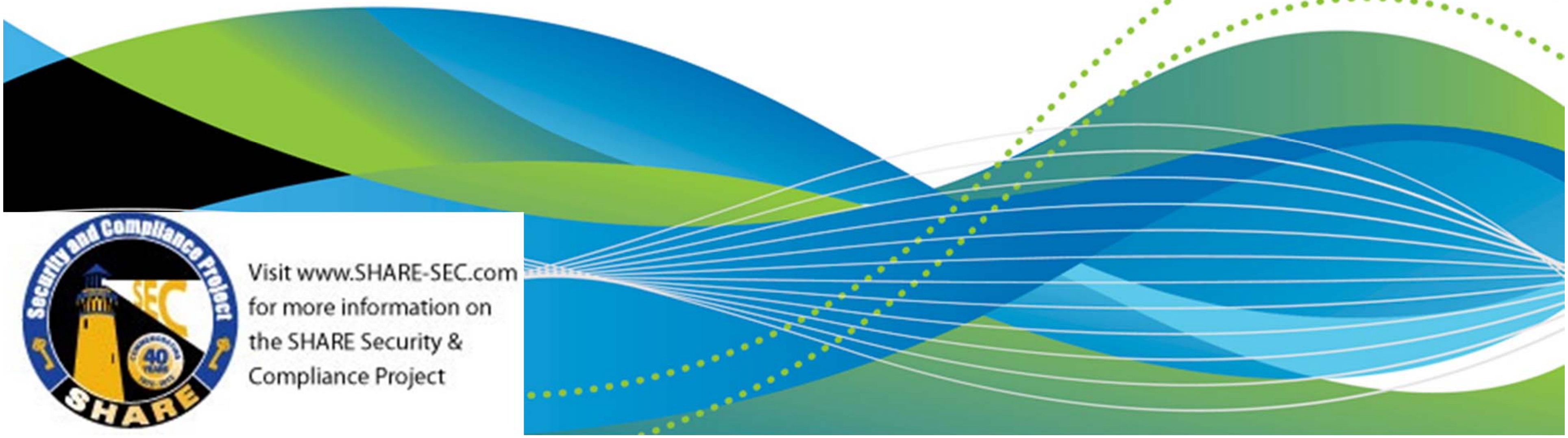
#SHAREorg

SHARE
Technology • Connections • Results

Engineering Auditability into Your Enterprise Data Center

David Hayes
U.S. Government Accountability Office

March 14, 2012
Session Number 10503



Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Topics

- Understanding the different audit processes and types of auditors
- Preparing for audits is a failed strategy
- Creating an auditable organization
- Maintaining the right distance from auditors
- Effectively communicating with auditors
- Responding to audit reports

Audits - Different Purposes and Different Auditors

- The terms audit and auditors can mean very different things and refer to very different entities
  - Auditors can be internal to an organization or from a variety of external sources
  - Activities referred as “audits” can represent a wide range of business functions
- Audits may or may not result in requirements for actions by those being audited
- Audits may or may not result in written reports to entities outside the organization being audited
- Often auditors do not talk to each other – or even know of the existence of each other

Preparing for Audits Can be Ineffective or Even Detrimental

- Good auditors are not predictable – effectively second guessing the focus of specific auditors may not be successful
- “Preparing” for audits often results in the creation of documentation for consumption by auditors. Auditors usually detect this type of documentation and may be inspired to concentrate on an area that probably hasn’t received adequate attention from management
- The process of having staff get ready for an audit can send them an unhealthy signal that certain control activities only have value to auditors

