NetIQ User Conferentie 2010

How to comply to Regulations

Shailes Nanda – Sales Engineer Benelux

shailes.nanda@attachmate.com

Definition Regulation

- Regulation:
  - Is the controlling mechanism that one applies to humans and/or communities by applying rules and/or restrictions

Why regulations?

- Protection of confidential information
  - Trade secrets
  - Intellectual property
  - Etc.
- Protection of public welfare
- Accountability of CEO/CFO
- Give costs to one benefits to others
- Proof integrity of financial reports

NO WONDER THIS COMPANY IS IN TROUBLE LOOK AT THESE OUTRAGEOUS SALARIES ESPECIALLY THIS FELLOWS.
... THAT'S YOURS SIR !!
STAFF SALARIES
MEANEY

How to comply to regulations?

Compliant for?

- WBP (wet bescherming persoonsgegevens
- Sarbanes-Oxley
- PCI-DSS
- NEN7510
- ISO27001:2005
- …

What is the challenge?

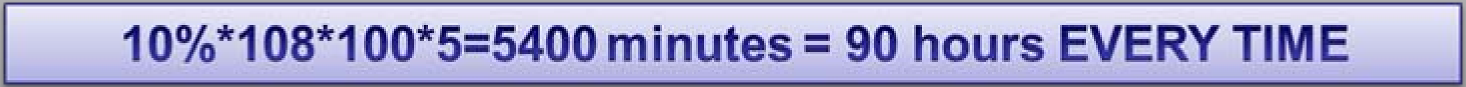
- Higher management responsible for compliancy
  - Reporting has been outsourced to IT staff
- IT staff not equipped with the right tools to deliver reporting
- Compliancy is not core business to company
- Outsourcing is not the solution
- Reporting is done by everyone on it’s own way and format, excel?
- If not comply to regulations then sanctions can follow

Example NEN7510

- Regulation for the Dutch Healthcare System
- Active for the EPD (Elektronisch patiëntendossier)
- NetIQ partners with Heroth, Dynasec
  - iComply

Example NEN7510

- Calculation
  - NEN7510 contains 108 technical controls to be checked
  - Let’s take 100 applications, operating systems and network components available
  - Let’s assume that 10% of technical controls applies to infrastructure components
  - Each check takes 5 minutes to control



10%*108*100*5=5400 minutes = 90 hours EVERY TIME

How to do it then?

- Use tooling for IT compliancy
  - Safes time
  - Regular and consequent reports
  - Same format
  - IT staff only responsible for maintenance
  - Responsibility still at Management level

