



Security Intelligence, Audit and Compliance



Agenda

Concerns

Actions

Is the Mainframe Vulnerable?

- **Hacking/Theft (just to mention a few)**
 - 2007 Department store mainframe security hack
 - 2008 Health care mainframe security hack
 - 2009 Mainframe computer physically lost from college campus
 - 2010 Airport mainframe computer physically removed
- **Insider Threat?**
 - Long considered the most serious threat
 - Insiders have access
 - Insiders have knowledge
 - Insiders have economic motivation
 - Insider collusion is a “force multiplier”

Mainframe security

What's the risk?

- Disclosure of sensitive data
- Service interruption
- Corruption of operational data
- Fraud and ID Theft
- Theft of services



What's at stake?

- Customer trust
- Reputation and Brand
- Privacy
- Integrity of Information
- Legal and Regulatory Action
- Competitive Advantage



Breach cost?

- \$ Research and recovery
- \$ Notify customers
- \$ Lost customer business
- \$ Problem remediation
- \$ Claims from trusted vendors and business partners



\$\$ *Damage to brand image*

Mainframe Vulnerabilities

Mainframe Security Report 1:

Security Officer Representation: We restrictively secure our mainframe based-on the concept of “least privilege”. Nobody gets access to anything unless it is approved.

Report Finding: The mainframe security and the protection-by-default mechanisms of the mainframe security software have been promiscuously configured to the point of providing access by default instead of protection. The security of system and application resources cannot be assured.

Reality of security contradicts perception

Mainframe Vulnerabilities

Mainframe Security Report 2:

Security Officer Representation: It is our practice to empower business units to make decisions regarding the security of their applications and services.

Report Finding: As authorized by a business unit, CICS regions were running with full security bypass privilege, leaving CICS technical resources and the data of all applications

No Security Implementation Standards
a.k.a. "Adult Supervision"

6 *programmers. Result: No separation of function between applications: no assurance of*

Mainframe Vulnerabilities

Mainframe Security Report 3:

Mainframe security is being managed and administered using legacy practices and standards that pre-date the increased technical sophistication of the mainframe and its increased leverage for Web-based services. As such, security is woefully inadequate to assure security, privacy, and compliance in the current environment.

Mainframe is Dead Legacy...

***Low investment, weak skills, weak governance,
maybe coupled with a false sense that the
mainframe is inherently secure***

Story of a Security Consultant

Unix System Services Hack

Due to the regular mis-configuration of security in the z Unix System Services environment and inappropriate use of security bypass privileges, one security practitioner has repeatedly demonstrated the ability to compromise mainframe security and grab any data desired.

His record hack time: Less than 20 minutes!!!

One of the successes was by invitation against a security software company.

Advice From a Career Auditor

**“You don’t know what you don’t know,
and what you don’t know will hurt...!”**

**Senior Manager ,
*U.S. Government Accountability Office***

SHARE 2012 Atlanta

SEC Project Keynote Presentation

Information Security Optimization Principles

Vision

- Strategy, Policy, Standards
- Governance, Organization
- Business Alignment

Visibility

- Information asset identification
- Risk assessment
- Prioritized focus and investment for early and high impact
- Event monitoring and investigation

Accountability

- Enterprise-wide ownership, responsibility, and participation
- Distributed responsibility for funding and executing solutions and processes

Sustainability

- Defined, continuous operational solutions and processes
- Automated balanced, coordinated, and cost-effective solutions to protect and enable the enterprise both ESM and support solutions
- Automation – audit reporting, monitoring and compliance

Advice From a Career Information Security Consultant

**“If nobody is minding the store,
someone will surely steal the goods”**

Quote from *Security Consultant from TATA America International Corporation*

The one thing you can do to immediately strengthen security without risking unintended denials of access is to initiate aggressive monitoring and investigation.

What you see will surprise you! The visibility will convince you! The implications will motivate you.

Obtain Security Intelligence: You need to determine what you don't know before you can do anything meaningful!

