# T3 - Enabling Technology to Automate ISO 27002

## Vijay Upadhyaya

September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Enabling Technologies For ISO 27002

Ed King
Vice President, Marketing And Product Management
Agiliance

September 21, 2009 – September 23, 2009

## Today Is Technology Geek Day

- What we will cover today
  - Enabling technologies for implementing ISO 27002 processes and controls
  - Strategy and recommendations about information security technology adoption
  - Deep dive in selected technologies
- What we will not bored you with today
  - What ISO 27002 is
  - Why ISO 27002 is good and important
  - How to implement ISO 27002 program
  - What controls do you need to pass an ISO 27002 audit

# Agenda

- Quick ISO 27002 overview & today's agenda
- Technology adoption strategy and opportunities
  - The information security stack and the maturity cycle
  - The $64,000 questions and practical challenges
  - A risk based approach for information security strategy
- Seven deadly sins of information security technology adoption
- Q&A

# 27002 – Info. Security Management

- Domain 4: Risk management
- Domain 5: Security policy
- Domain 6: Organization of information security
- Domain 7: Asset management
- Domain 8: Human resource security
- Domain 9: Physical & environmental security
- Domain 10: Communications & operations management
- Domain 11: Access control
- Domain 12: Systems acquisition, dev. & maintenance
- Domain 13: Information security incident management
- Domain 14: Business continuity management
- Domain 15: Compliance

## Enabling Technologies

- Sec. 4
- Sec. 5
- Sec. 6
- Sec. 7
- Sec. 8
- Sec. 9
- Sec. 10
- Sec. 11
- Sec. 12
- Sec. 13
- Sec. 14
- Sec. 15

Compliance Management

Card management

Patch Management

Identity Management

Disaster Recovery

E-Discovery

Secured Backup

Intrusion Prevention

Email Archiving

Fraud Prevention

Intrusion Detection

Secured Configuration Management

Policy Management

Firewall

Content Management

Security Incident & Event Management

Vulnerability Scanner

Vendor Risk Management

Video Security

Intrusion Detection

Incident Management

Application Security

Information Rights Management

Database Security

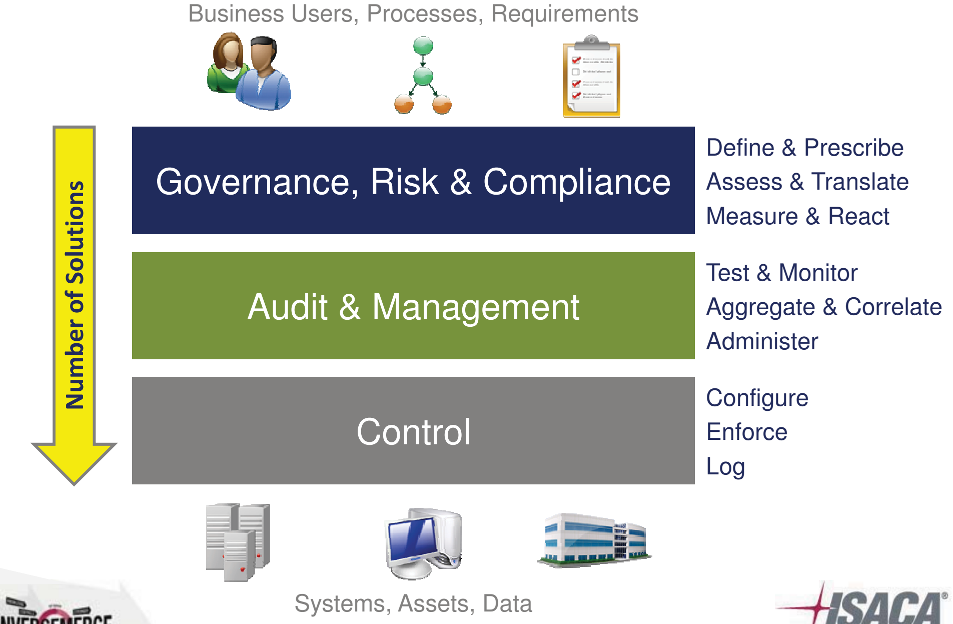
Privacy Management

Enterprise Risk Management

CONVERGEMERGE

ISACA Serving IT Governance Professionals San Francisco Chapter

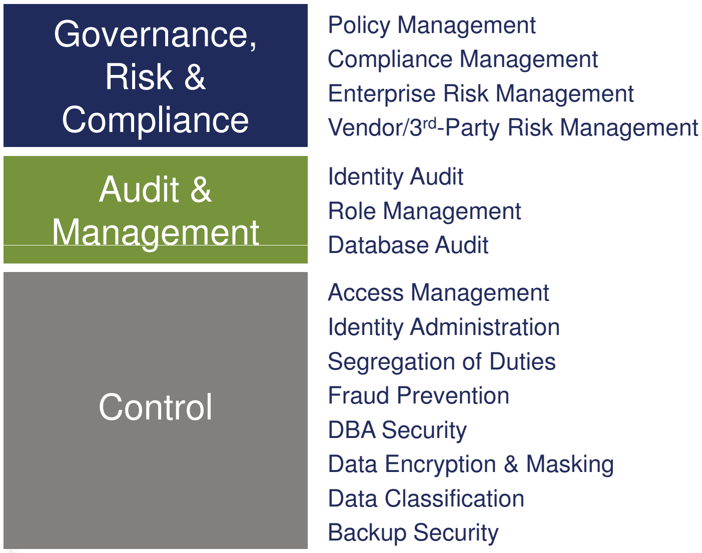
## Information Security Technology Stack



CONVERGEMERGE

ISACA Serving IT Governance Professionals San Francisco Chapter

# Today's Technology Drill Down



**Governance, Risk & Compliance**

Policy Management
Compliance Management
Enterprise Risk Management
Vendor/3rd-Party Risk Management

**Audit & Management**

Identity Audit
Role Management
Database Audit

**Control**

Access Management
Identity Administration
Segregation of Duties
Fraud Prevention
DBA Security
Data Encryption & Masking
Data Classification
Backup Security

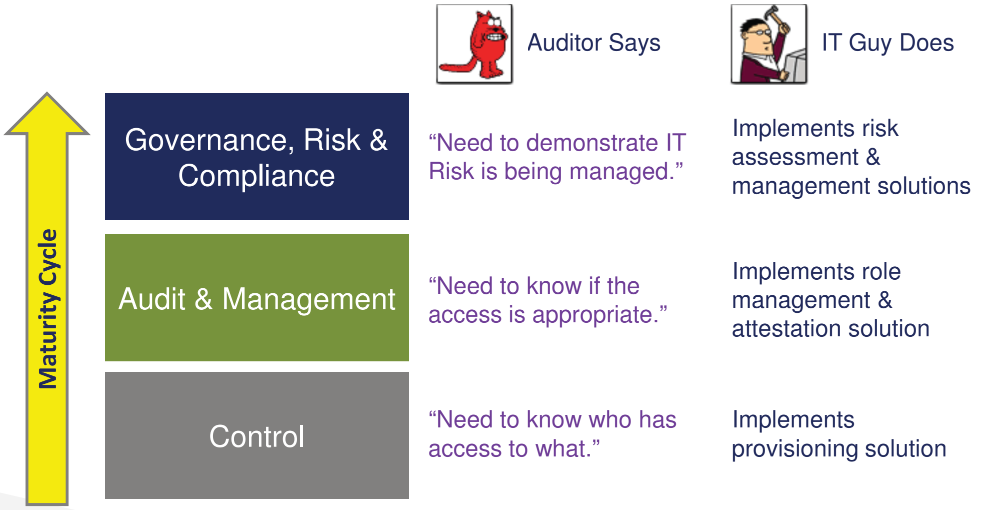
# The $64k Questions of Info Security

- Where do you start?
- What technologies do you need?
- Do you need more?

How does your organization answer these questions?

## Information Security Maturity Cycle

### An Identity Management Example



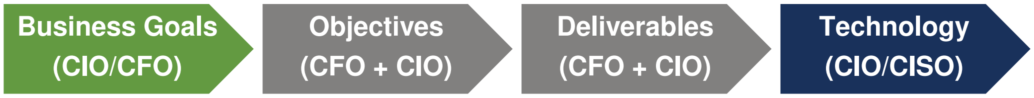
Maturity Cycle

| | Auditor Says | IT Guy Does |
|---|---|---|
| Governance, Risk & Compliance | “Need to demonstrate IT Risk is being managed.” | Implements risk assessment & management solutions |
| Audit & Management | “Need to know if the access is appropriate.” | Implements role management & attestation solution |
| Control | “Need to know who has access to what.” | Implements provisioning solution |

## Challenges With Bottom-Up Approach

- Auditor demands are often translated literally to help drive security agendas regardless of true intent
- Security project deployment methodologies are usually developed based on efficiency and security drivers
- Security projects deployed without risk and compliance as primary driver often fail to be useful to the business users in a timely manner
- Business users are asked to view, interpret and approve cryptic data with no business context
- Too much data is being generated so true risks is drown out by false alarms and low priority noise

# A Risk Based Methodology



**Business Goals (CIO/CFO)**

- Accountability
- Thoroughness
- Completeness
- Accuracy

All in the context of managed risk

**Objectives (CFO + CIO)**

- Consensus list of security risks
- Sample risk categories:
  - Segregation of duties
  - Super user access
  - Identity theft
  - Privacy
  - Hacking
  - Virus / bots
  - Data leakage

**Deliverables (CFO + CIO)**

- Consensus list mitigating controls for security risks
- Sample controls:
  - SoD policies
  - Single-use password
  - DB encryption
  - Anti-virus
  - Information rights mgmt.

**Technology (CIO/CISO)**

- Vendor decision
- Technology decision
- Technology mix
- Time frame
- Deployment strategy
- Degree of coverage
- Form of evidence

# Why Is This Better? Clear and Practical!

- Objectives, deliverables and values are all clearly stated, understood, and measureable in terms of:
  - Security risks & mitigation controls mapped to risks
- Business understands exactly what it is getting and it is MEASURABLE
- Business value does not have to wait for tech. nirvana
- Security team makes technology & logistic decisions
- Security team optimizes solution design according to risk appetite, don’t waste energy on low risk areas

## The $64k Questions of Info Security

- Where do you start?
  - What are the highest risks?
- What technologies do you need?
  - What is the risk reduction / dollar for each technology?
  - How much risk can the technology remove?
- Do you need more?
  - What is the incremental risk reduction / dollar spent?
  - Has the risk appetite been reached?

## What Is Needed For This Methodology

- A risk-aware asset DB as trusted source for:
  - Configuration data about assets from CMDB
  - Added risk and compliance information about each asset, such as data exposure, criticality score, covered regulations
  - Business data like attestation owners, role approvers, ….
  - Risk and compliance posture and evidences about each asset
- Risk management platform for:
  - Collaboratively develop list of access risks
  - Collaboratively determine what mitigation controls are needed
  - Map mitigation controls to access risks
  - Upload control assessment results and evidences
  - Measure access risks based on control assessment results

# Seven Deadly Sins of GRC Tech Adoption

## #1 Losing sight of risk management as the objective

- Compliance is not the end game
- Proactive risk management saves money in the long run
- Risk management is a continuous process
- Have a clear roadmap

# Seven Deadly Sins of GRC Tech Adoption

## #2 Rush to quick-fix solutions that cannot scale

- “Quick ROI” doesn’t have to mean “quick-fix”
- Don’t solve one problem today, but create a bigger problem for tomorrow
- Look for a quick-to-deploy, but also extensible and scalable GRC platform

## Seven Deadly Sins of GRC Tech Adoption

### #3 Underestimating the value of automation

- Strong control and risk management requires breadth and depth
- Control automation is not the same as process automation
- Continuous compliance cannot be done without control automation

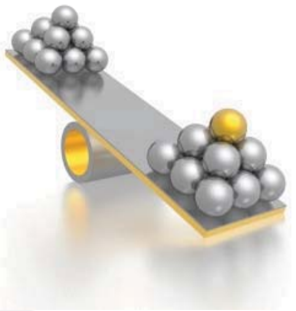
## Seven Deadly Sins of GRC Tech Adoption

### #4 Misjudging enterprise's appetite for customization

- Know your organization: build vs. buy
- Customization is a long term commitment
- Implement best-practice or just replicate legacy process?

# Seven Deadly Sins of GRC Tech Adoption

## #5 Not considering total cost of ownership



- Don’t get locked into expensive proprietary solutions
- Understand all the costs for the lifetime of the application before you buy
- Don’t forget cost of upgrade and future integrations

# Seven Deadly Sins of GRC Tech Adoption

## #6 Lack of input from all stakeholders

- GRC needs are across different groups
- A good GRC solution addresses both business and IT needs
- A good GRC solution solves business problems, but also has to be manageable

## Seven Deadly Sins of GRC Tech Adoption

### #7 Procrastinating technology adoption

- Process change takes trial and error over time
- Take an incremental approach to adoption but get busy
- More requirements coming – don't run into a brick wall

## To Learn More: www.agiliance.com

# Policy & Compliance

Monica McDermott
Senior Manager, Marketing
Agiliance

September 21, 2009 – September 23, 2009

ISACA Serving IT Governance Professionals San Francisco Chapter

## ISO 27002 Says…

- Section 5: Security policy
  - Ownership, development, review, approval, publication, and evaluation
  - Policy structure
  - Audit trail
- Section 14: Compliance
  - Compliance with laws, policies and standards
  - Assessment, corrective action
  - Manual checks: crypto, privacy, intellectual properties ….
  - Technical checks: vulnerability, penetrating testing, ….
  - Protection of information system audit tools

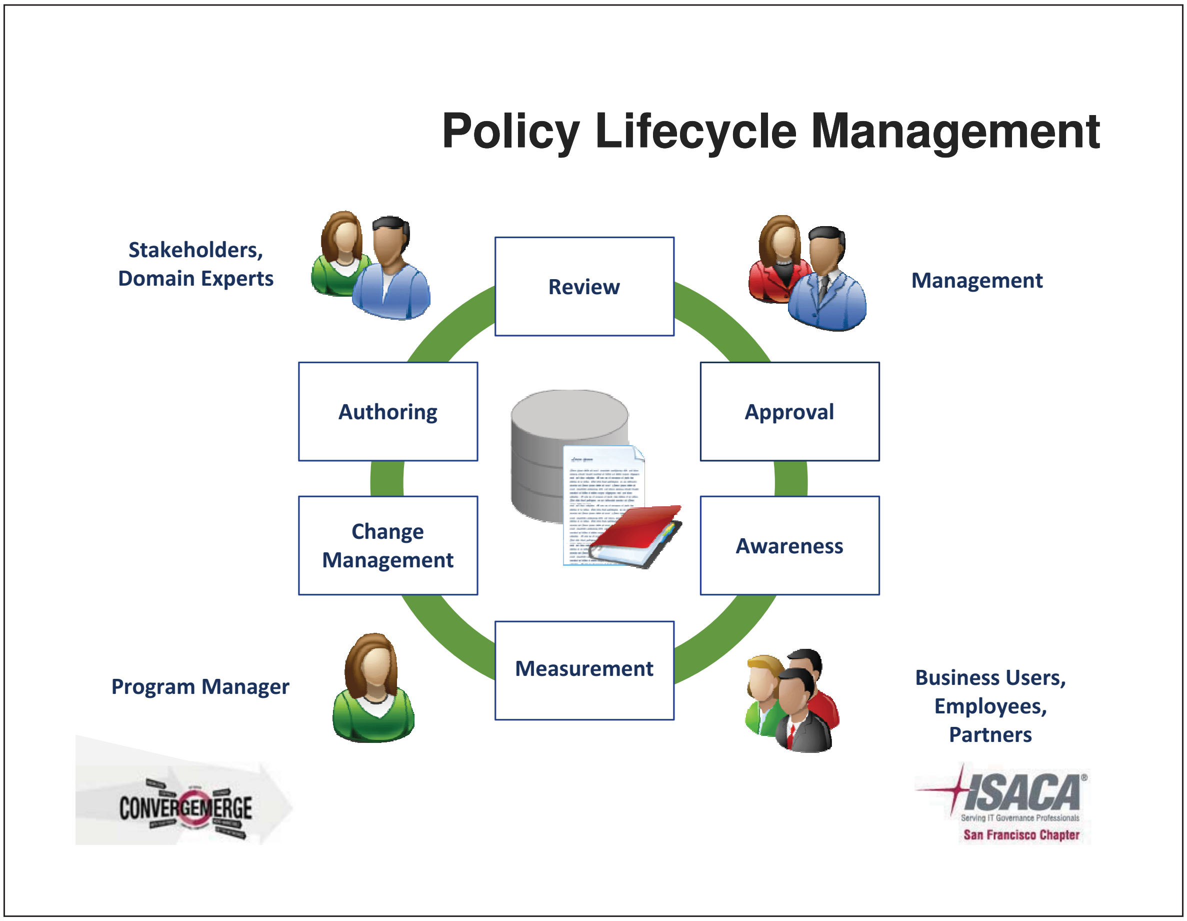
ISACA Serving IT Governance Professionals San Francisco Chapter