How NetIQ supports compliancy to regulations

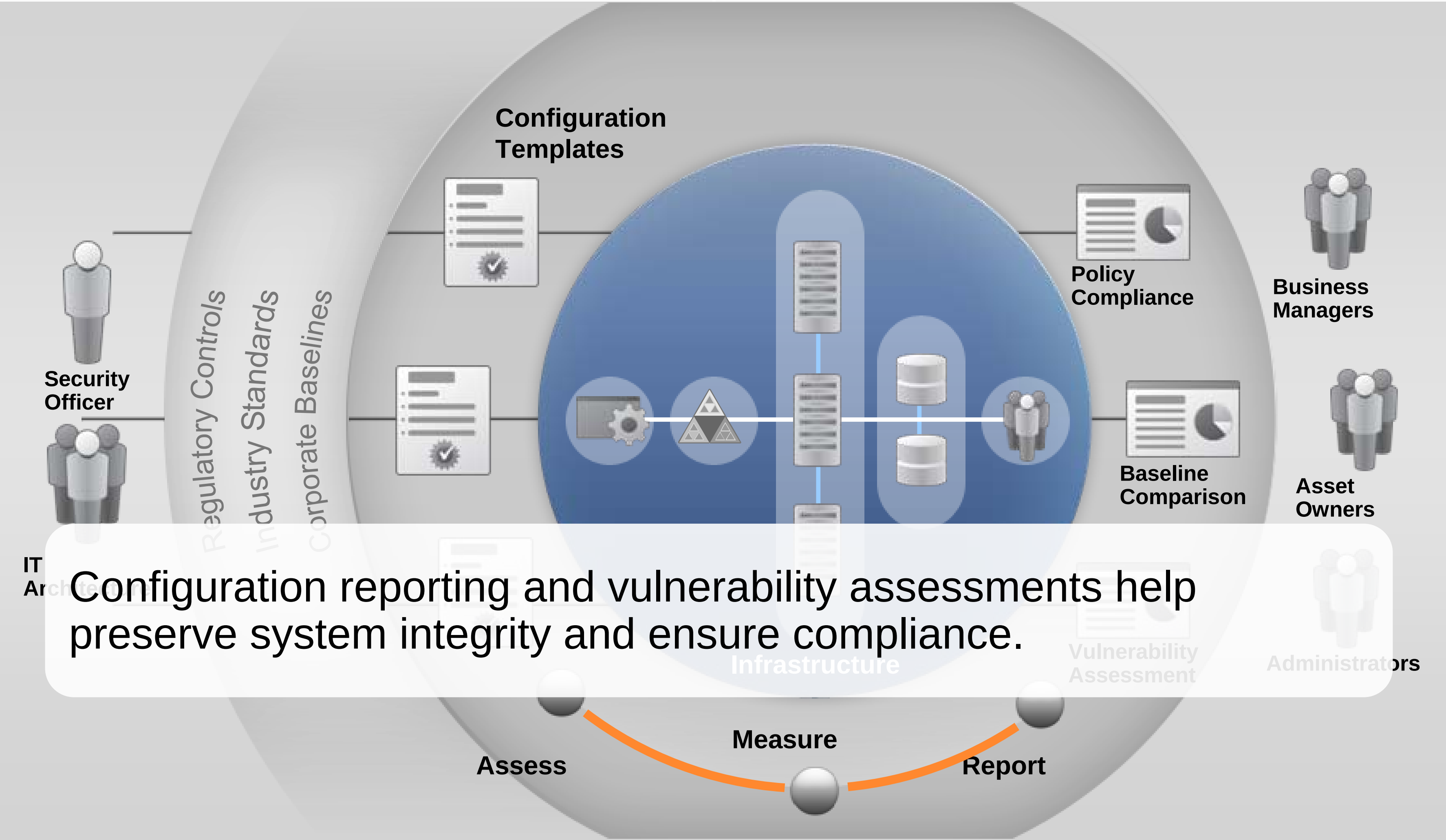
- NetIQ Secure Configuration Manager
  - proactively helps companies assess system configurations against best practices to comply with corporate and regulatory policies and to manage information security risk. This allows them to correct misconfigurations and exposures before they result in security breaches, failed audits or costly downtime.

NetIQ Secure Configuration Manager

Baselining & Delta Reporting

User Entitlement Reporting

- System Integrity Analysis



Configuration reporting and vulnerability assessments help preserve system integrity and ensure compliance.