A Final Keystone Issue



CIA

Relative to the Information Security trilogy of Confidentiality, Integrity, and Availability, legacy mainframe security implementations consistently exhibit a strong bias to Availability, at the expense of Confidentiality and Integrity.

A Final Keystone Issue: Balance Required

The letters 'C', 'I', and 'A' are rendered in a large, bold, teal font with a slight 3D effect and a drop shadow. They are spaced out horizontally across the center of the slide.

Balance is needed across C, I, and A to assure effective security. Lack of balance results in exposures and vulnerabilities

Your Conflict: Regulation versus Reality

Regulation



- **Change management**
 - Clearly defined process with approval and reporting
 - Ability to identify changes
- **Security management**
 - Separation of duties
 - Identification of exposures and mis-configurations
 - Clear audit trail and accountability
- **Data security**
 - Data confidentiality and integrity
 - Prevent improper access to financial, medical or personal data
 - Monitor access to data by technician, administrator, outsiders

Reality



- **Separation of duty impractical tasks with small teams**
- **Many highly authorized IDs necessary for final go-to technician**
- **Mainframe installations often rely on “system special” and “uid(0)”**
- **Red-tape bypassed for high-impact problem resolution**
- **Manual monitoring impractical due to volume of data**
- **Human mistakes cause service outages**
- **Cleanup projects are long running and expensive**

Concerns

Actions



erge

- **As you move into the action phase**

- You need to take the lead to set the foundations
- Prepare and obtain top level management support for a foundational Security Implementation & Administration Policies document (when was the last time these were reviewed)
- Actions must be based upon what you see and what needs to be controlled as defined by your policies that support the business compliance and risk
- What do you look for and how do you move towards the target state of control and compliance?
- What do you have in the way of software that can help or what do you need?
- **Automate** the review and enforcement of controls both existing and those established during this ongoing process

Common IT General Control Deficiencies

Excessive Access to Systems / Databases

- Developer / programmer access to production environment
- Developer / programmer access to production data
- DBA access
- System Administrator access

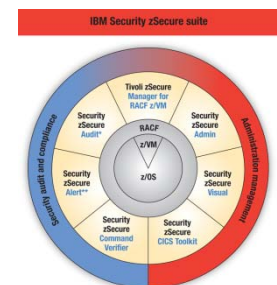
Lack of Access Controls

- User provisioning and administration
 - Changes in responsibilities
 - Changes in organization
 - Terminations
- No documented access policies and standards

General monitoring of the security infrastructure

Technology can help

- **Define the security policy in monitoring tools**
 - Operating system and security settings against baselines
 - Operating system and security changes against baselines
 - Data access against standards
 - Access by technicians should fit production profile
 - etc.
- **In case of conflict**
 - Deny the action, prevent the change from taking place, or
 - Issue a real-time message to data security officer, or
 - Generate an exception report for review by management
- **Document**
 - Baseline or security standard
 - Exceptions and transgressions