# Agenda

- Technologies for policy management
  - Challenges
  - Policy life cycle and enabling technologies
  - Collaboration, workflow, assessment, content management
  - Why not SharePoint?
- Technologies for compliance management
  - Challenges
  - Closed-loop, continuous compliance
  - Process automation/self assessment, controls automation, reports and dashboards, remediation automation
- Summary, Q&A

# Policy Management Challenges

- Collaboration between many stakeholders
  - Authors, contributors, reviewers, & approvers
  - Manage document versions & revisions, unintented overwrite
  - Different review processes by policy type, by dept., by region..
  - Different approval requirements by policy type, by dept…
- Inconsistent policy document format
  - Multiple policy types and templates
  - Not following best practice, not using approved verbiage
- Raise policy awareness across diverse employee base
  - Target only applicable policies for each employee
  - Measure comprehension and awareness levels
  - Different distribution channels for different policy types



# Policy Lifecycle Management

Stakeholders, Domain Experts

Review

Management

Authoring

Approval

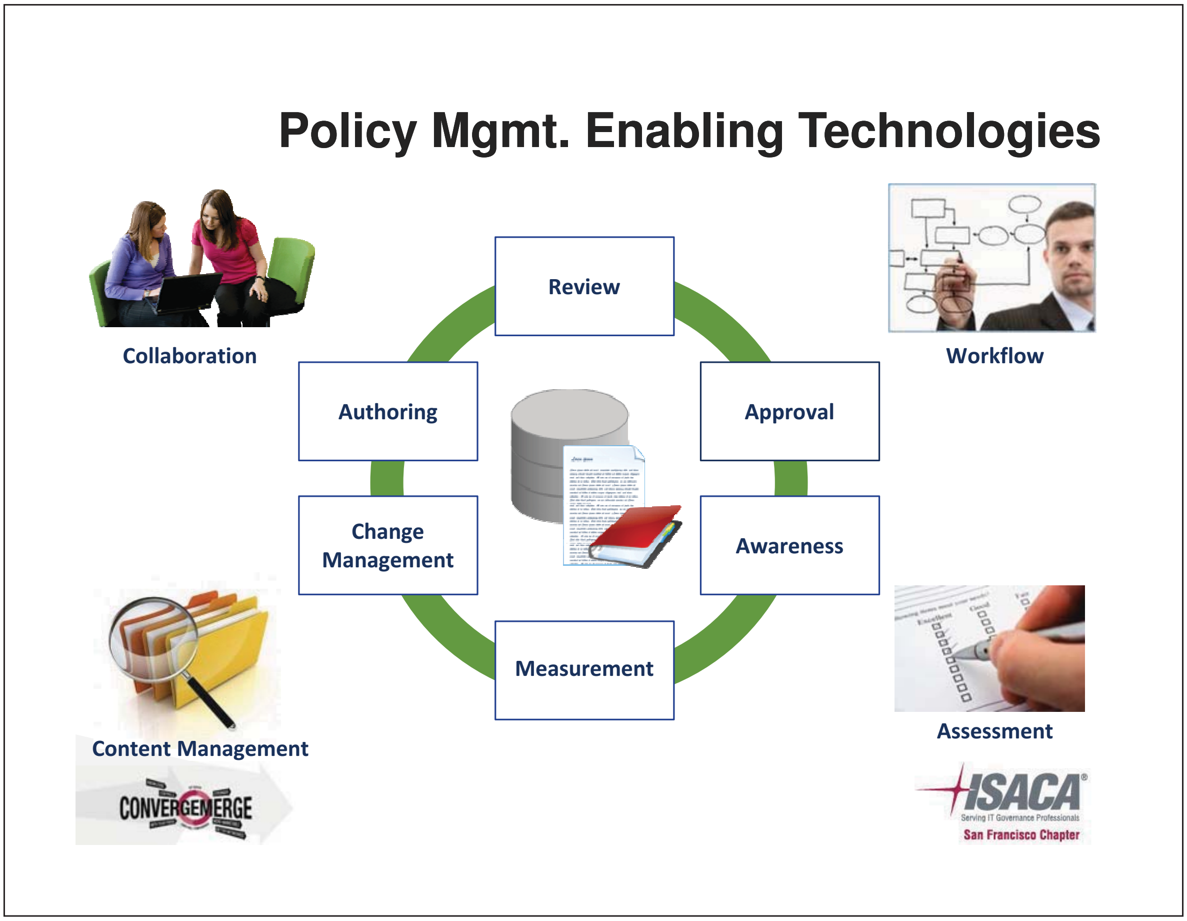
Change Management

Awareness

Measurement

Program Manager

Business Users, Employees, Partners



# Policy Mgmt. Enabling Technologies

Collaboration

Review

Workflow

Authoring

Approval

Change Management

Awareness

Measurement

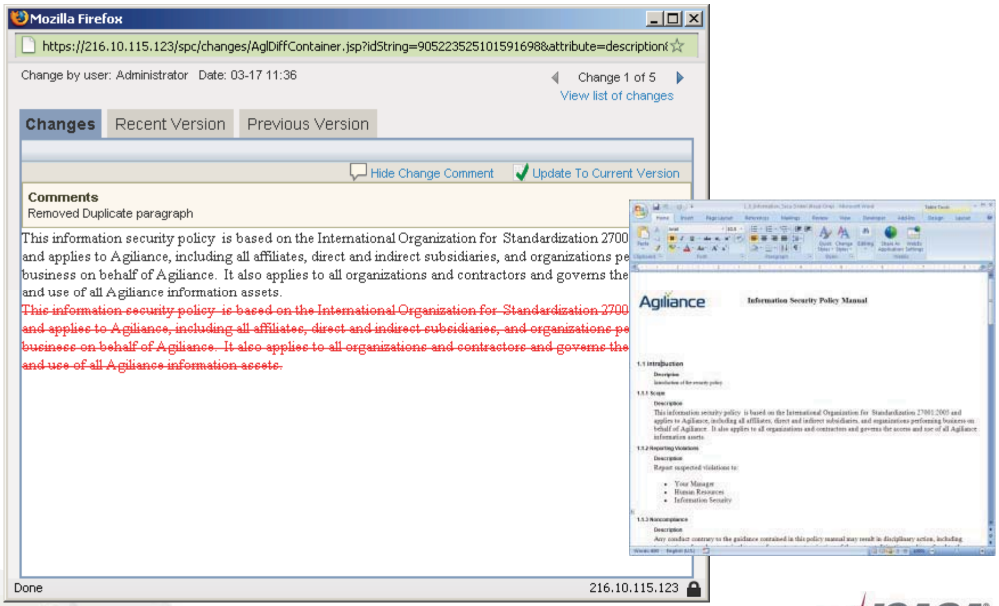
Content Management

Assessment

# Collaboration Technologies

- Multiple user simultaneous/sequential edit
- Role based access: owner, contributor, reviewer
- Track versions and revisions
- Policy template for structure, format, and verbiage
- What-you-see-is-what-you-get user interface
- Visual comparison tool
- Granular search down to policy section

# Collaborative Policy Authoring & Review



https://216.10.115.123/spc/changes/AglDiffContainer.jsp?idString=9052235251015916988attribute=description(

Change by user: Administrator Date: 03-17 11:36

**Comments**
Removed Duplicate paragraph

This information security policy is based on the International Organization for Standardization 2700 and applies to Agiliance, including all affiliates, direct and indirect subsidiaries, and organizations pe business on behalf of Agiliance. It also applies to all organizations and contractors and governs the and use of all Agiliance information assets.

~~This information security policy is based on the International Organization for Standardization 2700 and applies to Agiliance, including all affiliates, direct and indirect subsidiaries, and organizations pe business on behalf of Agiliance. It also applies to all organizations and contractors and governs the and use of all Agiliance information assets.~~

**Information Security Policy Manual**

1.1 Introduction

Description
Introduction of the security policy

1.1.1 Scope

Description
This information security policy is based on the International Organization for Standardization 27001:2005 and applies to Agiliance, including all affiliates, direct and indirect subsidiaries, and organizations performing business on behalf of Agiliance. It also applies to all organizations and contractors and governs the access and use of all Agiliance information assets.

1.1.2 Reporting Violations

Description
Report suspected violations to:

- Your Manager
- Human Resources
- Information Security

1.1.3 Noncompliance

Description
Any conduct contrary to the guidance contained in this policy manual may result in disciplinary action, including

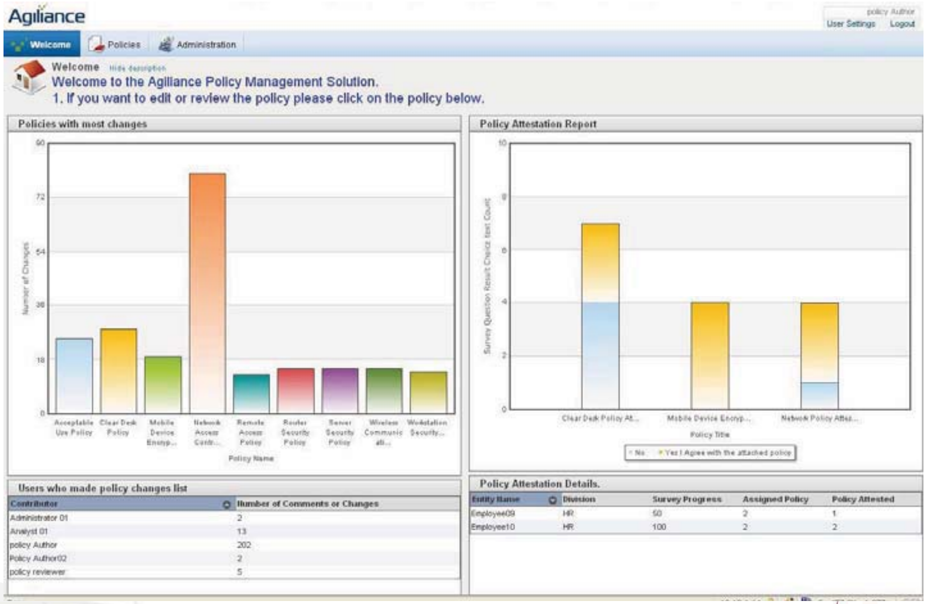
## Workflow Technologies

- Flexibility with configuration, no coding or scripting
- Consistent workflow with other GRC functions
- Routing, escalation, notification, delegation
- Different processes by policy type, department, region...
- Different approval modes, single, multiple, voting…
- Collaboration enabled at every stage

## Assessment Technologies

- Distribution portal
- Target applicable policies for each employee
- Simple attestation
- Measure comprehension and awareness levels with quiz
- Link to incidents and controls to measure policy effectiveness
- Dashboard for compliance & awareness
- Supplement with training programs

# Policy Dashboard



Welcome Hide description

Welcome to the Agiliance Policy Management Solution.

1. If you want to edit or review the policy please click on the policy below.

Users who made policy changes list

| Contributor | Number of Comments or Changes |
|---|---|
| Administrator 01 | 2 |
| Analyst 01 | 13 |
| policy Author | 202 |
| Policy Author02 | 2 |
| policy reviewer | 5 |

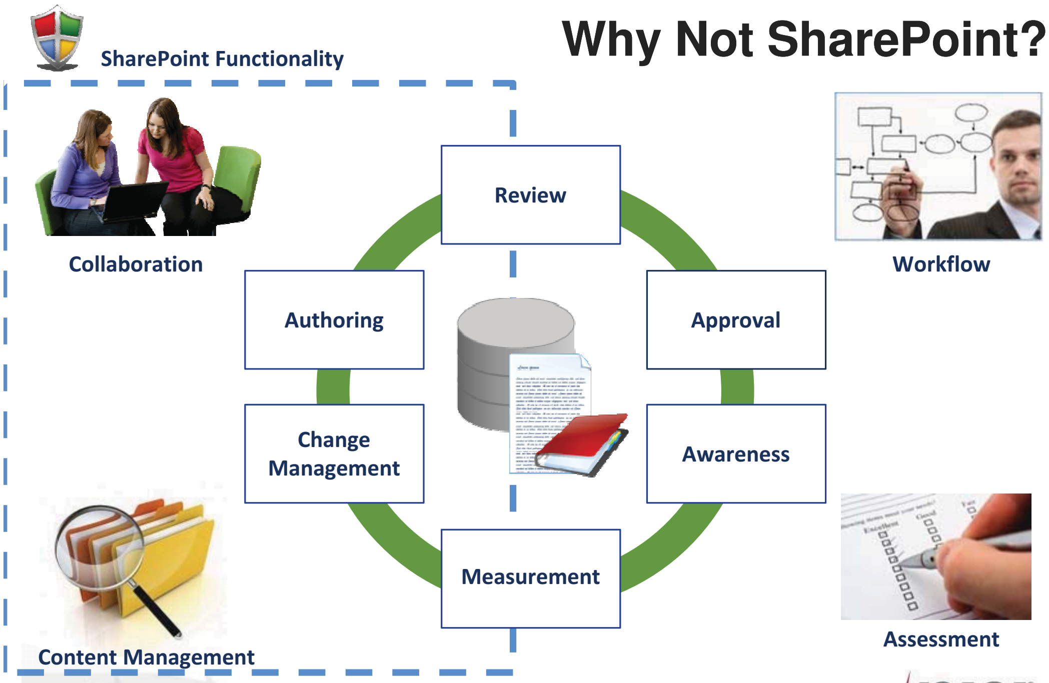
Policy Attestation Details.

| Entity Name | Division | Survey Progress | Assigned Policy | Policy Attested |
|---|---|---|---|---|
| Employee09 | HR | 50 | 2 | 1 |
| Employee10 | HR | 100 | 2 | 2 |

# Content Management Technologies

- Manage versions and revisions
- Full document lifecycle management with audit trail
- Role based access control
- Archival and backup
- Encryption and rights management if necessary

## Why Not SharePoint?



**"… He has erected a multitude of New Offices, and sent hither swarms of Officers to harass our people, and eat out their substance."**

A) American grievance against King George III of England in 1776

B) The new reality of regulatory compliance in 2010

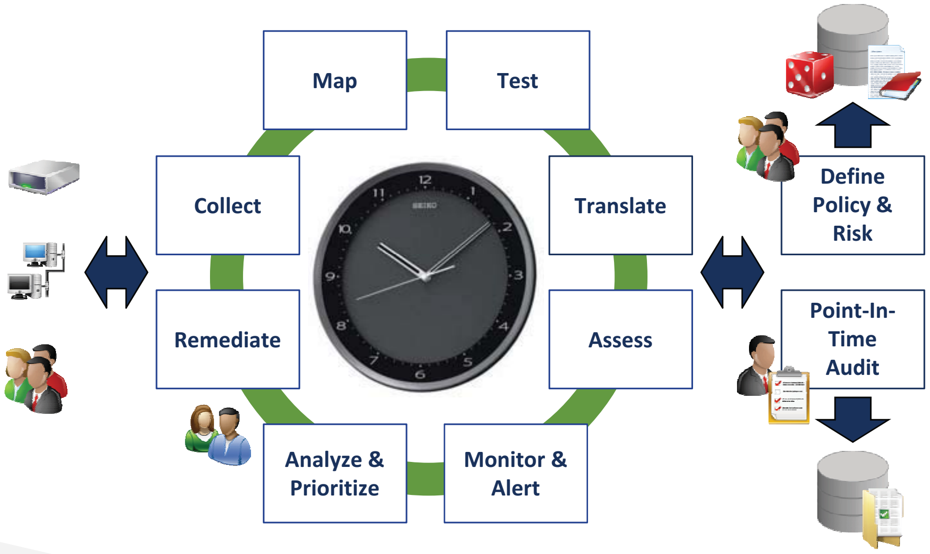
In CONGRESS, July 4, 1776.

