Compliance, Audits and Fire Drills: In the Way of Real Security?

Mark Estberg and John Howie
Microsoft Corporation

Session ID: SP01-203
Session Classification: Intermediate

Introduction

- Microsoft's Global Foundation Services (GFS) runs a world-class ISMS
  - **Our customer is Microsoft itself (not end users)**
  - Focus is proving the security and privacy of the data belonging to our internal customers
  - We are ISO/IEC 27001:2005 certified and undergo PCI DSS, SOC (formerly SAS 70) and FISMA audits
- Despite our program we constantly respond to:
  - Questions about compliance obligations
  - Inquiries from business groups and auditors
  - Fire Drills (both internal and external)

Example 1: Firedrill: Industry incident

- Last year a large online service provider was compromised
  - Microsoft Executives were concerned that Microsoft could be the next target
    - Exacerbated by press rumors and underground chatter
- Security teams across Microsoft were called in to monitor systems and networks
  - A significant amount of time was taken “doing what we already do”
  - Resources dedicated to incident response were not able to perform their usual duties

Example 2: Inquiry: Audit Preparation

- An internal customer contracted consultants to prepare them for an upcoming audit
  - Internal customer over-relied on others to tell them what was necessary and suitable
- Without proper coordination a lot of time was spent examining existing controls for suitability
  - GFS expertise was not relied upon and existing controls and technologies were questioned
    - Internal customer did not want to take a dependency on existing controls and technologies
  - Owners of existing controls spent unnecessary time convincing internal customer of adequacy of controls

Example 3: Compliance: Meeting Obligations

- Multiple compliance obligations for Microsoft appear to conflict with each other
  - Example is Account Lockout in FISMA and PCI DSS
- Obligations can be commercially infeasible or not applicable/required in some environments
  - Convincing internal customers and auditors that you have suitable compensating controls can be difficult
- Managing obligations leads to drawn out discussions with internal customers and auditors
  - Discussions focus on spirit of obligations versus implementation

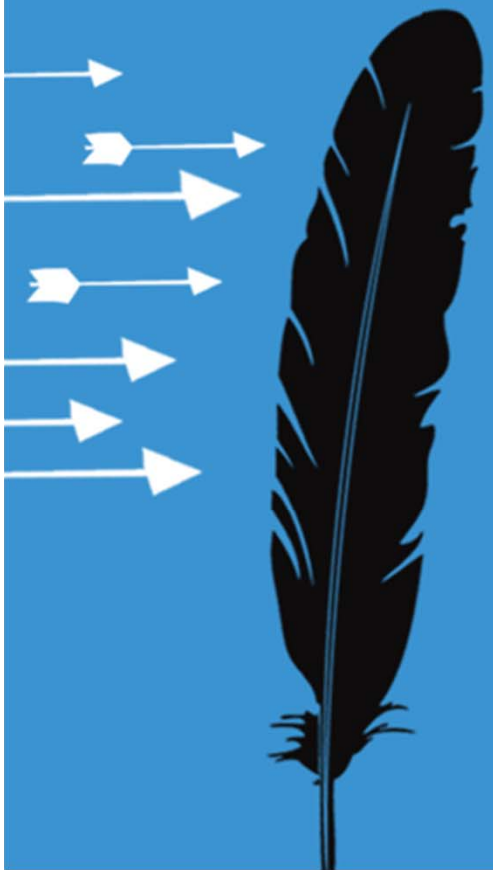
Example 4: Audit: Preparatory Work

- Multiple audits for obligations, standards, etc. assumed by internal customers consume time of control owners and operators
  - Passing audits can inadvertently take precedence over operating, monitoring, responding and optimizing the controls
  - Control owners and operators are required to spend more and more time collecting evidence and answers to auditors' questions
    - Often the same questions come up across different audits, or are asked year-over-year
  - SSAE 16 may make this worse!