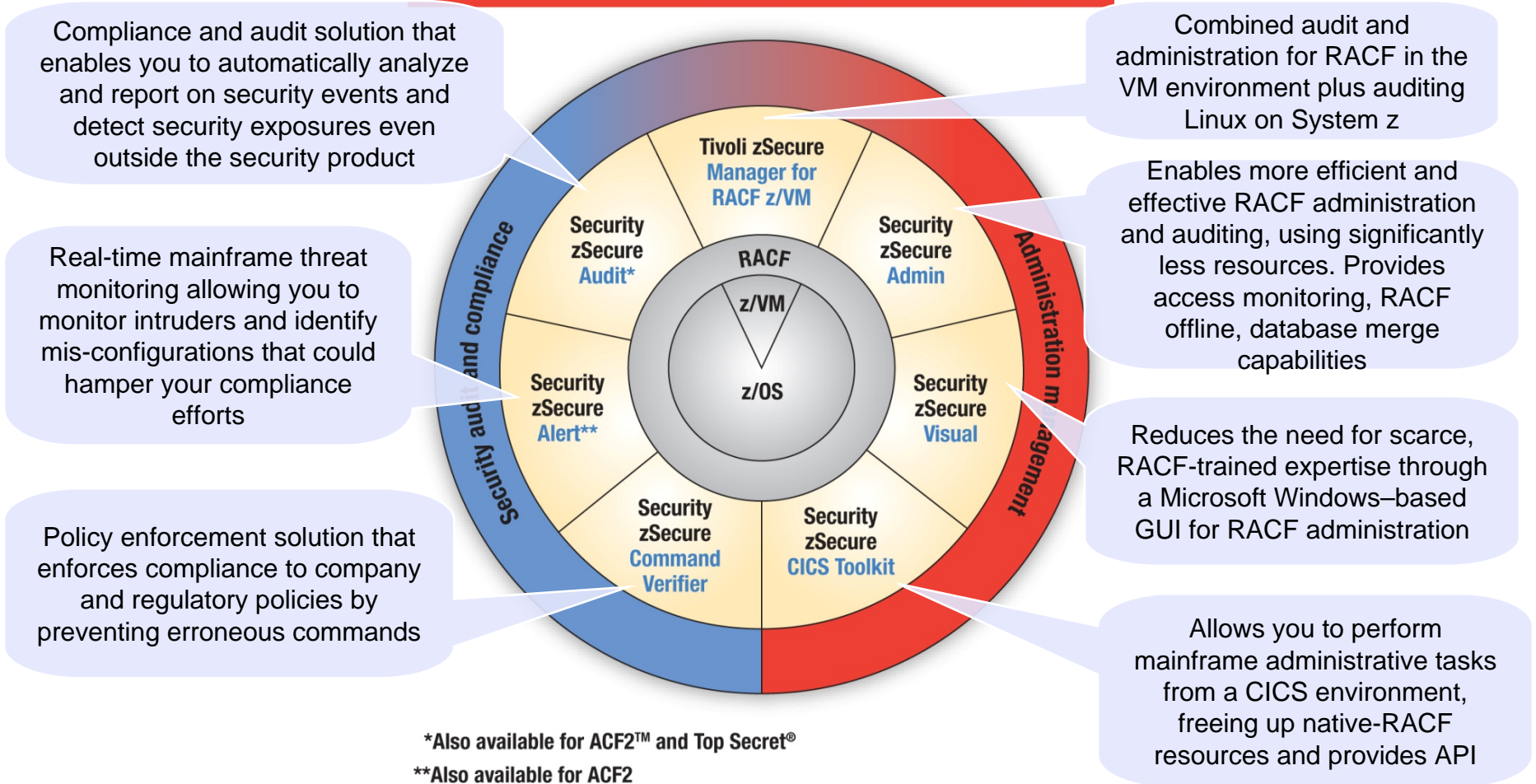


*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Introducing the IBM Security zSecure Suite

IBM Security zSecure suite



*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

AppScan Enterprise

Scalability & Control

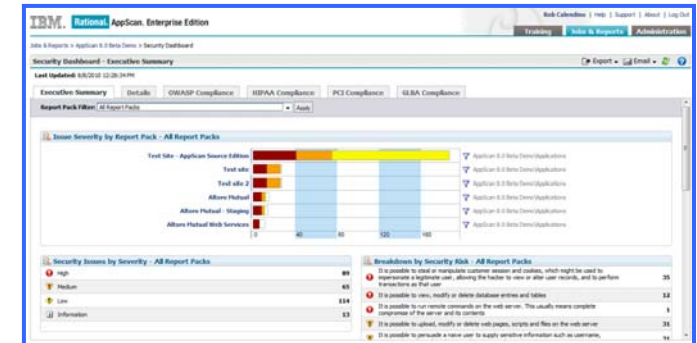
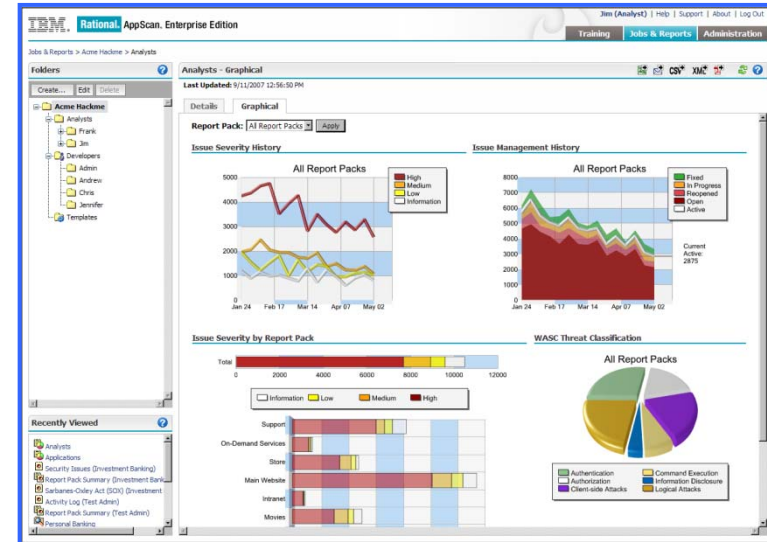
- Schedule and execute 1000s of application assessments
- Empower non-security experts to implement security best practices
- Manage user roles and access to reports
- Define scan permissions, policies and templates