The unanimous Declaration of the thirteen united States of America,

## Compliance Mgmt. Challenges

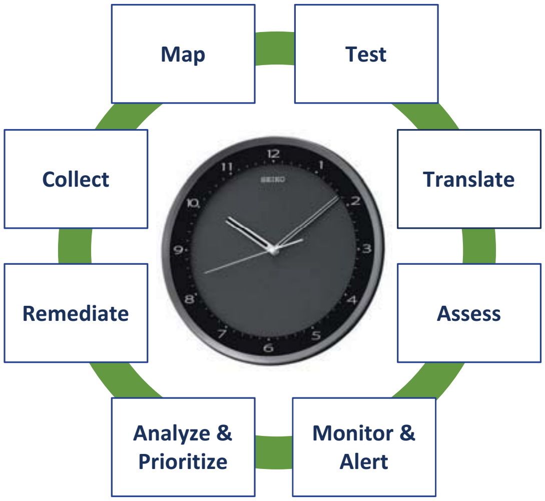
- Large number of country, state & industry specific compliance mandates
  - Forever trying to keep up with the mandates
- Independent and overlapping assessment efforts
  - Repetitive manual work for compliance team
  - Asset owners answer the same questions multiple times for different assessment efforts
- Compliance is a periodic "get it over with" exercise
  - It's viewed as a cost-center and a non-strategic effort
  - Under funded and under staffed
- Assessment effort is not tied into enterprise or operational risk

## Continuous, Closed Loop Compliance



# Compliance Automation Technologies

Control Automation



Process Automation Self Assessment

Remediation Automation

Reports & Dashboards

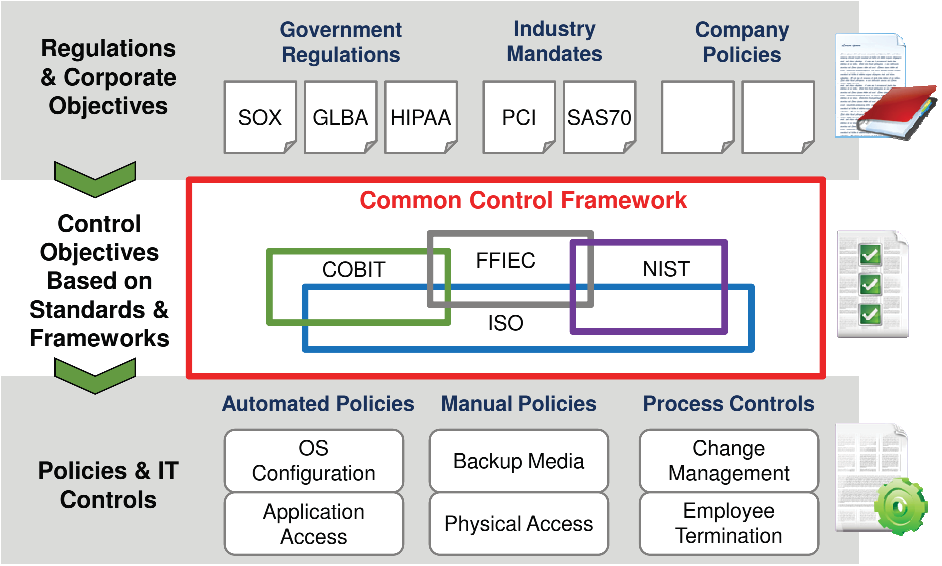
# Process Automation Self-Assessment

- 60% of control assessments are still manual
- Smart e-surveys with out-of-the-box contents
- Common control framework
- Classification and control assessment surveys
- Automated control assignment based on asset attributes
- Flexible workflow for assessment & mitigation
- Response negotiation and exception management
- Attach evidence and supporting documents
- Assessment scheduling

# Control Automation: You Already Have The Data

- eSurvey
- Configuration Management
- Vulnerability Management
- Incident Management
- DB Configuration & Access Checks
- Identity & Access Control Checks
- Application Controls Checks
- Segregation of Duties Checks
- Others

# Common Control Framework



Regulations & Corporate Objectives

Government Regulations: SOX, GLBA, HIPAA

Industry Mandates: PCI, SAS70

Company Policies

Control Objectives Based on Standards & Frameworks

Common Control Framework: COBIT, FFIEC, NIST, ISO

Policies & IT Controls

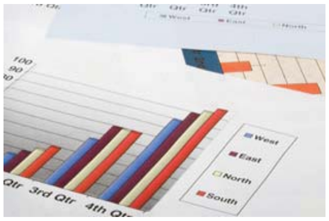
Automated Policies: OS Configuration, Application Access

Manual Policies: Backup Media, Physical Access

Process Controls: Change Management, Employee Termination

## Control Automation

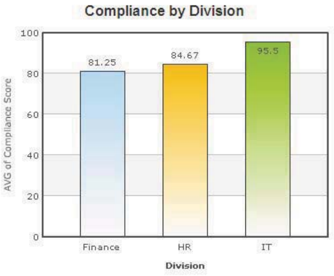
- Collect available data from existing management and security tools
- Flat file import is the bare minimum, rich data entities will require API/WS interfaces
- Out-of-the-box connectors, generic connectors, and connector development tools
- Automatically pass/fail control based on imported data
- Optional human review
- Integrated automated and self-assessments
- Critical for continuous, closed-loop, risk based process

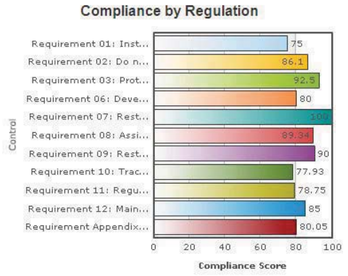


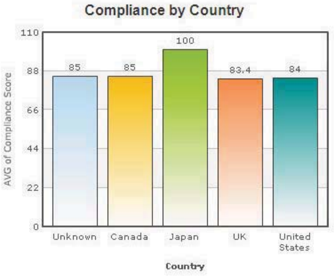
## Reports, Dashboards, Metrics

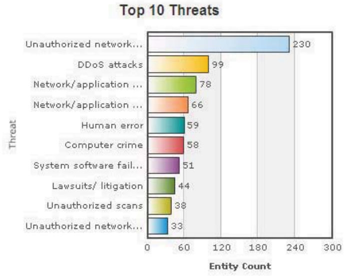
- You can’t improve on what you don’t measure
- Program and administration dashboards
- Management, executive, and audit reports
- Role aware reports and dashboards
- Automated, any-time report generation
- Report builder, incorporating objectives, control statements, assessment results, narratives, recommendations …
- Integrated compliance and risks metrics
- Tie incident data into measurements

# Start With The Dashboard





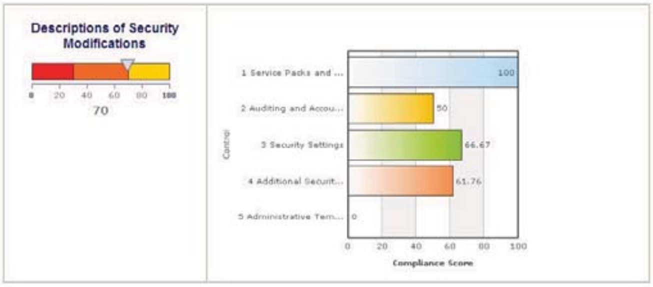




# Integrated Compliance & Risk Reports

### Compliance By PCI DSS Requirements

The following section provide the overall compliance score for each section and the compliance score for each sub-requirements



### Descriptions of Security Modifications

**1 Service Packs and Security Updates**

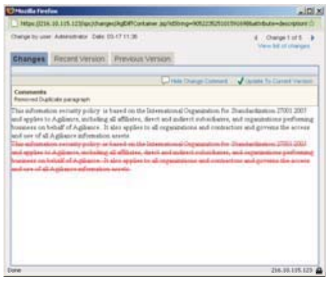
*Microsoft periodically distributes large updates to its operating systems in the form of Service Packs, as often as once every few months, or less frequently. Service Packs include all major and minor fixes up to the date of the service pack, and are extensively tested by Microsoft prior to release. In light of the vast number of applications available, it is entirely possible that a bug in a Service Pack may not be discovered, and may slip through this engineering analysis process. Service Packs should be used in a test environment before being pushed into production. If a test system is not available, wait a week or two after the release of a Service Pack, and pay attention to the Microsoft web site for potential bug reports. Additional mailing list and Internet resources are listed in the appendices of this document. It is important to be aware that Service Packs and Security Updates are not*

## Remediation Automation

- Automated mitigation
- Handled by existing security and IT management tools
  - Identity and access management
  - System provisioning
  - Configuration management
- These tools have limited and overlapping GRC capabilities → need to rationalize solution architecture

## Policy Management Technology Summary

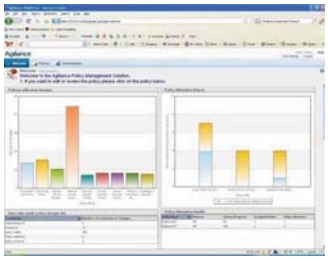
- Collaborative platform for policy authoring, review & approval
- Document management infrastructure with full audit
- Easy to use for business users: WYSIWYG, search, …
- Promote and measure policy awareness & compliance
- Link policy to process and technical controls, incidents and risks



Comments
Removed Duplicate paragraph

This information security policy is based on the International Organization for Standardization 27001 2005 and applies to Agiliance, including all affiliates, direct and indirect subsidiaries, and organizations performing business on behalf of Agiliance. It also applies to all organizations and contractors and governs the access and use of all Agiliance information assets.

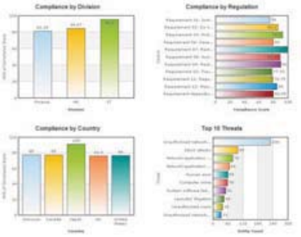
~~This information security policy is based on the International Organization for Standardization 27001 2005 and applies to Agiliance, including all affiliates, direct and indirect subsidiaries, and organizations performing business on behalf of Agiliance. It also applies to all organizations and contractors and governs the access and use of all Agiliance information assets.~~



Welcome to the Agiliance Policy Management Solution

## Compliance Mgmt. Technology Summary

- Integrated compliance solution for automated and self-assessment
- Connectors for automated testing
- Out-of-the-box content for the most popular regulatory mandates & compliance frameworks
- Test once and comply many
- Workflow based automation & collaboration platform
- Automated and dynamic report generation



Compliance By PCI DSS Requirements
Descriptions of Security Modifications
Descriptions of Security Modifications
1 Service Packs and Security Updates

## To Learn More: www.agiliance.com

# Data Security

Roxana Bradescu
Senior Director, Product Marketing, Data Security
Oracle

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

## ISO 27002 Says…

- Section 7: Asset Management
- Section 11: Access Control
  - Information classification
  - Information labeling and handling
  - Encryption
  - Data protection
  - Access control policy and user access management
- Other relevant sections on information backup, protection of organizational records, privacy, encryption, audit logging

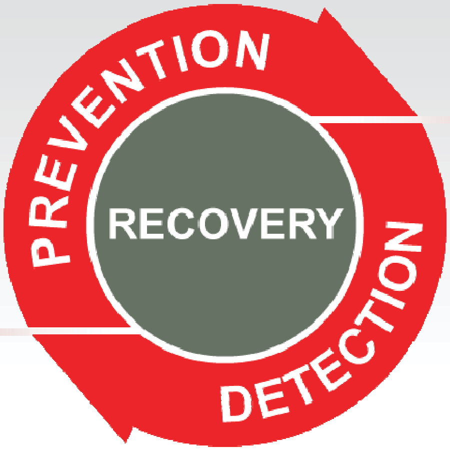
ISACA
Serving IT Governance Professionals
San Francisco Chapter

## Agenda

- Technologies for prevention
- Technologies for detection
- Defense in-depth
- Summary, Q&A

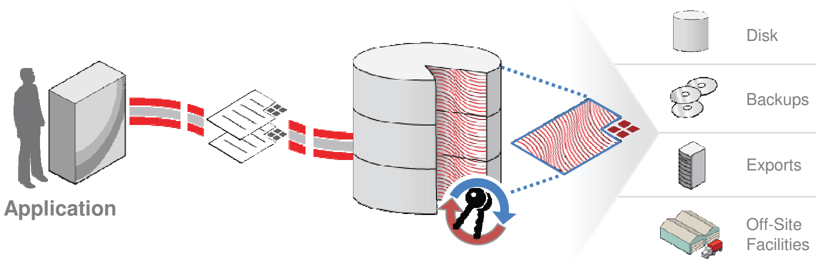
## Securing Data in Your Database

- Encryption
- Masking
- Classification
- Access Control



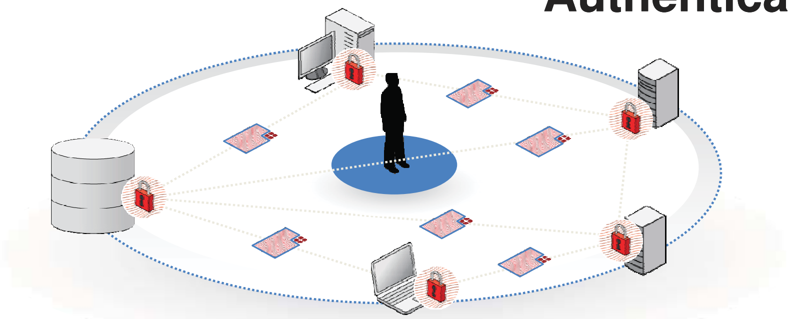
- Activity Monitoring
- Change Tracking
- Discovery and Assessment
- Secure Configuration

# Data Encryption



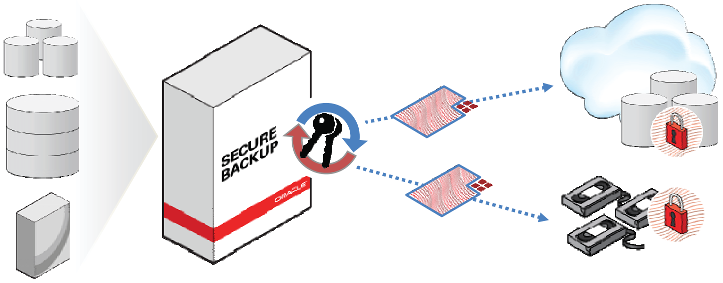
- Complete encryption for data at rest
- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management

# Network Encryption & Strong Authentication



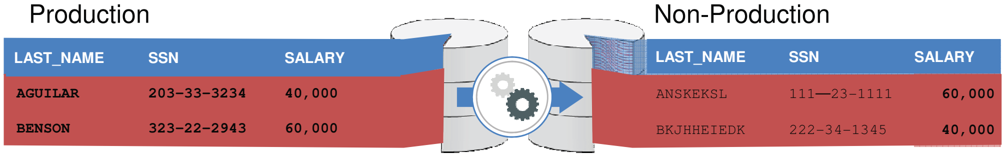
- Standard-based encryption for data in transit
- Strong authentication of users and servers
- No infrastructure changes required
- Easy to implement

# Secure Backup



- Secure data archival to tape or cloud
- Easy to administer key management
- Fastest Oracle Database tape backups
- Leverage low-cost cloud storage