NetIQ Secure Configuration Manager

● **User Entitlement Reporting**

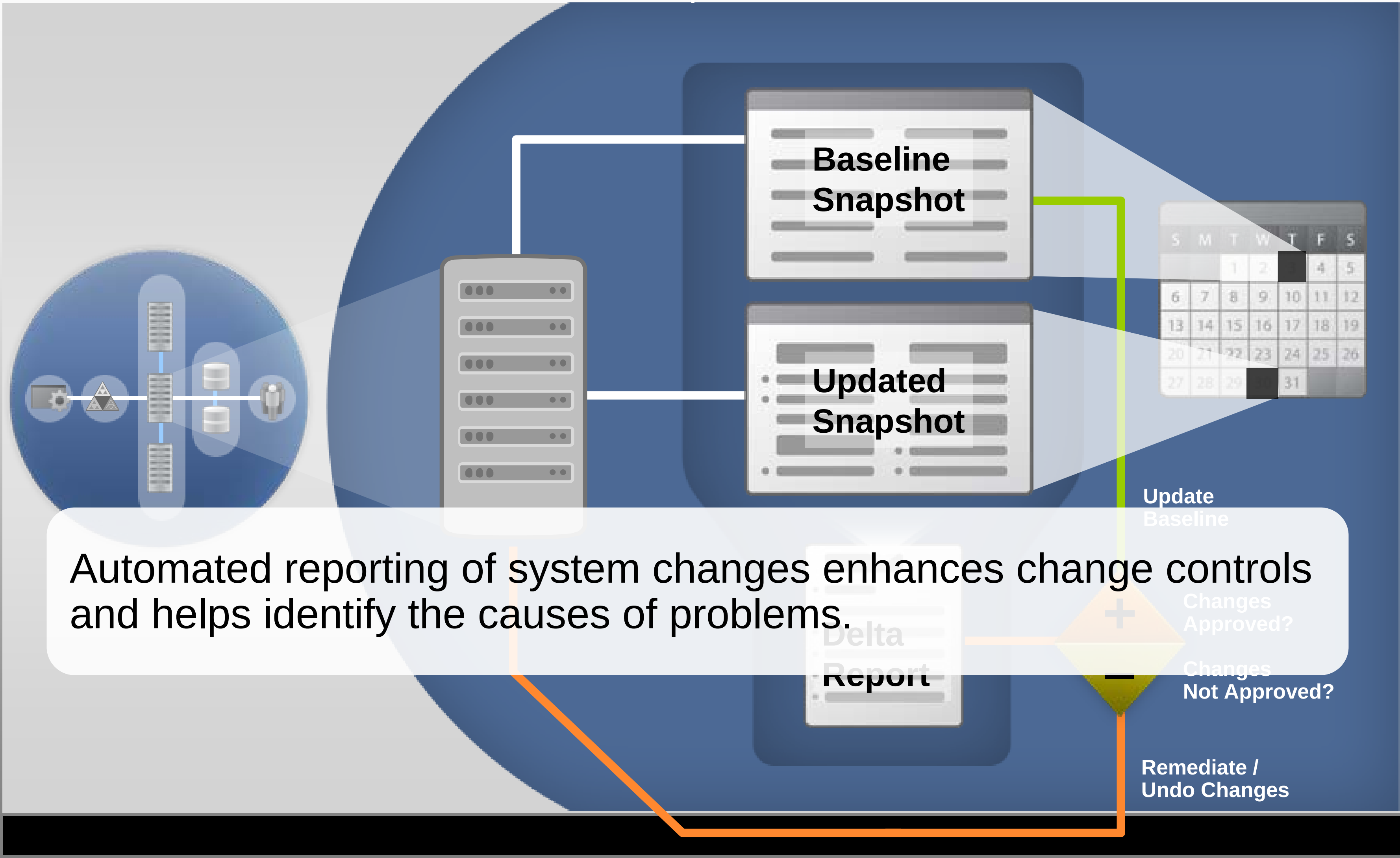
System Integrity Analysis

User Effective Permissions
Object Level Permissions
Access this computer from the network
Add workstations to domain
Adjust memory quotas for a process
Allow logon through terminal services
Back up files and directories
Bypass traverse checking
Change the system time
Create a token object
Create permanent shared objects
Debug programs
Force shutdown from a remote system
Generate security audits
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Log on as a service
Manage auditing and security log
Perform volume maintenance tasks
Profile single process
Profile system performance
Replace a process level token
Restore files and directories
Shut down the system
READ_CONTROL
ACCESS_SYSTEM_SECURITY
GENERIC_READ
Read & Execute
WRITE_OWNER
SYNCHRONIZE
DS_READ_PROP
DS_WRITE_PROP
DS_LIST_OBJECT
DS_CONTROL_ACCESS

Automated entitlement reporting streamlines reviews, helping to maintain up-to-date access privileges and to demonstrate compliance.