Visibility & Compliance

- Dashboards of application security risk
- Non-compliance risk (40+ compliance reports)

Measure & Improve

- Number of issues by severity
- Top security issues and risks
- Trending of issues over time



Baseline

- **Why establish a baseline**
 - Each system will have specific and different characteristics
 - Know where you started
 - Know where you are headed
 - Know where you have gotten

- **Examples**
 - Freeze an image of your operating system
 - Unload a copy of your security definitions

Baselines

- **Use the baselines to create “Where we are”**
- **Examples to consider**
 - **z/OS Integrity**
 - **z/OS itself**
 - **System Critical Datasets**
 - **Authorized Libraries**
 - **Program Properties Table (PPT)**
 - **Command Authority (System, Operator)**
 - **User Supervisor Calls (SVCs)**
 - **ESM**
 - **ESM System Options**
 - **Critical User Attribute (CUA)**
 - **Public Data Sets and Resources**
 - **Password (Default and Trivial)**
 - **ESM Common Problems**
- **What do these look like?**

Find mis-configuration and vulnerabilities

▪ Situation:

- z/OS and RACF protect each other
 - System datasets must be protected...
- Verifying the protection is time consuming

▪ Best Solution Available?:

- Individual reports for RACF, PARMLIB, UNIX....
 - Manual correlation and verification?
- Annual external audit

zSecure Solution

- zSecure Audit takes information from RACF, z/OS, UNIX
 - o Identifies inconsistencies and vulnerabilities
 - o Shows the privileged users that can chance z/OS, RACF
 - Or bypass security
 - o Adhoc reports
 - o Automatic reporting and monitoring in batch jobs

AUTOMATION, AUTOMATION, AUTOMATION

Reduce human error and increase security levels

System Critical Datasets

- **Many system datasets and activities are critical to overall security and effectiveness.**
- **SYS1.PARMLIB**
 - The IEASYSxx member of SYS1.PARMLIB contains controlling system parameters that specify how other members are to be used by the system as well as certain operating characteristics.
- **SMF Datasets**
 - Certain system libraries are instrumental to the operation of MVS providing controlling parameters as well as history and audit trail functions. Any violation of those datasets could severely impact system reliability and personnel accountability.
- **Master Catalog**
 - The MVS Master Catalog contains indices used to reference other catalogs and data groups. Write access to the Master Catalog should be restricted. Such access could potentially damage strategic information or, perhaps, render the system unusable.