# Data Masking
# Irreversible De-Identification



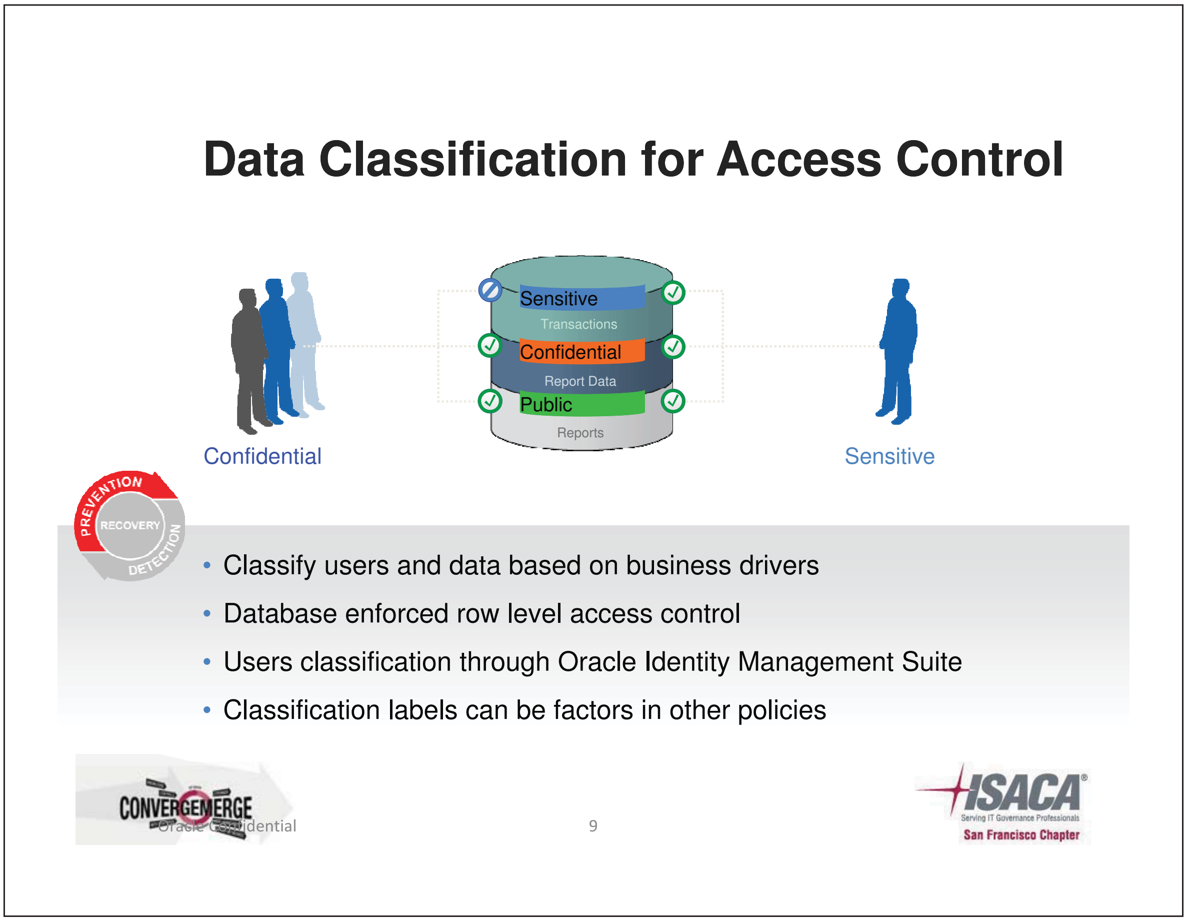
Production

| LAST_NAME | SSN | SALARY |
|---|---|---|
| AGUILAR | 203-33-3234 | 40,000 |
| BENSON | 323-22-2943 | 60,000 |

Non-Production

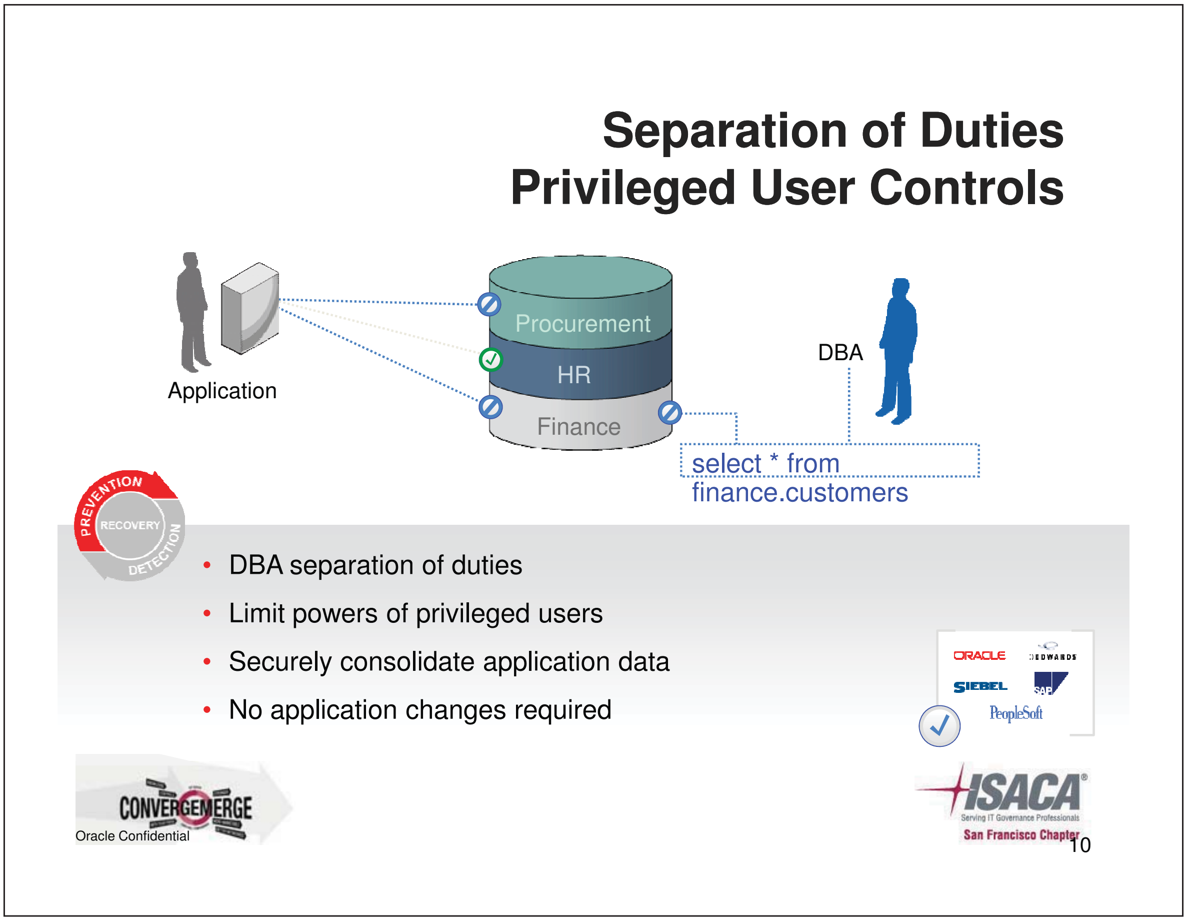
| LAST_NAME | SSN | SALARY |
|---|---|---|
| ANSKEKSL | 111—23-1111 | 60,000 |
| BKJHHEIEDK | 222-34-1345 | 40,000 |

- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Sensitive data never leaves the database
- Extensible template library and policies for automation



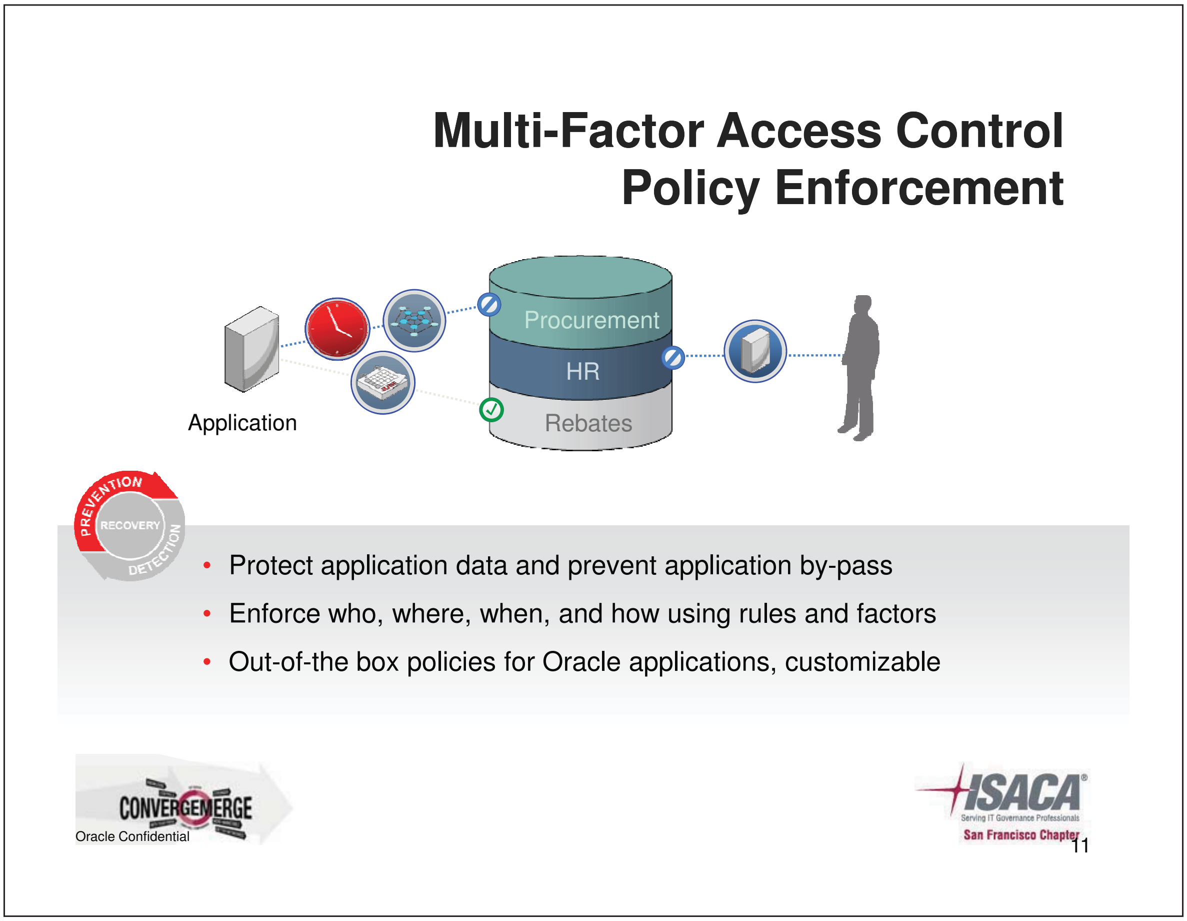
# Data Classification for Access Control

- Classify users and data based on business drivers
- Database enforced row level access control
- Users classification through Oracle Identity Management Suite
- Classification labels can be factors in other policies



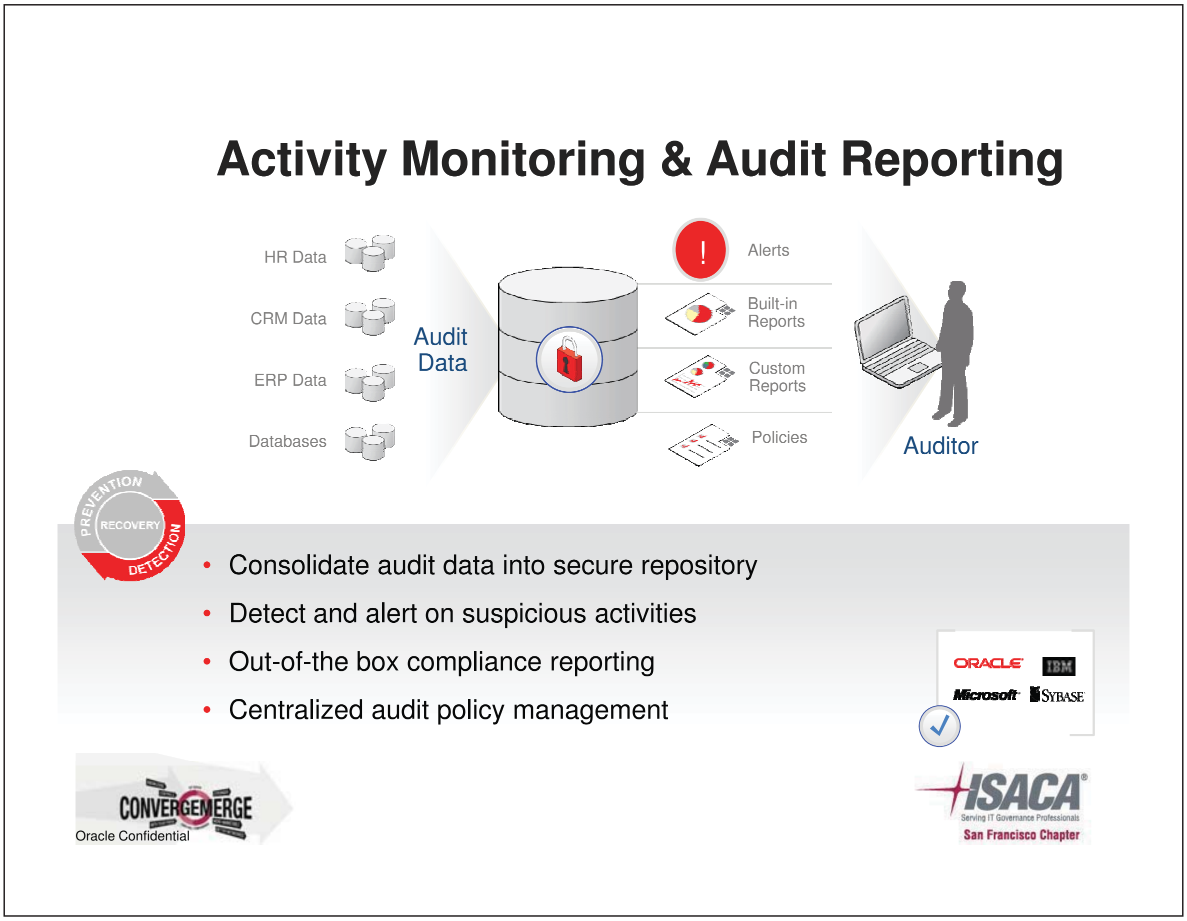
# Separation of Duties Privileged User Controls

- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required



# Multi-Factor Access Control Policy Enforcement

- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

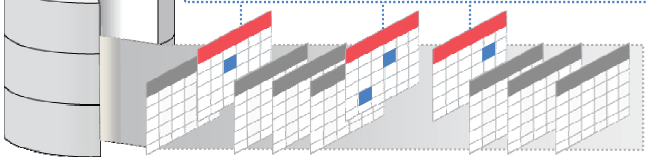


# Activity Monitoring & Audit Reporting

- Consolidate audit data into secure repository
- Detect and alert on suspicious activities
- Out-of-the box compliance reporting
- Centralized audit policy management

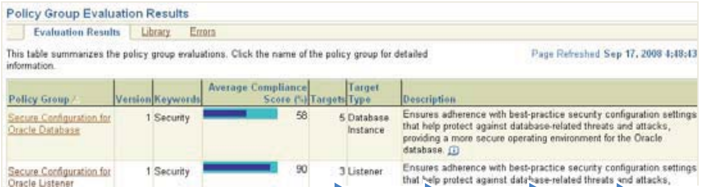
# Secure Change Tracking

```
select salary from emp AS OF TIMESTAMP
'02-MAY-09 12.00 AM‘ where emp.title = ‘admin’
```



- Transparently track data changes
- Efficient, tamper-resistant storage of archives
- Real-time access to historical data
- Simplified forensics and error correction

# Vulnerability Assessment Secure Configuration



Policy Group Evaluation Results

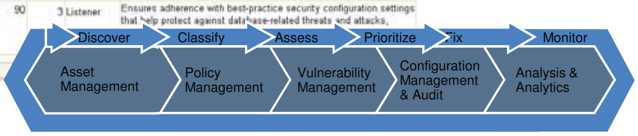
Evaluation Results | Library | Errors

This table summarizes the policy group evaluations. Click the name of the policy group for detailed information.