NetIQ Secure Configuration Manager

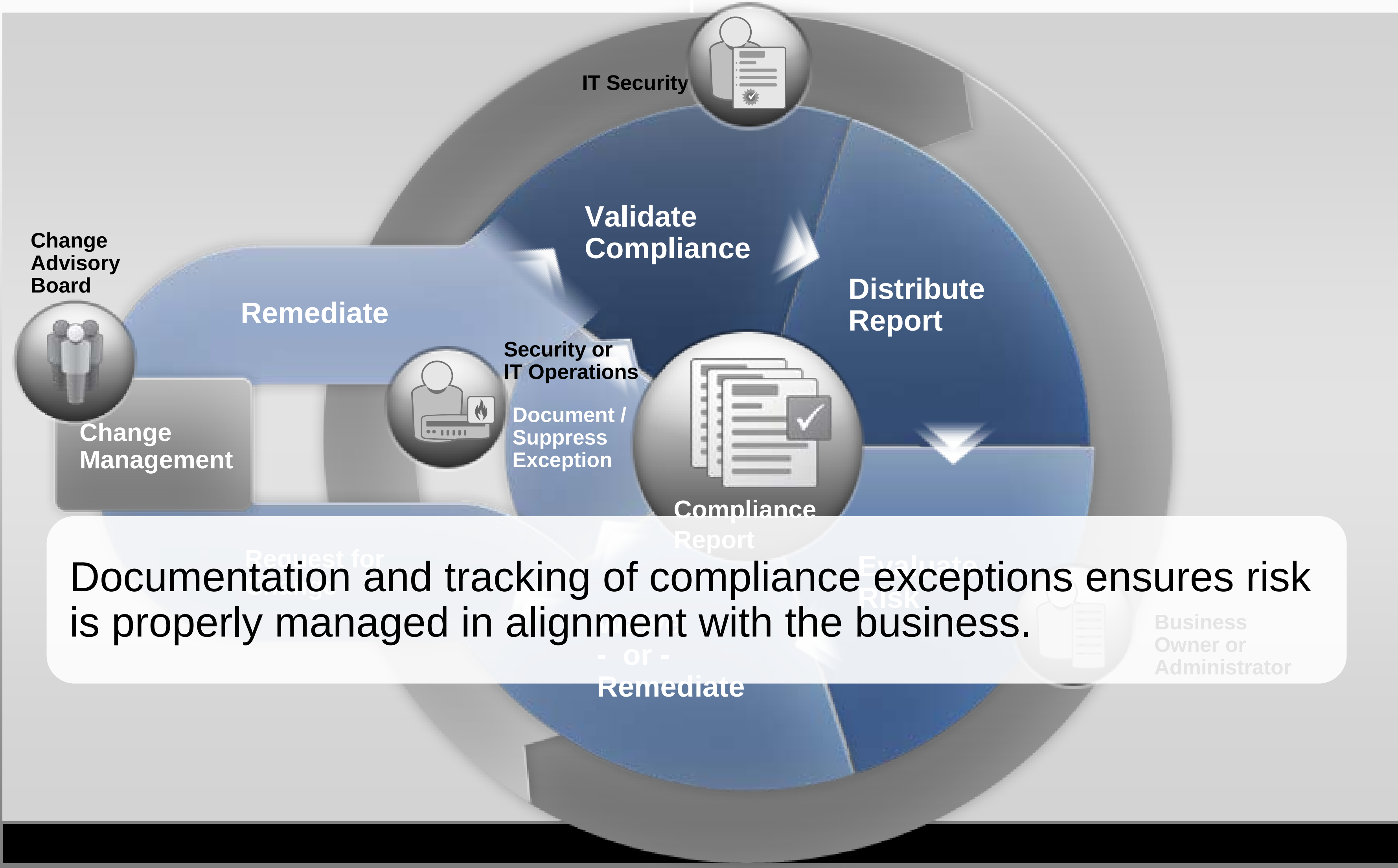
- ● **Baselining & Delta Reporting**
- User Entitlement Reporting
- System Integrity Analysis



Automated reporting of system changes enhances change controls and helps identify the causes of problems.

NetIQ Secure Configuration Manager

- **Business Exception Management**
- Baselining & Delta Reporting
- User Entitlement Reporting
- System Integrity Analysis



Documentation and tracking of compliance exceptions ensures risk is properly managed in alignment with the business.

Additionally

- **VigilEnt Policy Center (VPC)** is the most comprehensive solution for developing, tracking, and reporting on corporate governance documents. This solution includes policies, standards, and procedures from any department including Compliance, Human Resources, Information Technology, Legal, and Physical Security.
- A successful VPC implementation provides increased levels of employee awareness and results in raising corporate compliance to applicable laws, regulations, and guidance that affect organizations in any industry.