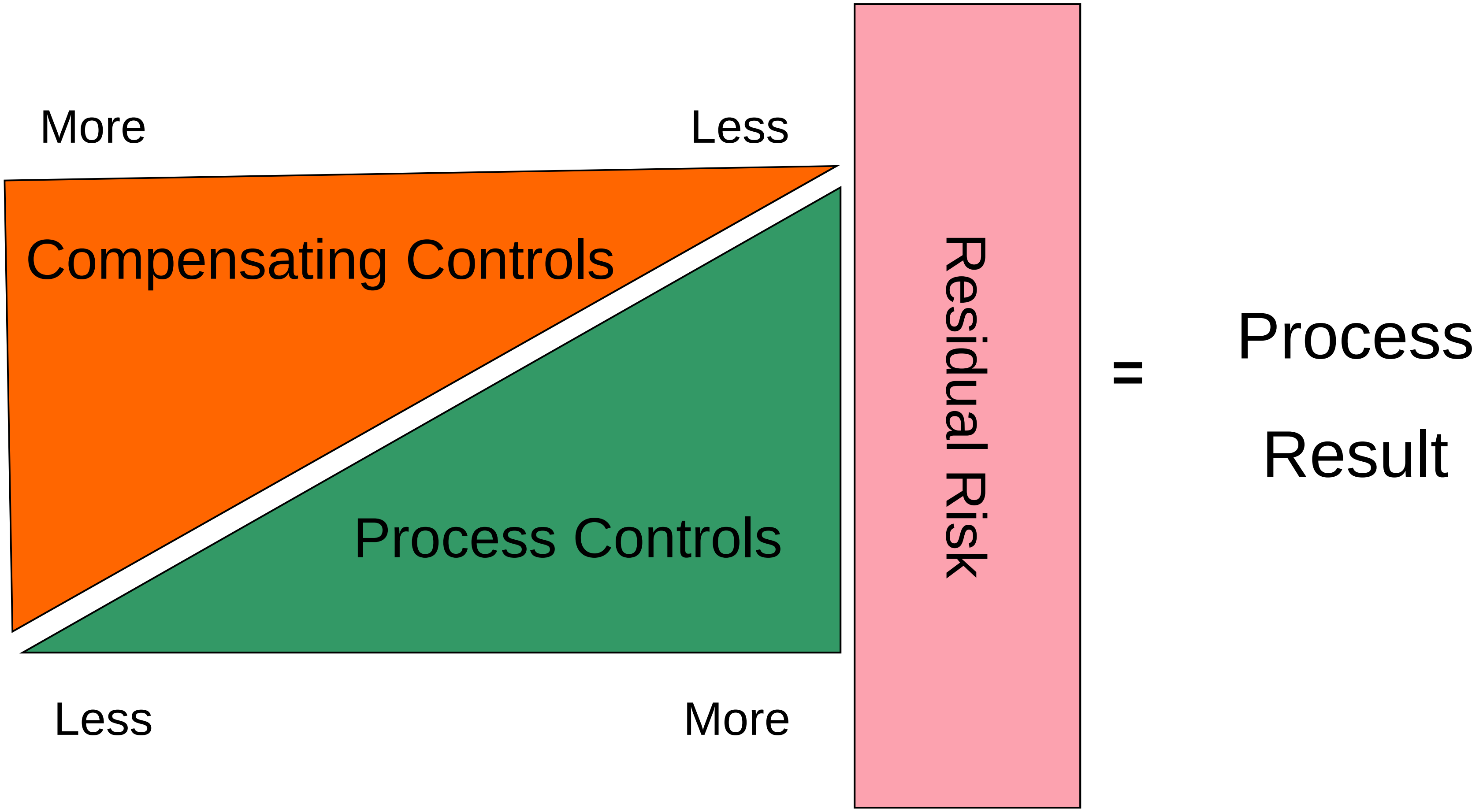
Characteristics of an Auditable Organization

- Information security and compliance processes are components of an organization’s broader internal control structure
- The organization’s (and their customers’) control objectives are well defined and clearly communicated to all levels of the organization
- The applicable security and compliance standards are integrated into the business processes in place that are designed to achieve the control objectives
- The organization has effective processes in place to maintain a nearly continuous baseline of their control environment and be able to detect and react to changes in a timely manner

Characteristics of an Auditable Organization (more)

- The organization’s operating processes self-enforce most of the security standards and compliance requirements
- While maintaining competitive service offerings to its customers, the enterprise data center doesn’t permit customers to create avoidable vulnerabilities
- Management facilitates the identification of risk at all levels by motivating everyone in the organization to be risk aware and risk adverse