Page Refreshed Sep 17, 2008 4:48:43

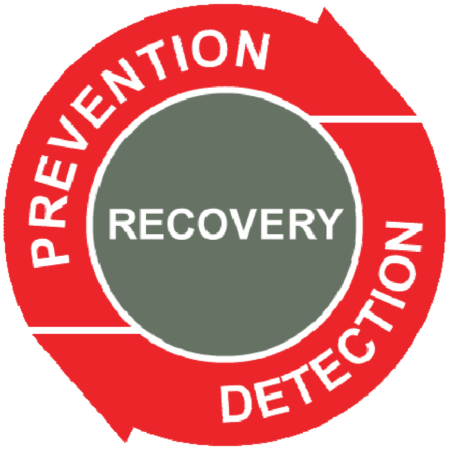
| Policy Group | Version | Keywords | Average Compliance Score (%) | Targets | Target Type | Description |
|---|---|---|---|---|---|---|
| Secure Configuration for Oracle Database | 1 | Security | 58 | 5 | Database Instance | Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for the Oracle database. |
| Secure Configuration for Oracle Listener | 1 | Security | 90 | 3 | Listener | Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks, |

Evaluation Results | Library | Errors



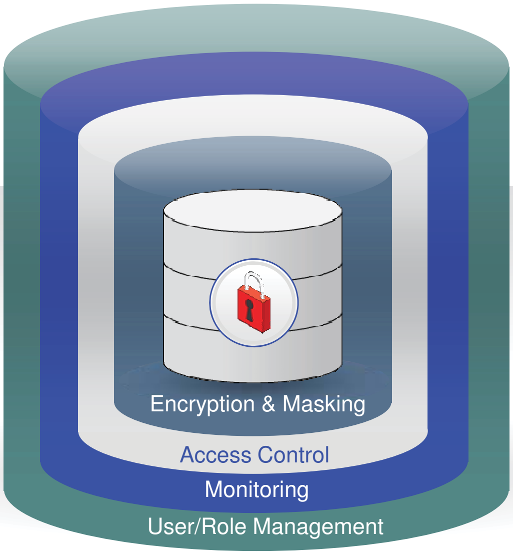
- Database discovery
- Continuous scanning against 375+ best practices and industry standards, extensible
- Detect and prevent unauthorized configuration changes
- Change management compliance reports

# Complete Database Security Solution

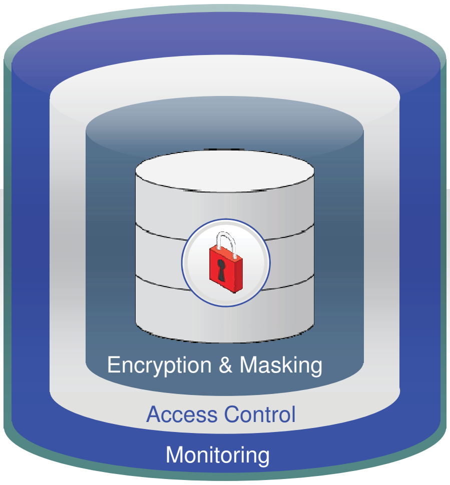


- Data Encryption
- Network Encryption
- Strong Authentication
- Secure Backup
- Data Masking
- Data Classification
- Separation of Duties
- Privileged User Control
- Multi-Factor Authentication
- Monitoring & Audit
- Change Tracking
- Vulnerability Scanning
- Secured Configuration

# Database Defense-in-Depth



# Database Defense-in-Depth



## Monitoring

- Configuration  Management
- Audit Vault
- Total Recall

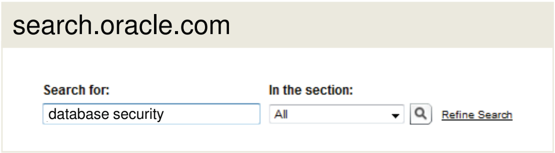
## Access Control

- Database Vault
- Label Security

## Encryption & Masking

- Advanced Security
- Secure Backup
- Data Masking

# For More Information



search.oracle.com

Search for: database security

In the section: All

or

oracle.com/database/security

# Identity Management

Eric Leach
Director, Product Management, Identity Management
Oracle

ISACA Serving IT Governance Professionals San Francisco Chapter

## ISO 27002 Says…

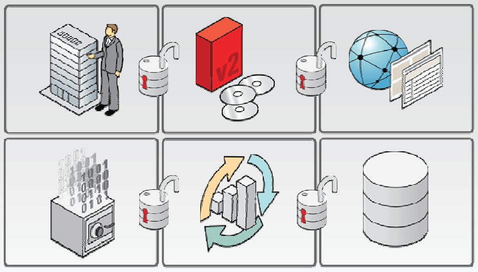
- Section 11: Access Control
  - Access control policy
  - Information access and data protection
  - Role based access, privilege management
  - Password management
  - Access request, approval and review processes
  - Removal of access rights
- Other relevant sections on system documentation security, physical security, human resources security, network security, electronic commerce, on-line transactions

# Agenda

- Enterprise Challenges
- Role Based Access Controls
  - Role Management
  - Provisioning
  - Self-service & Delegated Administration
  - Authentication & SSO
  - Authorization & Entitlements
  - Fraud Prevention
  - Compliance Reporting & Attestation

# Security End-to-End

## Aligning & integrating point solutions

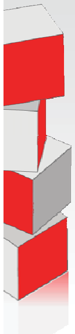


- Context lost across infrastructure tiers
- Partner integration hurdles
- Operational maintenance a major pain point

## Integrated Security

How do I integrate my partners, my apps, my web services, my data – everything?

## Keeping Tabs on $$$

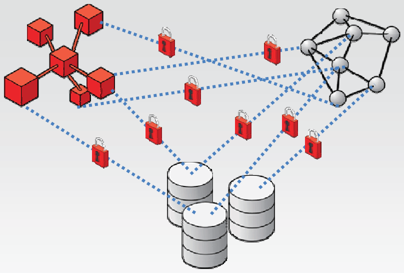


- User Productivity
- Compliance & Remediation Costs
- Unused Assets/Opportunity Costs
- Security Breach Remediation Costs

It Adds Up

## Security Simplified

**Making security easier, simpler, more effective**

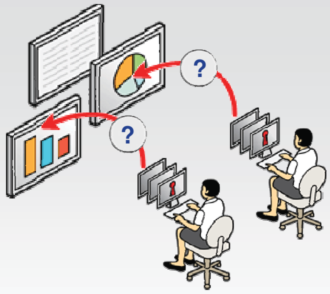


- Fragmented policies & a lack of business friendliness
- Integration & enforcement silos
- Complexity overwhelms business agility

! Enterprise Security is still too complex, too fragmented, and too difficult to integrate!

## Active Compliance

### Richer, more meaningful compliance data



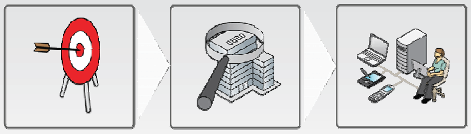
- Determining when and how roles & permissions are used
- Adding “runtime” data to attestation & compliance reports
- Future proofing against additional regulations

### ✓ Compliance 2.0

I can report on “who has access to what” – how do I actively monitor what people are using?

## Risk Mitigation

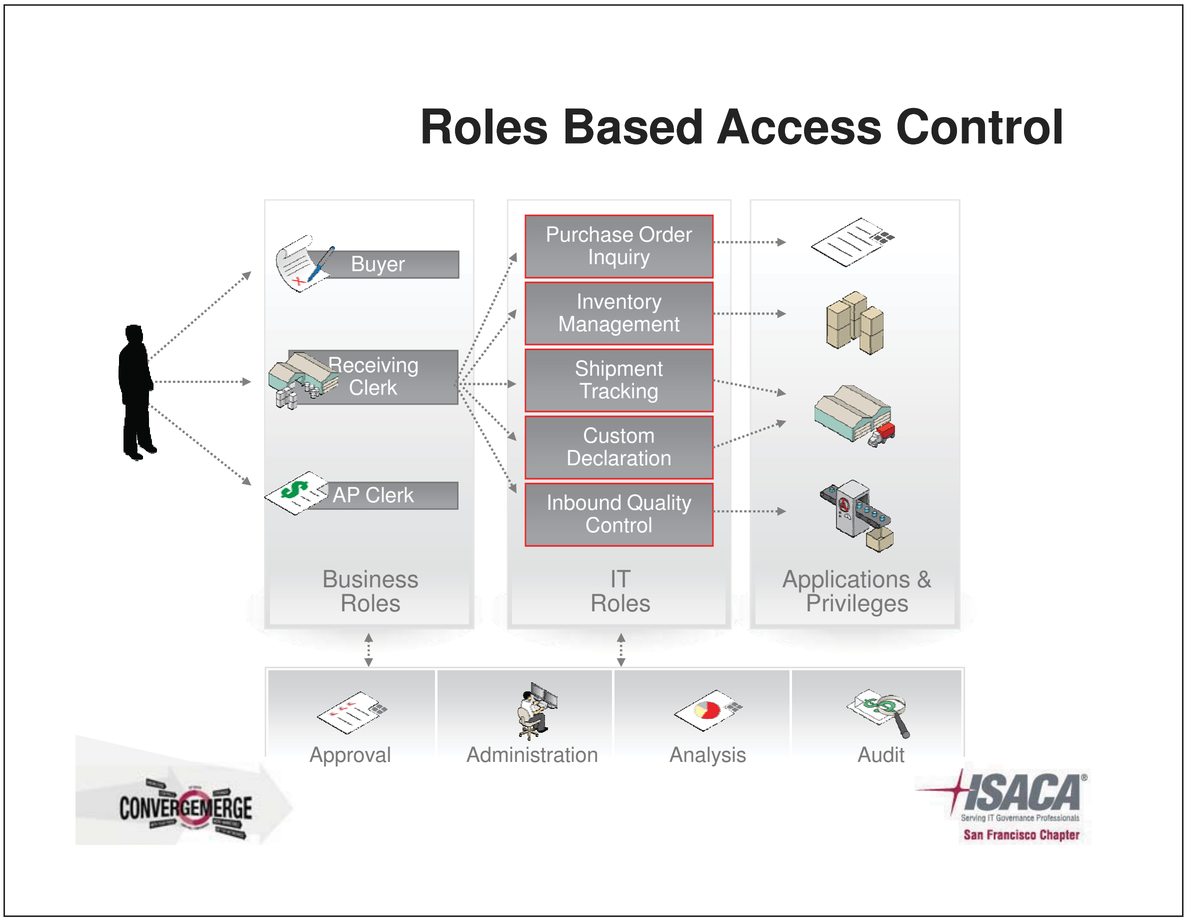
### Adapting security to new threats



- Shifting from reactive to proactive threat mitigation posture
- Quickly identify any anomaly
- Adding cost effective layers to existing apps and data security

### Risk Analytics

I’m not sure of my exposure – what’s my biggest risk? Hackers? Insiders?



# Roles Based Access Control

Purchase Order Inquiry

Buyer

Inventory Management

Receiving Clerk

Shipment Tracking

Custom Declaration

AP Clerk

Inbound Quality Control

Business Roles

IT Roles

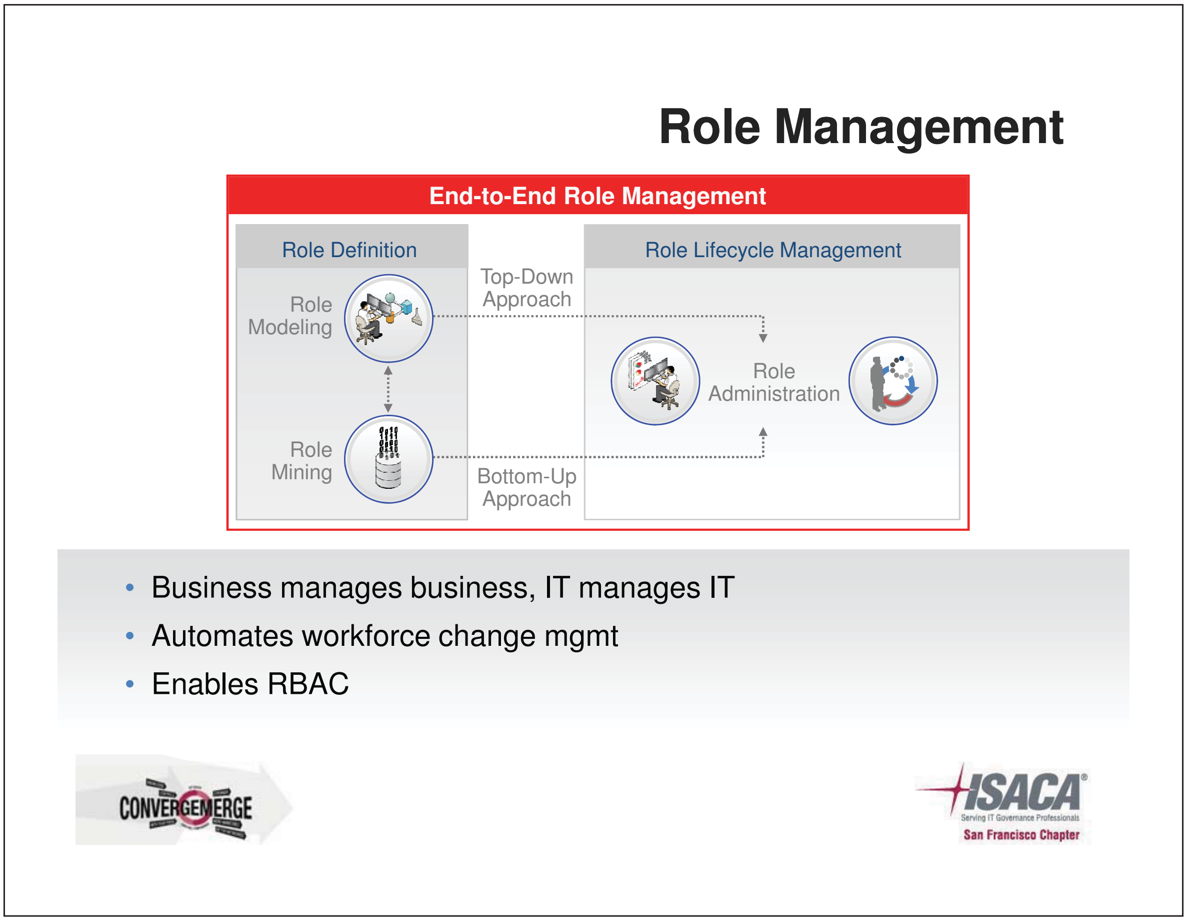
Applications & Privileges

Approval

Administration

Analysis

Audit



# Role Management

End-to-End Role Management

Role Definition

Role Lifecycle Management

Top-Down Approach

Role Modeling

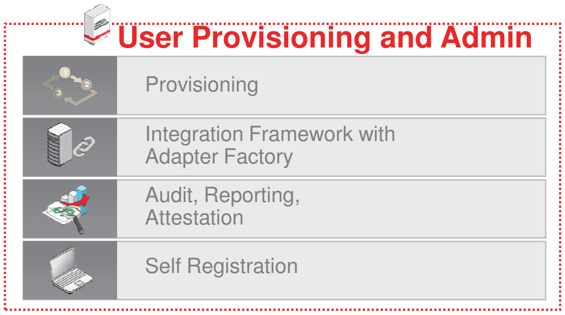
Role Administration

Role Mining

Bottom-Up Approach

- Business manages business, IT manages IT
- Automates workforce change mgmt
- Enables RBAC

# User Provisioning



User Provisioning and Admin

Provisioning

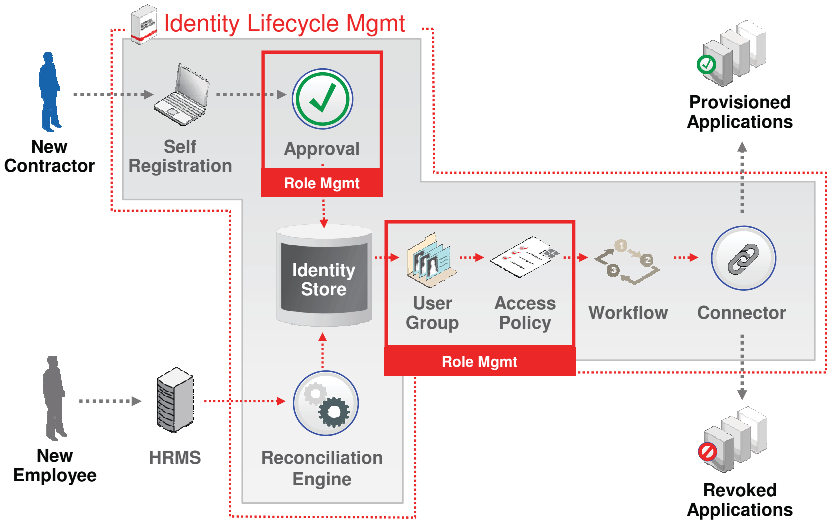
Integration Framework with Adapter Factory