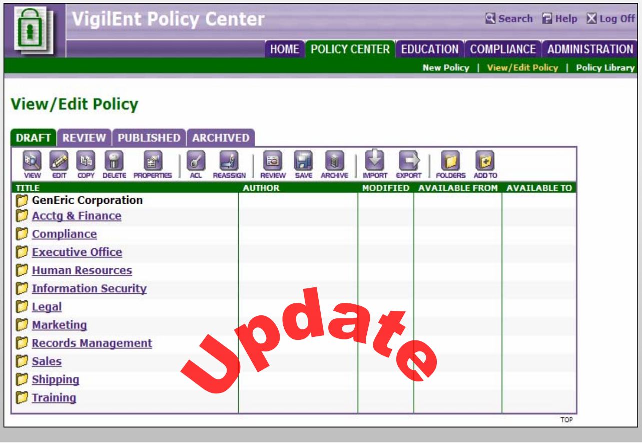
> **“Having a common single point for policy creation, compliance, assessment, enforcement and awareness training will significantly improve security management by providing a security foundation which can comprehensively manage the entire enterprise’s IT risks.”**
>
> – Roberta Witty, Gartner.

Policy Life Cycle using VPC

Publish
To targeted users and groups for specified time period

Review - Comment
By specific users assigned to policy

Create - Import - Modify
Templates, Libraries, Existing Content



VigilEnt Policy Center

Search | Help | Log Off

HOME | POLICY CENTER | EDUCATION | COMPLIANCE | ADMINISTRATION

New Policy | View/Edit Policy | Policy Library

View/Edit Policy

DRAFT | REVIEW | PUBLISHED | ARCHIVED

VIEW EDIT COPY DELETE PROPERTIES ACL REASSIGN REVIEW SAVE ARCHIVE IMPORT EXPORT FOLDERS ADD TO

TITLE	AUTHOR	MODIFIED	AVAILABLE FROM	AVAILABLE TO
GenEric Corporation				
Acctg & Finance				
Compliance				
Executive Office				
Human Resources				
Information Security				
Legal				
Marketing				
Records Management				
Sales				
Shipping				
Training				

TOP

Assess - Educate - Test
Same process as Policies – Links to internal/external content sites

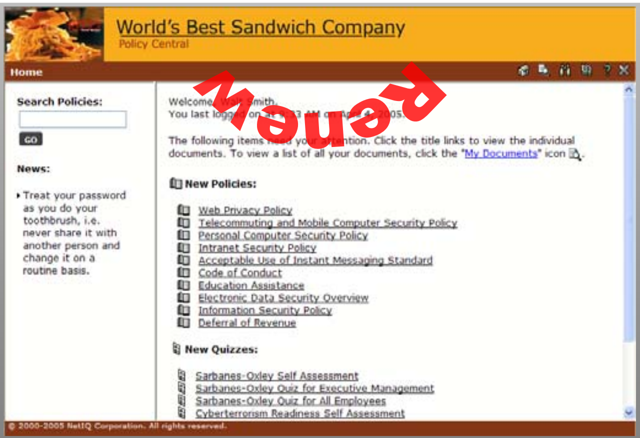
Compliance Reports
Policies Read – Policies Understood
Test Scores – Assess Effectiveness

Archive
Retire expired policies

Incident Reporting
Report security incidents and policy violations

Search
Find specific policy guidance

Review
All acknowledged policies are accessible for later review



World's Best Sandwich Company
Policy Central

Home

Search Policies:

GO

News:

- Treat your password as you do your toothbrush, i.e. never share it with another person and change it on a routine basis.

Welcome, Walt Smith.
You last logged on at 9:33 AM on April 4, 2005.

The following items need your attention. Click the title links to view the individual documents. To view a list of all your documents, click the "My Documents" icon.

New Policies:

- Web Privacy Policy
- Telecommuting and Mobile Computer Security Policy
- Personal Computer Security Policy
- Intranet Security Policy
- Acceptable Use of Instant Messaging Standard
- Code of Conduct
- Education Assistance
- Electronic Data Security Overview
- Information Security Policy
- Deferral of Revenue

New Quizzes:

- Sarbanes-Oxley Self Assessment
- Sarbanes-Oxley Quiz for Executive Management
- Sarbanes-Oxley Quiz for All Employees
- Cyberterrorism Readiness Self Assessment

© 2000-2005 NetIQ Corporation. All rights reserved.

Read
Track users' acknowledgements

Learn
Follow links to additional content

Quiz - Assess
Validate level of understanding

More info

- http://www.netiq.com/solutions/regulatory/default.asp
- www.icomply.nl
- March 4, 2010 extensive seminar on implementing NEN7510

Questions?