A Few of the System Critical Datasets – Automatically Checked by IBM Security zSecure

- APF data sets
- LPA data sets
- Page data sets
- Swap data sets
- ESM data sets
- RRSF data sets
- SMF recording data sets
- System dump data set
- TSO user administration data set UADS
- SYS1.NUCLEUS and SYS1.LPALIB
- JES2 and JES3 checkpoint data sets
- JES2 and JES3 spool data sets
- JES2 and JES3 parameter data set
- JES2 and JES3 STC/TSU proclib
- MSTR proclib
- MSTR parameter library
- MSTR VIO administration
- DFHSM data set BCDS, MCDS, OCDS
- HFS data sets
- DMS database DMSFILES
- DMS authorized parameter library
- DMS default parameter library
- CA1 tape management catalog TMC
- DFSMS SCDS and ACDS (integrity)
- IODF file, if DSN could be found
- Couple data sets
- RMM control dataset
- TLMS volume master file VMF
- ABR archive control file ACF

Command Authority

- **Execution of operator and/or system commands should be controlled by ESM**
- **INSPECT:**
 - JES2 parameters for command authority on:
 - INTRDR
 - JOBCLASS
 - TSUCLASS
 - STCCCLASS
 - SDSF
 - Netview
 - Check for other products bypassing ESM for operation and/or system commands, like Omegamon etc.

Common ESM Problems

- **USER/GROUP Maintenance**
 - Finding user and grouping inconsistencies
- **PROGRAM Class Maintenance**
 - Check for obsolete conditional permission lists when program definitions have been removed
 - Check for non-existent data set/volume program combinations
 - Checking for program definitions not describing any physical module
- **DATASET Maintenance**
 - Finding and protecting unprotected data sets checks depending on the current protection setting
 - Removing unused discrete definitions - resulting from volume-level operations
 - Finding and removing redundant discrete definitions
 - Removing unused generic definitions (after deletion of 'subject' data sets)
 - Finding and resetting unnecessary ESM-indicated bits (where no discrete definition exists)
- **STARTED Class Maintenance**
 - Finding inconsistencies in started task definitions

Beyond Baseline: Automated Clean up and Control

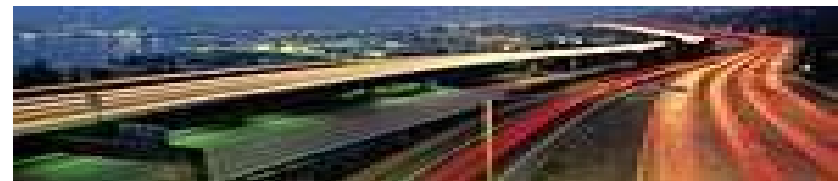
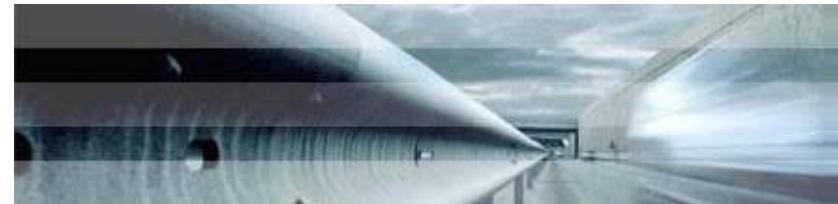
- **Now you have established the baselines – you can clean up**
- **BUT**
 - How do you maintain and prevent re-contamination?
 - After the fact – clean up
 - using SMF event reporting
 - Utilizing your baseline comparison reports
 - Before the fact – prevent the problem
 - Once your policies are defined and codified
 - Establish a means to prevent conditions outside the policies from taking place – control and verify commands, before their execution can undo

Beyond Baselines – Maintenance

- **z/OS is an evolving platform**
- **Technical expertise and awareness is paramount**
- **Honing skills must be ongoing**
- **Products employed to evaluate and control must grow**
- **Automate processes where possible –**
 - Machine speed / reaction time
 - Repetitive tasks
 - Consistent and continuous monitoring to enable timely detection and enforcement

Benefits of Automating with Technology

- Facilitate compliance with security requirements and policies
- Leverage seamless integration with an enterprise-wide view of audit and compliance efforts
- Monitor and audit incidents to help detect and prevent security exposures, as well as assess compliance
- Automate routine administrative tasks to help reduce costs and improve productivity
- Understand the security baseline and when it changes to keep security intelligence at its highest and up to date