Audit, Reporting, Attestation

Self Registration

- Complete user lifecycle administration and management
- Enforces SoD, compliance
- Eliminates ghost accounts, excess or erroneous privileges

# Policy Based Provisioning



Identity Lifecycle Mgmt

New Contractor

Self Registration

Approval

Role Mgmt

Identity Store

User Group

Access Policy

Role Mgmt

Workflow

Connector

Provisioned Applications

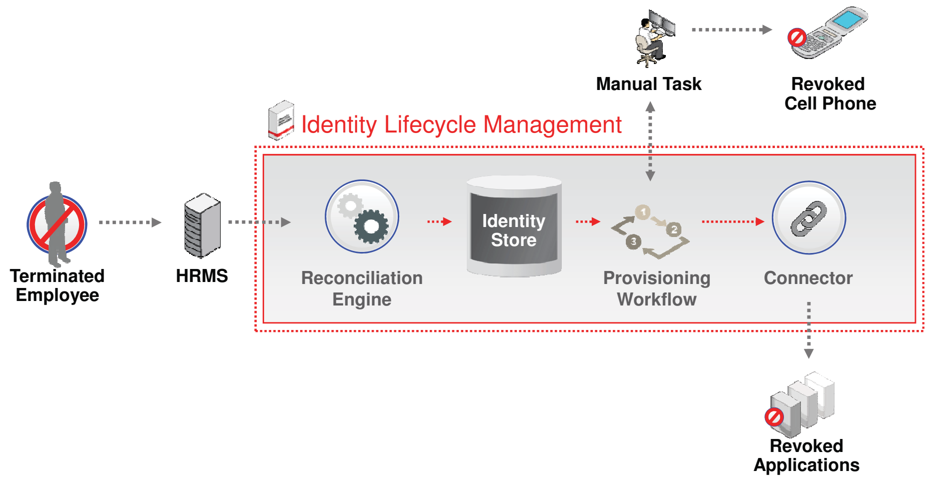
Revoked Applications

New Employee

HRMS

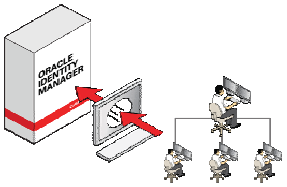
Reconciliation Engine

# Automated De-Provisioning



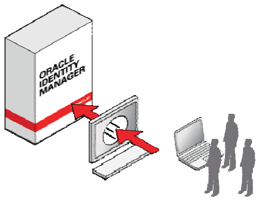
# Self Service and Delegated Admin

## Delegated Admin



Manager assigning proxy user

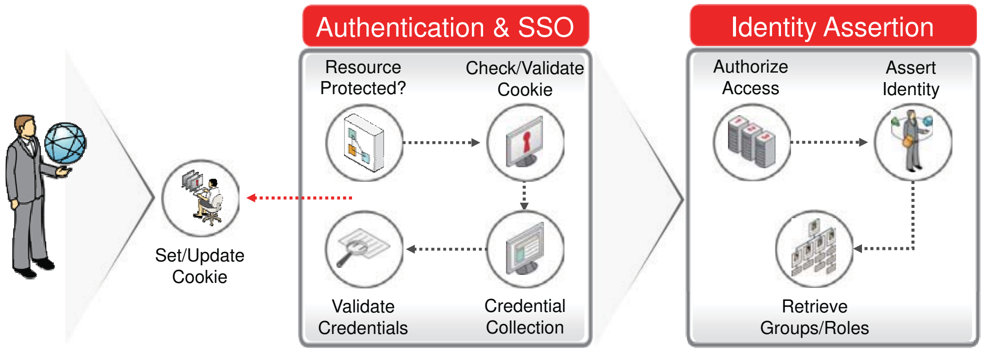
## Self-Service



User doing password reset

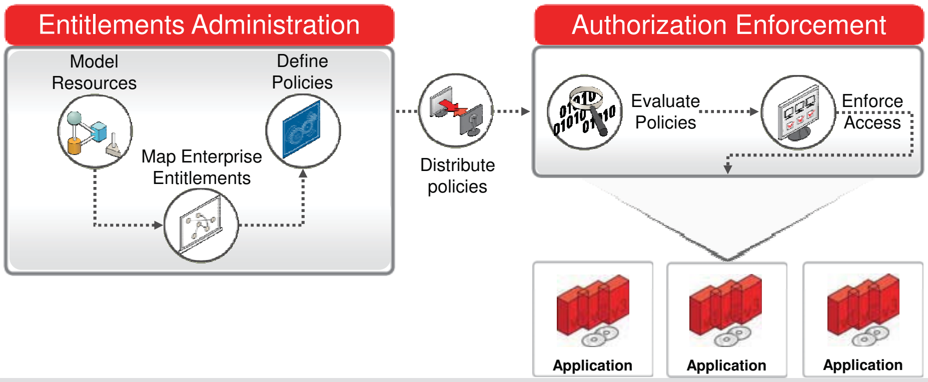
- Self Service Account Requests
- Delegated Administration
- Password Reset and Profile Management

# Single Sign-On



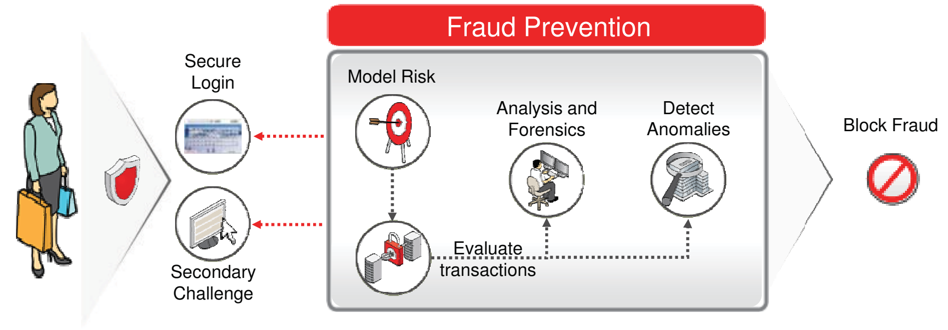
- Business-defined security
- Centralized policies
- Enterprise wide enforcement
- Seamless application integration

# Authorization & Entitlements



- Complete enterprise security
- Fine-grained entitlements
- Granular enforcement & controls

# Fraud Prevention



Fraud Prevention

Secure Login

Secondary Challenge

Model Risk

Analysis and Forensics

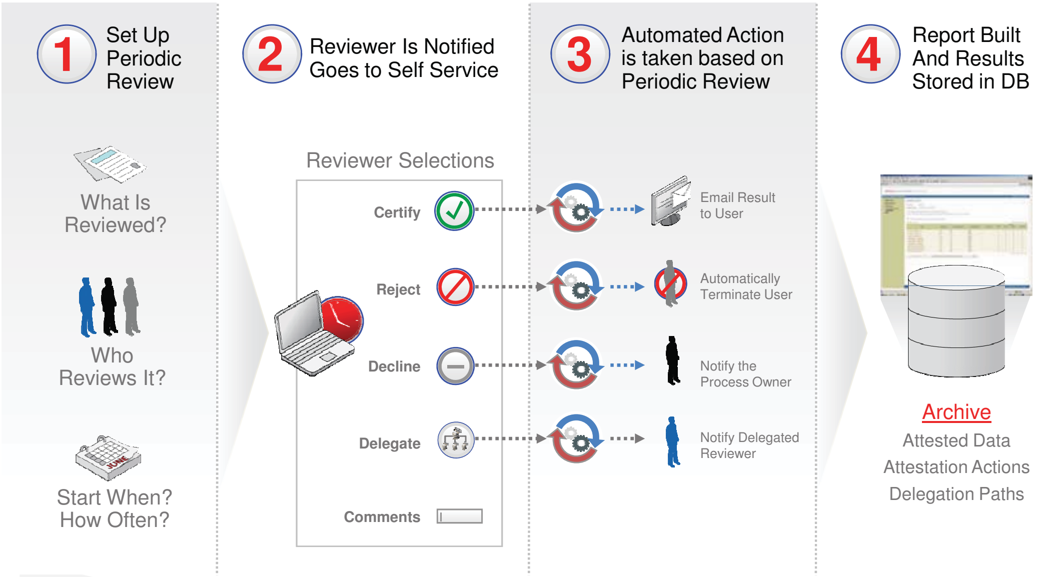
Detect Anomalies

Evaluate transactions

Block Fraud

- Contextual risk evaluation
- Strengthened authentication
- Real-time anomaly detection
- Reporting and forensics

# Web-Based Attestation



1 Set Up Periodic Review

What Is Reviewed?

Who Reviews It?

Start When? How Often?

2 Reviewer Is Notified Goes to Self Service

Reviewer Selections

Certify

Reject

Decline

Delegate

Comments

3 Automated Action is taken based on Periodic Review

Email Result to User

Automatically Terminate User

Notify the Process Owner

Notify Delegated Reviewer

4 Report Built And Results Stored in DB

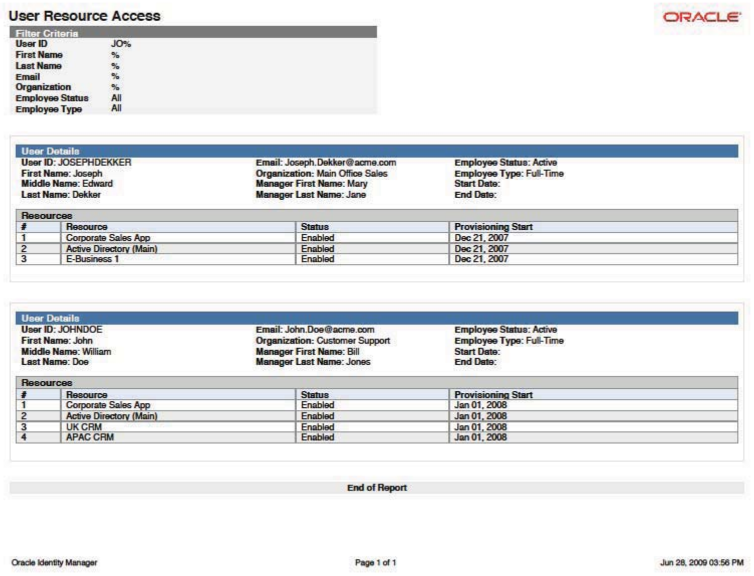
Archive

Attested Data

Attestation Actions

Delegation Paths

# Automated Compliance Reporting



## User Resource Access

ORACLE

**Filter Criteria**

| | |
|---|---|
| User ID | JO% |
| First Name | % |
| Last Name | % |
| Email | % |
| Organization | % |
| Employee Status | All |
| Employee Type | All |

**User Details**

| | | |
|---|---|---|
| **User ID:** JOSEPHDEKKER | **Email:** Joseph.Dekker@acme.com | **Employee Status:** Active |
| **First Name:** Joseph | **Organization:** Main Office Sales | **Employee Type:** Full-Time |
| **Middle Name:** Edward | **Manager First Name:** Mary | **Start Date:** |
| **Last Name:** Dekker | **Manager Last Name:** Jane | **End Date:** |

**Resources**

| # | Resource | Status | Provisioning Start |
|---|---|---|---|
| 1 | Corporate Sales App | Enabled | Dec 21, 2007 |
| 2 | Active Directory (Main) | Enabled | Dec 21, 2007 |
| 3 | E-Business 1 | Enabled | Dec 21, 2007 |

**User Details**

| | | |
|---|---|---|
| **User ID:** JOHNDOE | **Email:** John.Doe@acme.com | **Employee Status:** Active |
| **First Name:** John | **Organization:** Customer Support | **Employee Type:** Full-Time |
| **Middle Name:** William | **Manager First Name:** Bill | **Start Date:** |
| **Last Name:** Doe | **Manager Last Name:** Jones | **End Date:** |

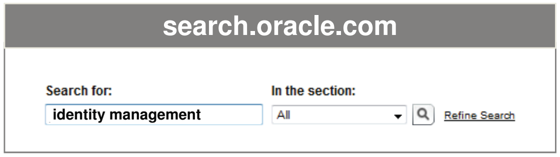
**Resources**

| # | Resource | Status | Provisioning Start |
|---|---|---|---|
| 1 | Corporate Sales App | Enabled | Jan 01, 2008 |
| 2 | Active Directory (Main) | Enabled | Jan 01, 2008 |
| 3 | UK CRM | Enabled | Jan 01, 2008 |
| 4 | APAC CRM | Enabled | Jan 01, 2008 |

**End of Report**

Oracle Identity Manager Page 1 of 1 Jun 28, 2009 03:56 PM

# For More Information



search.oracle.com

Search for: identity management

In the section: All

or

oracle.com/identity

# Streamline & Succeed: Managing and Monitoring Vendor/Partner Risk Management (VRM)

Varun Badhwar

Force.com Security Manager, salesforce.com

September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

## Agenda

- Introduction:
  - Speaker Bio
  - Need for a VRM Program
  - Implementation Challenges
  - Myths
- Implementing a Successful Vendor Risk Management Program:
  - End-to-End Assessment Process
  - Identify Risks
  - Define Controls and Requirements
  - Collect and Analyze Data
  - Conduct Follow-up Testing
  - Determine Assessment Frequency

CONVERGEMERGE

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

## Speaker Bio

- **Current Role:** Define and manage security strategy, and enforce compliance for AppExchange: *a software as a service (SaaS) marketplace with over 800 third-party business applications*

- **Previous Role:** Consultant within KPMG's Information Security practice, focused on ISO 17799/27001/27002 consulting, audit and risk management services

## Why Invest in a VRM Program?

- Compliance Requirements:
  - Regulatory requirements (GLBA, FFIEC, HIPAA, SOX, PCI, etc.)
  - Industry standards (ISO, COBIT, ITIL, etc.)
  - Organizational security requirements

- Business Requirements:
  - Financial loss
  - Reputational damage
  - Attrition and negative impact on the ability to procure additional business

# Common Implementation Challenges

How do I effectively mitigate risks?

How do I stay within my budget?

How do I effectively manage resources?

How do I ensure efficiency, transparency & scalability?

