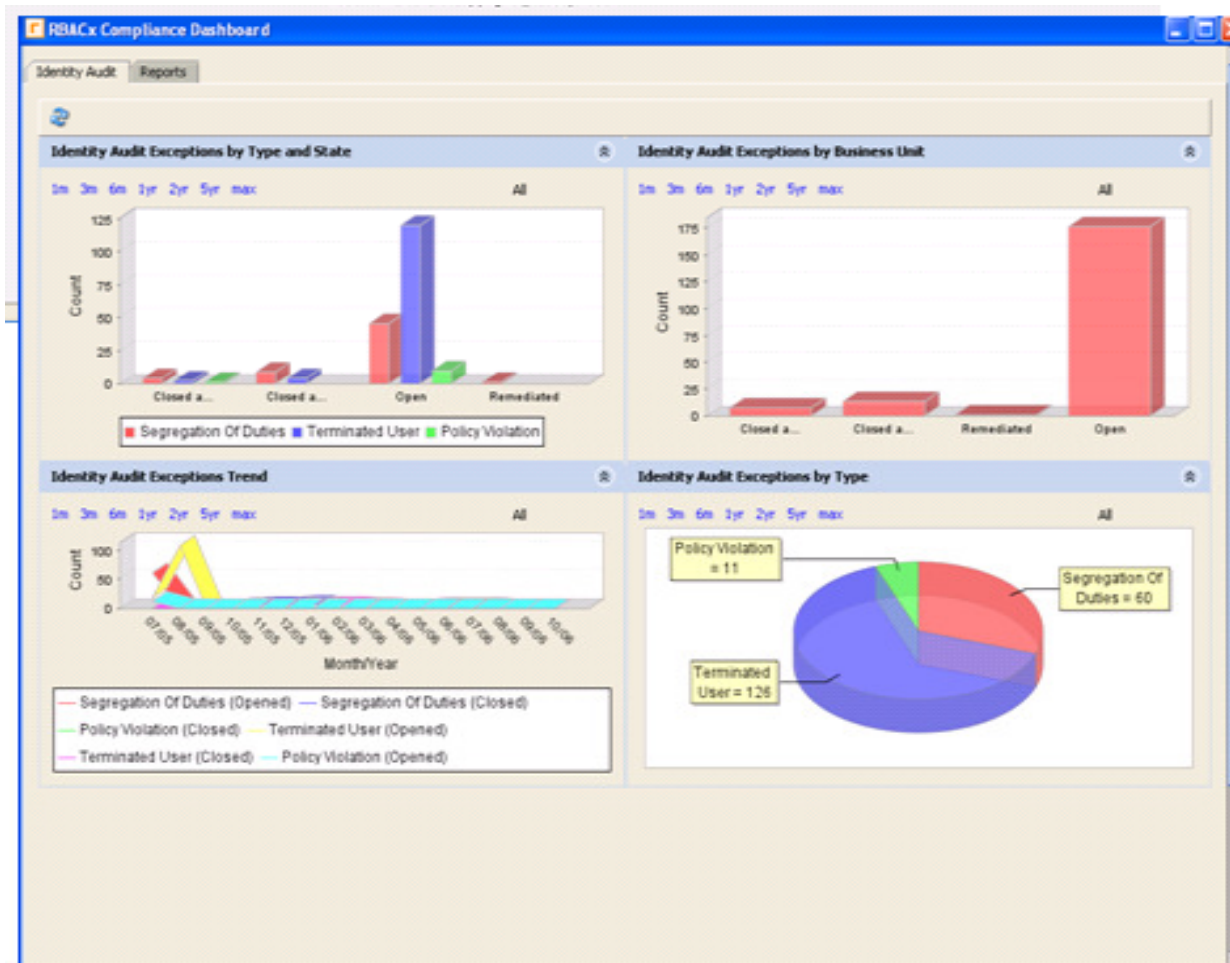
# Sample Automated Recertification Screen 4

## Screen 4 – Dashboard to track recertification campaigns



## Sample Automated Recertification Screen 5

Screen 5 – Dashboard to track recertification campaigns



## Key Benefits to Automation

---

- Simplified user experience
- Efficiency and cost savings gained through automation
- Can be run more frequently in less time, allowing faster detection
- Improved visibility into who has access to what
- Change control validation/reconciliation through closed loop system
- Provides a high-quality, reliable system of record for auditable evidence of compliance
- Reduced cost, complexity & burden of access review & certification
- Improved risk management through sustainability of compliance

## Closing Thoughts

---

- Access recertification and attestation is a critical part of effective detective access controls as well as regulatory compliance
- Manual recertification processes are costly, time-consuming, and sometimes ineffective resulting in weak/ineffective controls or non-compliance
- Access recertification and attestation campaigns can be automated with vendor tools or with existing ITSM help desk solutions
- Automation can lead to improved access controls related to quality, reliability and sustained compliance



## Questions

### Contact:

Stoddard Manikin

[smanikin@logictrends.com](mailto:smanikin@logictrends.com)

770-551-5045

## Thank You