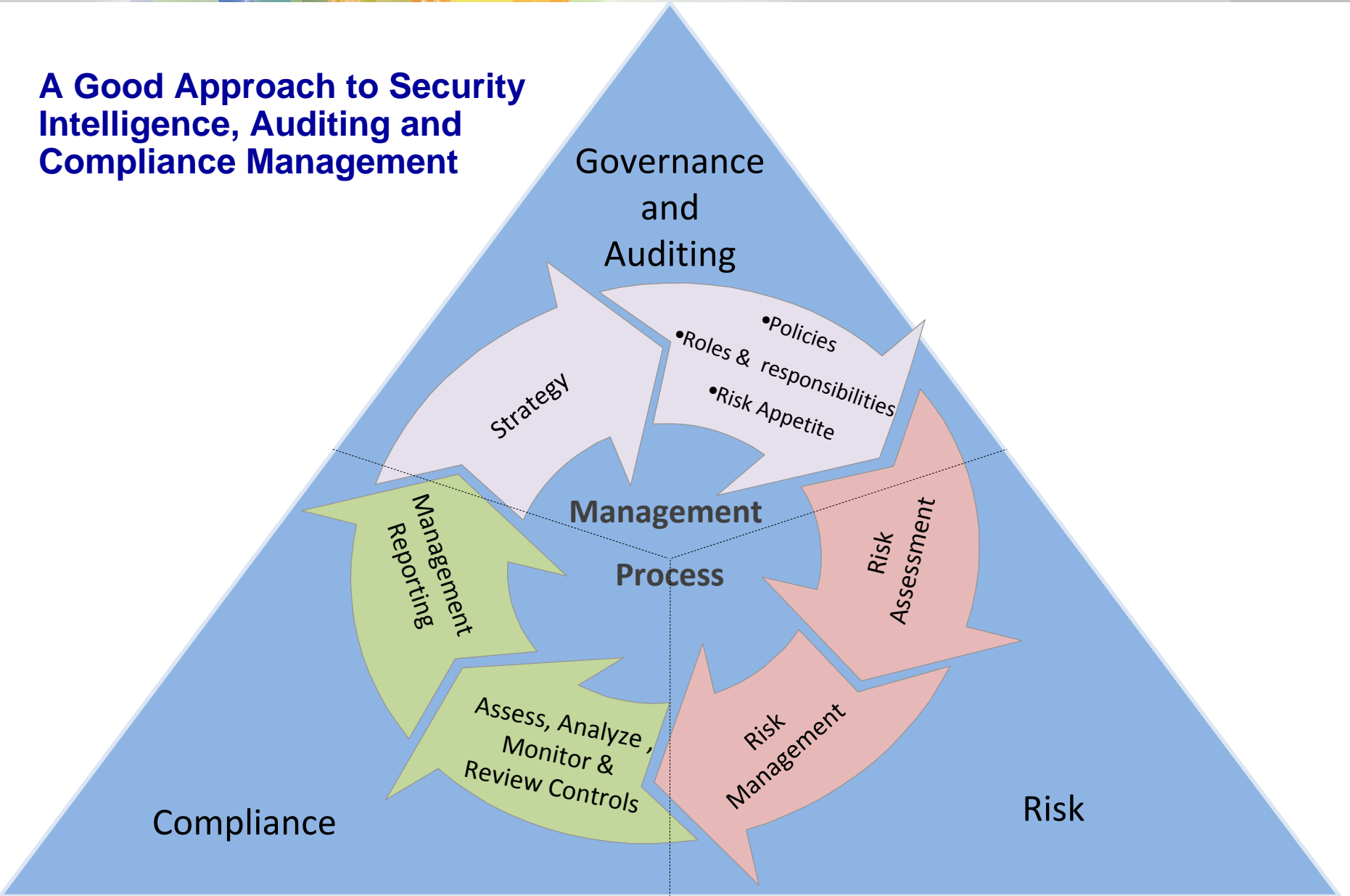
Beyond Baselines – Moving Forward

- **Now**
 - Baselines to measure progress
 - Baselines to compare changes
 - Clean up the environment
 - Prevent subsequent contamination

- **You can answer the question:**

How Secure is My Mainframe?

A Good Approach to Security Intelligence, Auditing and Compliance Management



QUESTIONS

?