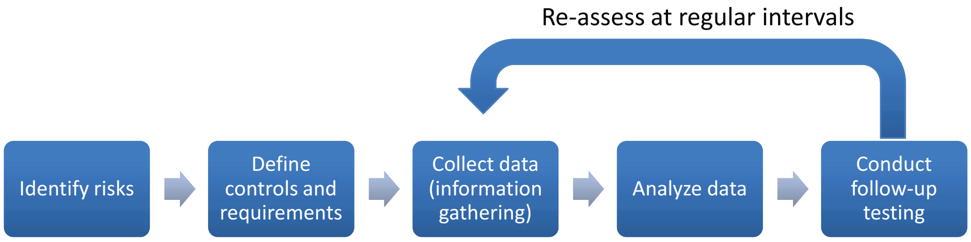
# VRM Myths

- Technology or certain standards/frameworks alone mitigate an organization’s risks
- VRM is a one-time process
- VRM significantly increases costs

# Agenda

- Introduction:
  - Speaker Bio
  - Need for a Vendor Risk Management Program
  - Program Challenges
  - Myths
- Implementing a Successful Vendor Risk Management Program:
  - End-to-End Assessment Process
  - Identify Risks
  - Define Controls and Requirements
  - Collect and Analyze Data
  - Conduct Follow-up Testing
  - Determine Assessment Frequency

# End-to-End Vendor Assessment Process



Re-assess at regular intervals

Identify risks

Define controls and requirements

Collect data (information gathering)

Analyze data

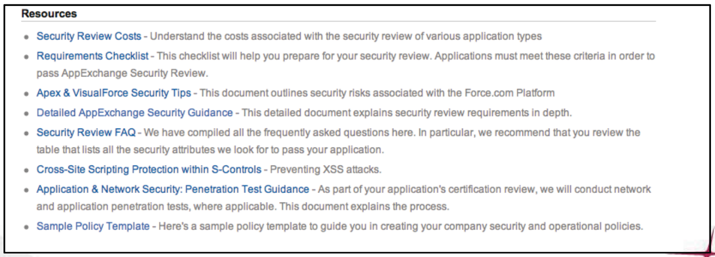
Conduct follow-up testing

# Identify Risks

- Identify risks arising from leveraging 3rd party service providers
- Determine applicable regulatory and/or industry standards
- Rank identified risks by criticality to the organization

# Define Controls & Requirements

- Identify controls to mitigate risks
  - Leverage existing standards (COBIT, ISO, etc.) as guidance – *do not re-invent the wheel*
  - Define "proprietary" controls where adequate coverage is not provided
- Alignment with industry standards ensures higher program adoption (internal and external)
- Comprehensively document requirements, guidelines and standards for 3rd parties



**Resources**

- Security Review Costs - Understand the costs associated with the security review of various application types
- Requirements Checklist - This checklist will help you prepare for your security review. Applications must meet these criteria in order to pass AppExchange Security Review.
- Apex & VisualForce Security Tips - This document outlines security risks associated with the Force.com Platform
- Detailed AppExchange Security Guidance - This detailed document explains security review requirements in depth.
- Security Review FAQ - We have compiled all the frequently asked questions here. In particular, we recommend that you review the table that lists all the security attributes we look for to pass your application.
- Cross-Site Scripting Protection within S-Controls - Preventing XSS attacks.
- Application & Network Security: Penetration Test Guidance - As part of your application's certification review, we will conduct network and application penetration tests, where applicable. This document explains the process.
- Sample Policy Template - Here's a sample policy template to guide you in creating your company security and operational policies.

**An example of resources documented and made available to all AppExchange ISVs**

## Collect & Analyze Data

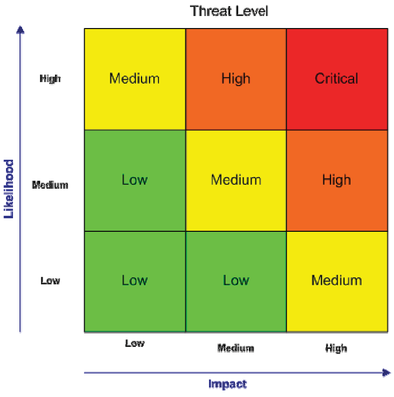
- “Legacy” data collection techniques (Excel, word doc, etc.) are inefficient and non-scalable
- Leverage an automated solution to:
  - Streamline data collection with online surveys
  - Track information (progress, risk, etc.) in real-time
  - Create workflow and approval rules to expedite processing
  - Reduce manual overhead (email follow-ups, data processing and analysis, risk categorization, etc.)
  - Allow staff to focus on core risk-mitigation activities

## Conduct Follow-up Testing

- Validate information provided by 3rd parties
  - Review supporting documentation
  - Conduct “spot checks”
- Conduct hands-on security testing (if applicable)
  - Application scans
  - Network scans, etc.
- Document and report findings
- Establish path to remediation with vendor

# Determine Assessment Frequency

- Effective vendor risk management programs are recurring
  - Organizational risks, security vulnerabilities and 3rd party environments in a state of flux
- Frequency determined by either:
  - Regulatory requirements, or
  - Risk ranking of the service provider based on initial assessment



Threat Level

| Likelihood | Low | Medium | High |
|---|---|---|---|
| High | Medium | High | Critical |
| Medium | Low | Medium | High |
| Low | Low | Low | Medium |
| | Impact | | |

# Conclusion

- An effective VRM program must:
  - Leverage a combination of automated and manual techniques to identify and mitigate risks
  - Increase compliance with regulatory, industry and organizational requirements
  - Include an on-going (periodic) assessment plan
  - Reduce long-term costs to the organization

# Risk Management

Ed King
Vice President, Marketing And Product Management
Agiliance

September 21, 2009 – September 23, 2009

## ISO 27002 Says…

- Section 4: Risk Assessment and Treatment
  - Identify, quantify, and prioritize risks
  - Risk analysis: estimating the magnitude of risks
  - Risk evaluation: comparing the estimated risks against risk criteria to determine the significance of the risks
  - Risk treatment (accept, apply control, avoid, transfer)
- Other relevant sections on segregation of duties, information security co-ordination, external party risks, human resource security, physical security, information and communication risks, system monitoring, vulnerability, business continuity

# Agenda

- Technologies for risk management
  - Challenges
  - Modeling, assessment, measurement
- Risk as anchor for an enterprise GRC platform
  - Why integrated platform?
  - Risk centric approach to compliance
  - Risk as the universal measuring stick
- Q&A

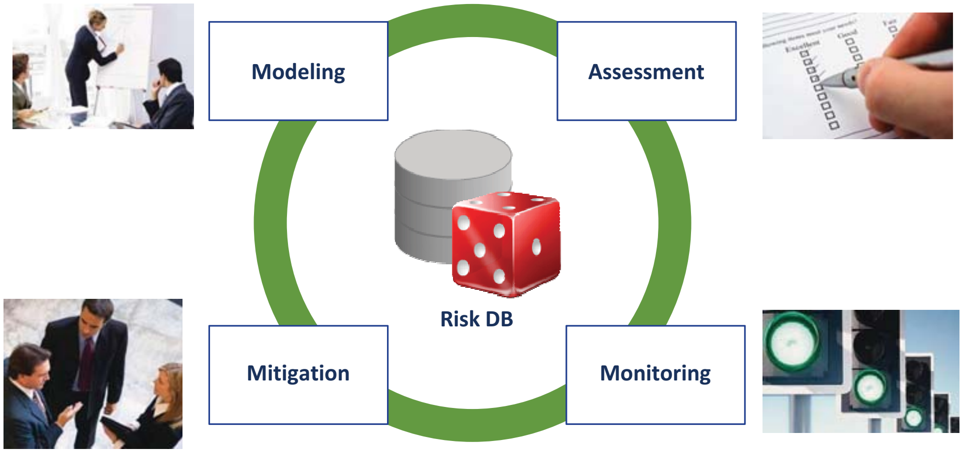
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Risk Management Challenges

- Non-uniform approach to risk
  - Different teams, different systems, different methodologies
  - Separate risks for security, operations, people, environment …
- “The blind mice” view of risk
  - Partial and incomplete risk models
  - Decisions are being made with false sense of security
  - Insiders explore gaps across functional areas
- Risk is inherently real-time
  - Rely on manual processes and point-in-time risk snapshots
  - No means to measure and report in real-time
- Inaccurate assessment of risk
  - Unable to involve domain experts efficiently

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Risk Management



# Risk Modeling

- Collaboration platform for identification and modeling
- Workflow driven review and approval
- Single platform for IT & non-IT risks
- Support for any model NIST, COSO,  BITS, RMA ...
- Configurable risk parameters and calculations
  - E.g: Asset Criticality, Single Loss Expectancy, Annualized Rate of Occurrence, …
- Qualitative and/or quantitative models
  - Monetizable quantitative model
- What-if analysis

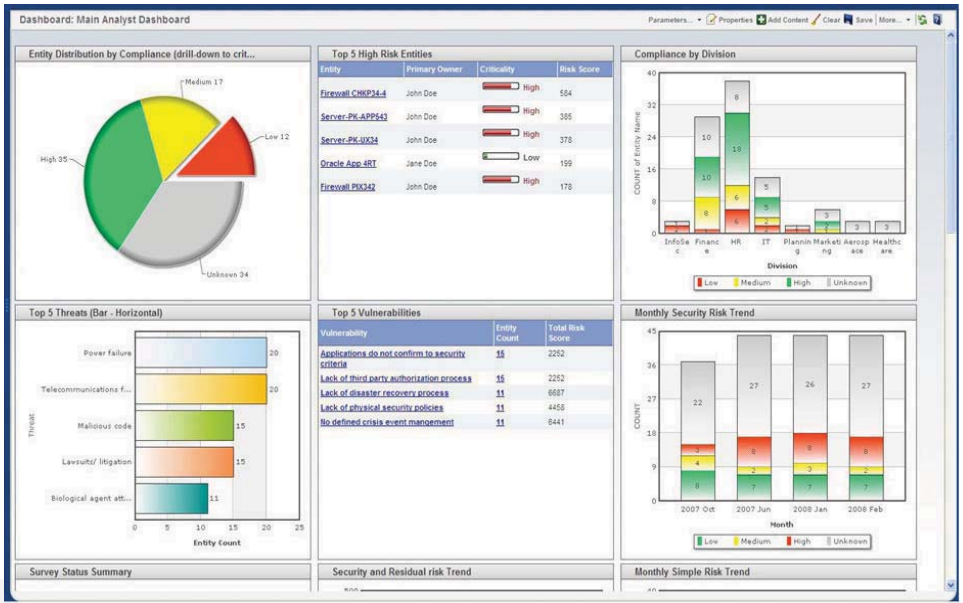
# Risk Assessment

- Assessment survey with out-of-the-box contents
- Automated asset classification based on attributes
- Automated risk calculation based on control assessments
- Workflow based assessment
- Manual overwrite option for automated calculations
- Response negotiation and exception management
- Attach evidence and supporting documents
- Assessment scheduling

# Risk Monitoring

- Real-time Key Risk Indicators, measurement for effectiveness of controls and policies
- The “nerve center” for GRC program
- Comprehensive view of risk:
  - Aggregated view of risk across risk categories
  - Inherent, remedial & current risks
  - Monetizable risk indicators
  - Point-in-time and trending

# Role Based Risk Dashboards


Dashboard: Main Analyst Dashboard
Parameters... Properties Add Content Clear Save More...
Entity Distribution by Compliance (drill-down to crit...
Medium 17
Low 12
High 35
Unknown 34
Compliance by Division
COUNT of Entity Name
InfoSec Finance HR IT Planning Marketing Aerospace Healthcare
Division
Low Medium High Unknown
Top 5 Threats (Bar - Horizontal)
Power failure 20
Telecommunications f... 20
Malicious code 15
Lawsuits/ litigation 15
Biological agent att... 11
Threat
Entity Count
Monthly Security Risk Trend
COUNT
2007 Oct 2007 Jun 2008 Jan 2008 Feb
Month
Survey Status Summary
Security and Residual risk Trend
Monthly Simple Risk Trend

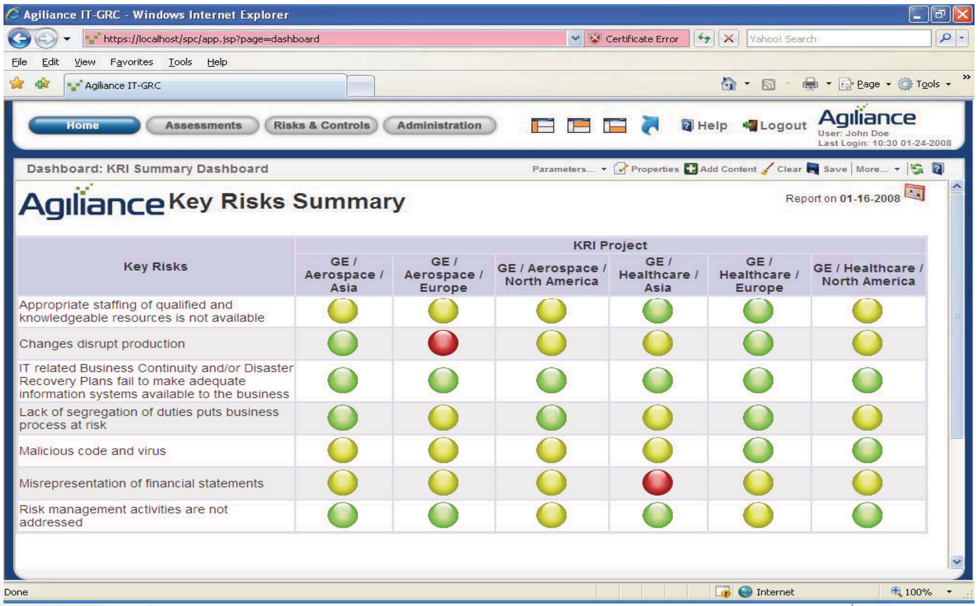
Top 5 High Risk Entities

| Entity | Primary Owner | Criticality | Risk Score |
|---|---|---|---|
| Firewall CHKP34-4 | John Doe | High | 584 |
| Server-PK-APP543 | John Doe | High | 385 |
| Server-PK-UX34 | John Doe | High | 378 |
| Oracle App 4RT | Jane Doe | Low | 199 |
| Firewall PIX342 | John Doe | High | 178 |

Top 5 Vulnerabilities

| Vulnerability | Entity Count | Total Risk Score |
|---|---|---|
| Applications do not confirm to security criteria | 15 | 2252 |
| Lack of third party authorization process | 15 | 2252 |
| Lack of disaster recovery process | 11 | 6687 |
| Lack of physical security policies | 11 | 4458 |
| No defined crisis event mangement | 11 | 6441 |

# Key Risk Indicators Dashboard

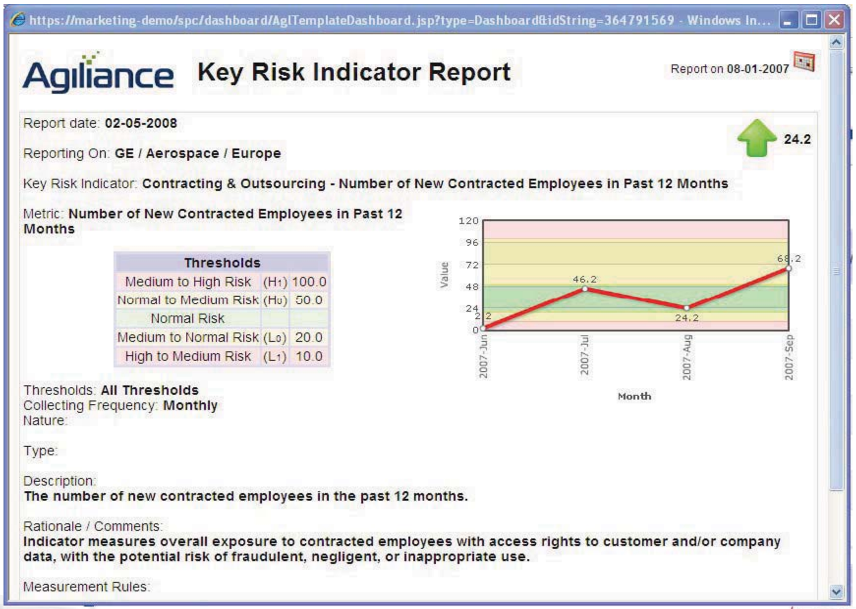

Agiliance IT-GRC - Windows Internet Explorer
https://localhost/spc/app.jsp?page=dashboard
Certificate Error
Yahoo! Search
File Edit View Favorites Tools Help
Agiliance IT-GRC
Page Tools
Home
Assessments
Risks & Controls
Administration
Help
Logout
Agiliance
User: John Doe
Last Login: 10:30 01-24-2008
Dashboard: KRI Summary Dashboard
Parameters... Properties Add Content Clear Save More...
Done
Internet
100%

Agiliance Key Risks Summary

Report on **01-16-2008**

| Key Risks | KRI Project | | | | | |
|---|---|---|---|---|---|---|
| | GE / Aerospace / Asia | GE / Aerospace / Europe | GE / Aerospace / North America | GE / Healthcare / Asia | GE / Healthcare / Europe | GE / Healthcare / North America |
| Appropriate staffing of qualified and knowledgeable resources is not available | 🟡 | 🟡 | 🟡 | 🟢 | 🟢 | 🟡 |
| Changes disrupt production | 🟢 | 🔴 | 🟡 | 🟡 | 🟢 | 🟡 |
| IT related Business Continuity and/or Disaster Recovery Plans fail to make adequate information systems available to the business | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Lack of segregation of duties puts business process at risk | 🟢 | 🟡 | 🟢 | 🟡 | 🟢 | 🟡 |
| Malicious code and virus | 🟡 | 🟡 | 🟡 | 🟡 | 🟢 | 🟢 |
| Misrepresentation of financial statements | 🟡 | 🟡 | 🟡 | 🔴 | 🟡 | 🟡 |
| Risk management activities are not addressed | 🟢 | 🟢 | 🟡 | 🟢 | 🟡 | 🟢 |

# Key Risk Indicator Trends



https://marketing-demo/spc/dashboard/AglTemplateDashboard.jsp?type=Dashboard&idString=364791569 - Windows In...