Auditable Organizations Make Transparent Decisions



More

Less

Compensating Controls

Process Controls

Less

More

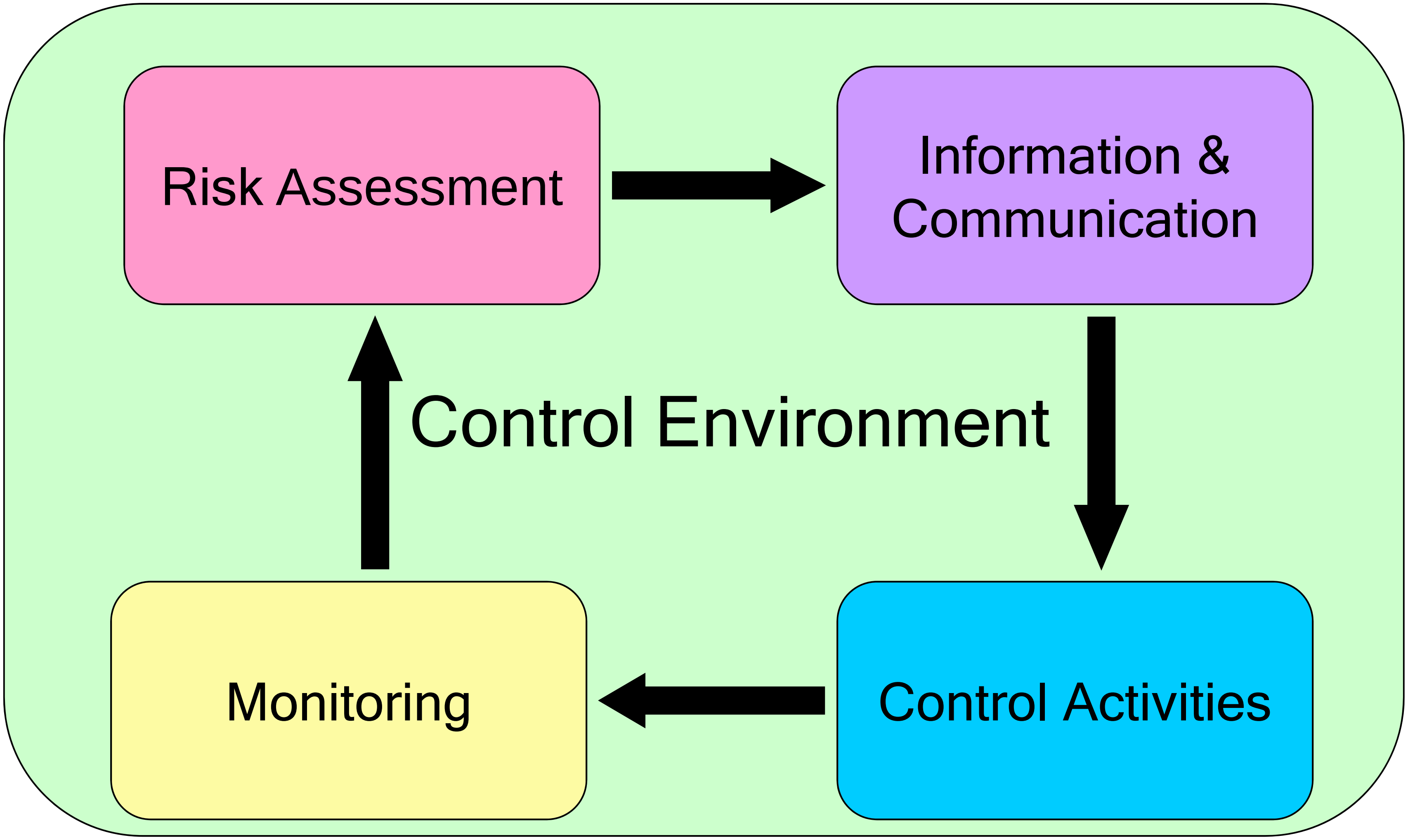
Residual Risk

=

Process

Result

Auditable Organizations Have an Internal Control Culture – Visible to Everyone


Risk Assessment

Information & Communication

Control Environment

Control Activities

Monitoring

Being Auditable – The Proper Relationship with Auditors

- Understand that auditors must maintain a healthy distance from the organization’s decision making processes
- Auditable organizations maintain and communicate protocols for interacting with internal and external auditors
- Auditors have no *authority* to impose requirements
- Auditors have no authority to *approve* any management decision

Communicating Effectively With Auditors

- Auditable organizations utilize trained and authorized staff as liaisons between operations staff and auditors
- Auditors are considered to be customers of the enterprise data center (Note: external auditors must not be considered part of the organization’s control environment)
- Operational control information used by the organization is provided to the auditors in response to their information requests
- Auditable organizations stay actively engaged with their auditors and elicit open discussions of the auditors’ observations and preliminary concerns

Auditable Organizations Effectively Respond to Audit Reports

- Organizations that incorporate the audit process into their control culture proactively develop their corporate positions when adverse audit conclusions are expected
- Organizations that successfully support the audit process provide timely written comments to the auditors whenever they are given the opportunity to comment
- The auditors recommendations need to be carefully scrutinized, as they become milestones that the organization’s performance will be measured against
- Written disagreements with auditors are carefully crafted in the context of the organization’s stated control objectives, thereby minimizing the auditors ability to successfully rebut – remember that auditors get the last word