## Agiliance Key Risk Indicator Report

Report on 08-01-2007

Report date: **02-05-2008**

**24.2**

Reporting On: **GE / Aerospace / Europe**

Key Risk Indicator: **Contracting & Outsourcing - Number of New Contracted Employees in Past 12 Months**

Metric: **Number of New Contracted Employees in Past 12 Months**

| Thresholds | | |
|---|---|---|
| Medium to High Risk | ($H_1$) | 100.0 |
| Normal to Medium Risk | ($H_0$) | 50.0 |
| Normal Risk | | |
| Medium to Normal Risk | ($L_0$) | 20.0 |
| High to Medium Risk | ($L_1$) | 10.0 |

Thresholds: **All Thresholds**
Collecting Frequency: **Monthly**
Nature:

Type:

Description:
**The number of new contracted employees in the past 12 months.**

Rationale / Comments:
**Indicator measures overall exposure to contracted employees with access rights to customer and/or company data, with the potential risk of fraudulent, negligent, or inappropriate use.**

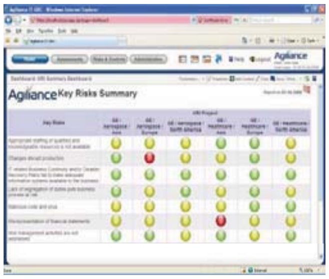
Measurement Rules:

# Risk Mitigation

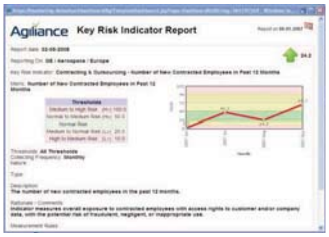
- Integrated actions: secure, remediate, transfer & accept
- Workflow driven mitigation
- Document mitigation plan, compensating controls, exceptions …
- Automatically rank risks by critically to prioritize mitigation, configurable prioritization model
- Integrate to enterprise ticketing systems

# Risk Management Technology Summary

- Single integrated risk management platform, across IT and non-IT, internal and external
- Collaboration platform to enable participation of domain experts in identifying and modeling risks
- Configurable calculations for lost expectations, risk score, risk criticality
- Closed loop risk management with mitigation



Agiliance Key Risks Summary



Agiliance Key Risk Indicator Report

Reporting On: [illegible] / Aerospace / Europe

Key Risk Indicator: Contracting & Outsourcing - Number of New Contracted Employees in Past 12 Months

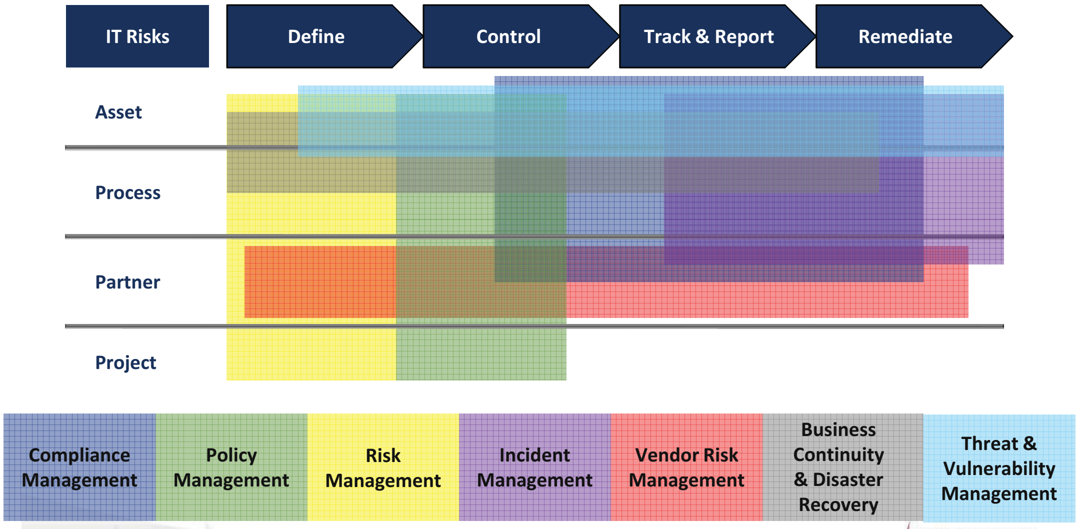
Thresholds: All Thresholds

Collecting Frequency: Monthly

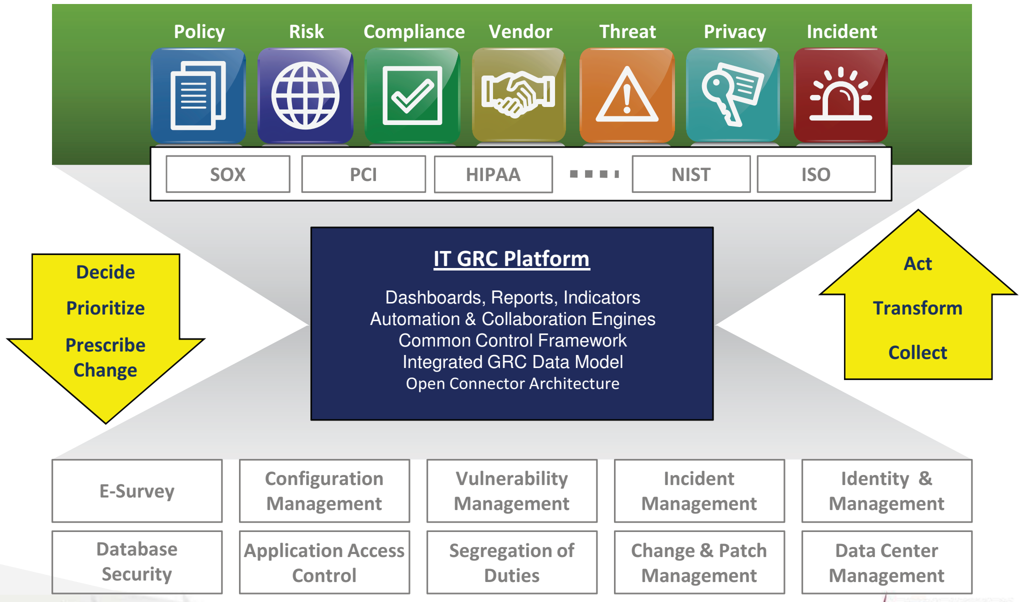
Description: The number of new contracted employees in the past 12 months.

Rationale / Comments: Indicator measures overall exposure to contracted employees with access rights to customer and/or company data, with the potential risk of fraudulent, negligent, or inappropriate use.

# The Need For An IT-GRC Platform



# IT GRC Solution



Policy | Risk | Compliance | Vendor | Threat | Privacy | Incident

SOX | PCI | HIPAA | ▪▪▪▪ | NIST | ISO

Decide

Prioritize

Prescribe Change

**IT GRC Platform**

Dashboards, Reports, Indicators
Automation & Collaboration Engines
Common Control Framework
Integrated GRC Data Model
Open Connector Architecture

Act

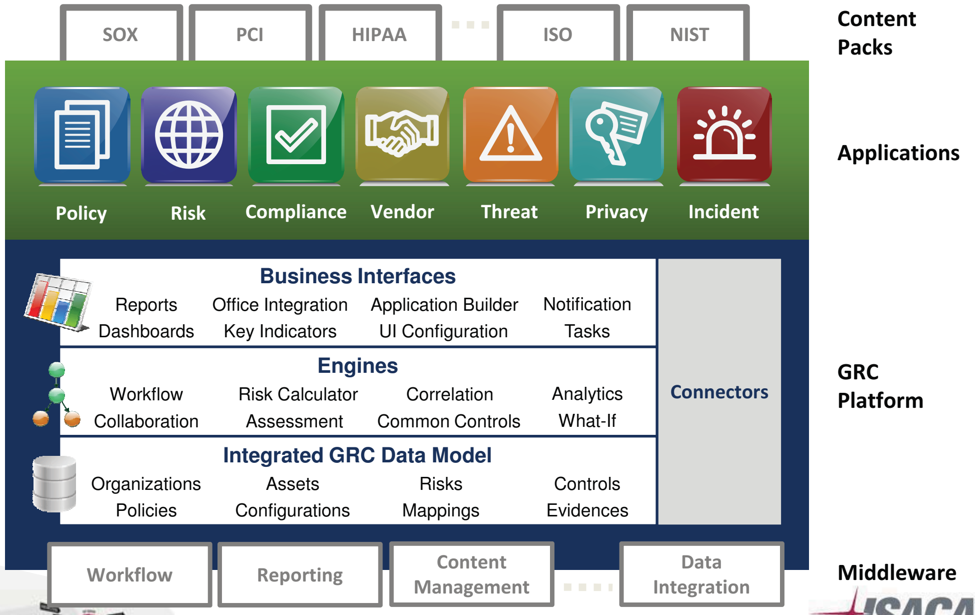
Transform

Collect

E-Survey | Configuration Management | Vulnerability Management | Incident Management | Identity & Management

Database Security | Application Access Control | Segregation of Duties | Change & Patch Management | Data Center Management

# IT GRC Platform Architecture



SOX | PCI | HIPAA | ▪▪▪ | ISO | NIST

Content Packs

Policy | Risk | Compliance | Vendor | Threat | Privacy | Incident

Applications

**Business Interfaces**

Reports | Office Integration | Application Builder | Notification
Dashboards | Key Indicators | UI Configuration | Tasks

**Engines**

Workflow | Risk Calculator | Correlation | Analytics
Collaboration | Assessment | Common Controls | What-If

**Integrated GRC Data Model**

Organizations | Assets | Risks | Controls
Policies | Configurations | Mappings | Evidences

Connectors

GRC Platform

Workflow | Reporting | Content Management | ▪▪▪▪ | Data Integration

Middleware

# Some Core GRC Applications

## Policy
Collaborative policy lifecycle mgmt.

Policy distribution & compliance testing

## Vendor Risk
Partner classification & risk assessment

Delegated administration

## Enterprise Risk
Collaborative risk definition & mapping

Real time risk monitoring

## Threat & Vulnerability
Monitor, test & Remediate

Scan, virtual scan & advanced warning

## Compliance
Manual & automated assessment

Compliance reporting & metrics

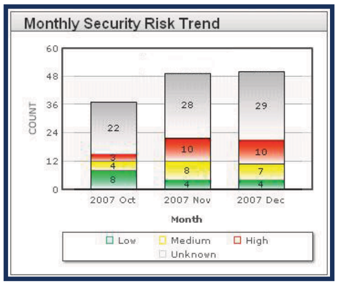
## Privacy
Compliance & impact assessments

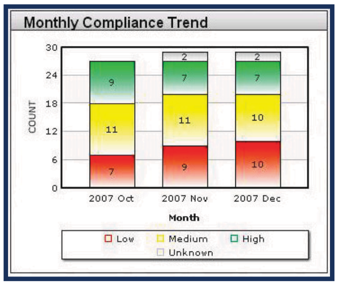
Policy awareness & incident readiness

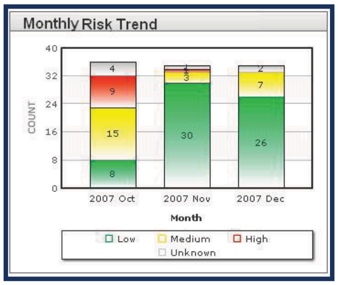
## Incident
Incident lifecycle Management

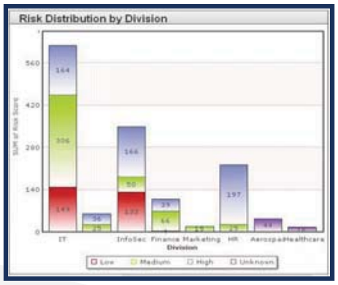
Operationalize response plan

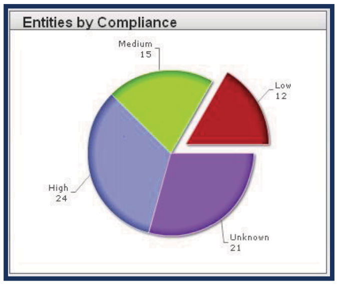
# “Single Pane of Glass” for GRC

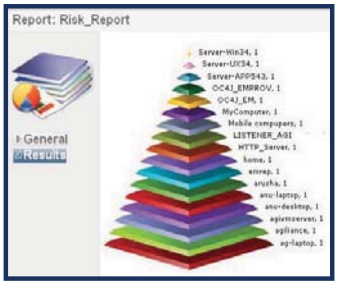




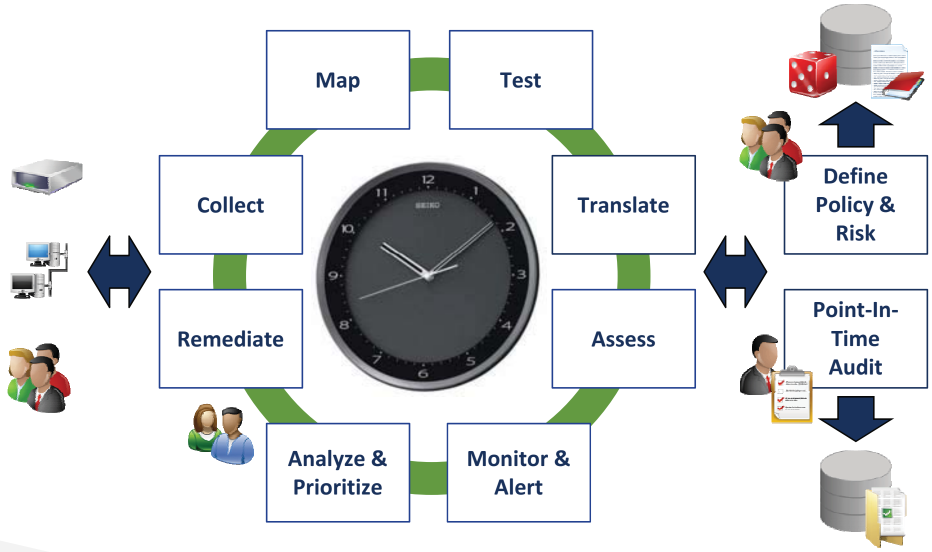








# Continuous, Closed Loop Automation



CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

# Why Continuous, Closed Loop GRC?

Because They Don't Work By Your Audit Schedule!

Hackers

Disgruntled Employees

Careless Employees

Identity Thieves

CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

# Compliance ≠ Managed Risk

- Spring 2007: PCI certified
- March 2008: 4.2 million credit card numbers lost from breach
- 1,800 fraud cases, class action lawsuit, CIO resigned

- Summer 2008: PCI certified
- November 2008: 1.5 million payroll cards and 1.1. million social security numbers lost from breach
- $9 millions in fraudulent cash withdraws

- Spring 2008: PCI certified
- Late 2009: hackers gained access to 100 million credit card transactions for weeks, impact still being assessed
- $12.6 millions charged against earnings

# Continuous Is Cheaper & More Scalable

**Periodic Audit Efforts**
**Large Scale Audit Projects**
**Massive Amount of Data**
**Expensive Consultants**
**Exposure Between Audits**

**Continuous Risk & Compliance**
**Exception Based Alerts**
**Point-In-Time Compliance Snapshot**
**Automated Processes**
**Continuous Risk Management**

## How do you justify any business investment, including anything for IT, security and privacy?

Improve profitability,
and/or
reduce operational risk

## To Learn More: www.agiliance.com