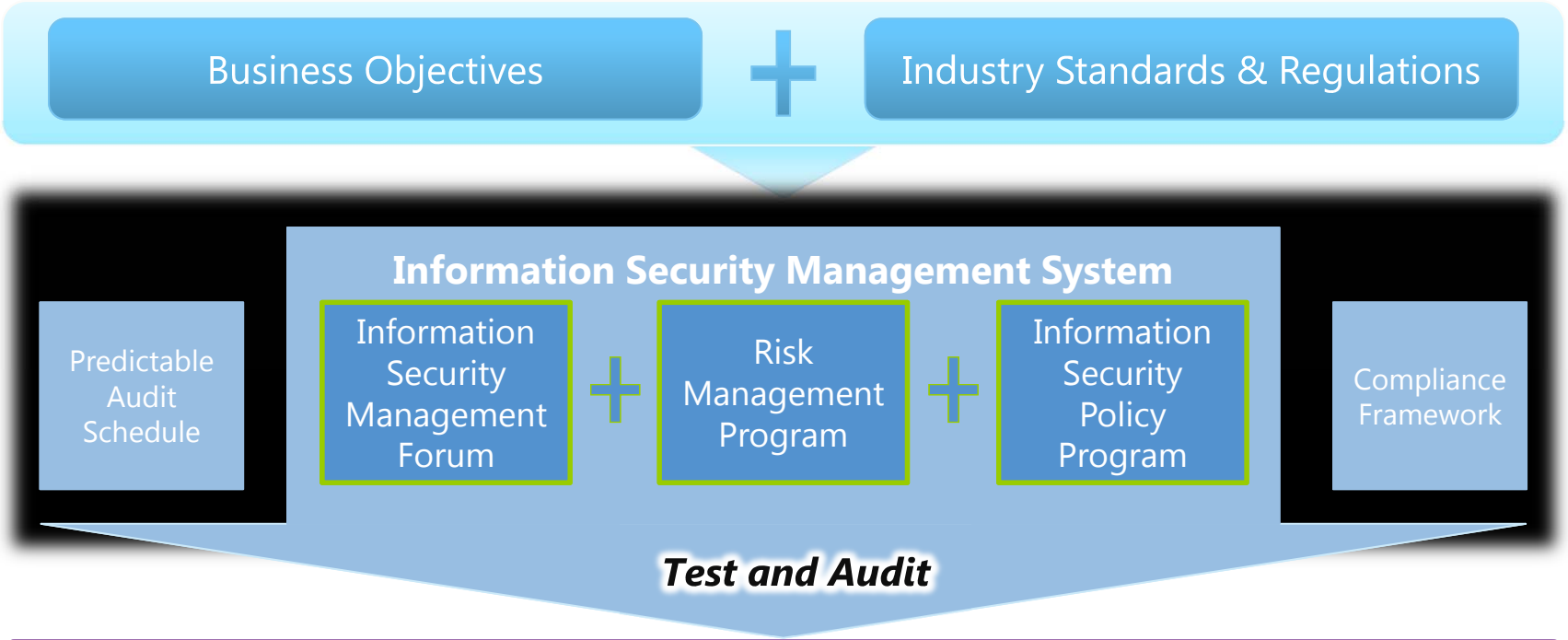
Minimizing The Distractions

- The key to minimizing distractions is:
  - Leveraging your Information Security Management System (ISMS)
  - Building a compliance framework
  - Integrating security and other control monitoring
- Distractions will continue to occur, and you have to accept that
  - The more mature your program is the more success you will likely have in minimizing them, though

Microsoft's Information Security Management System and Compliance Framework



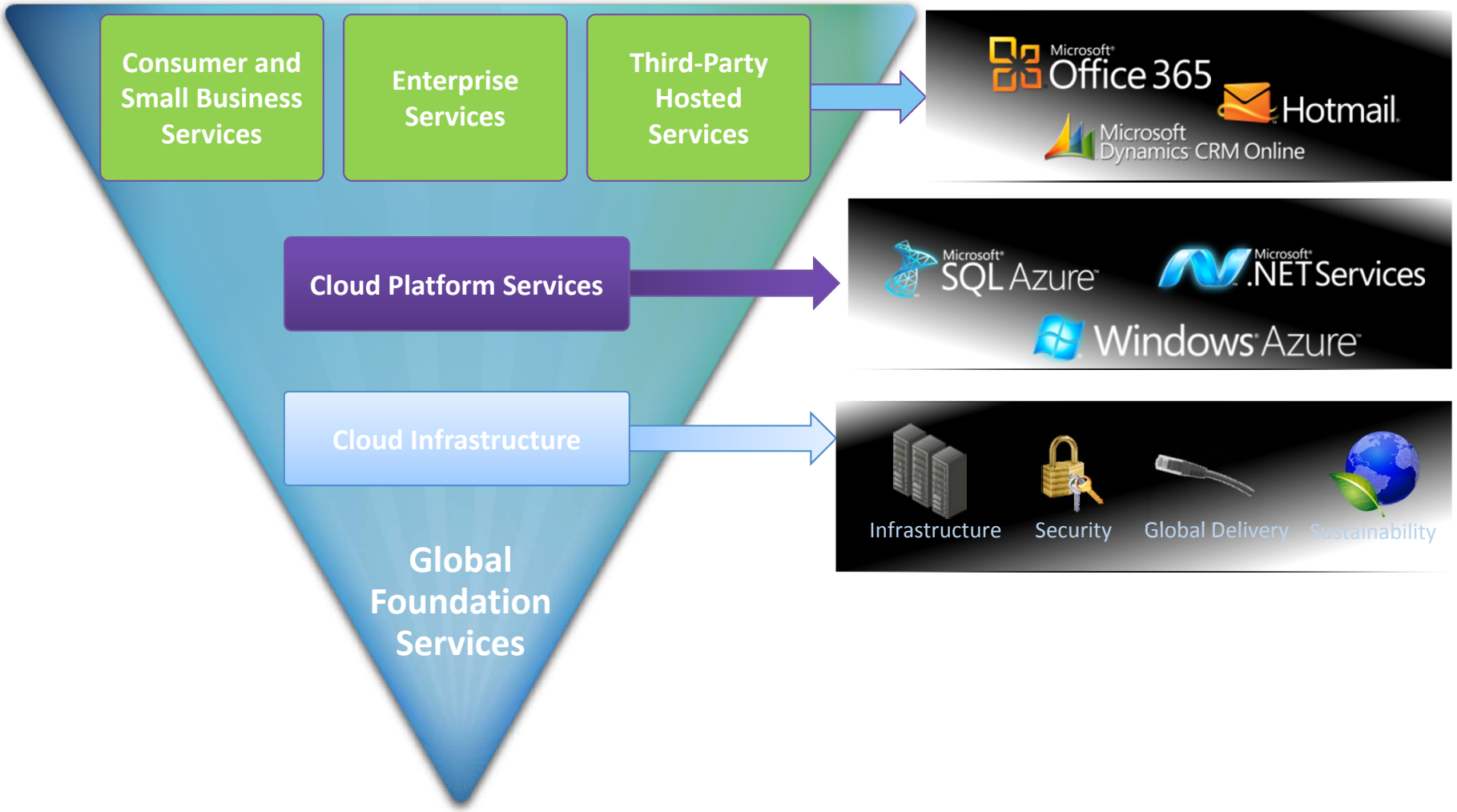
ISO/IEC 27001:2005 ISMS At Microsoft



Certificates and Attestations

- ISO / IEC 27001:2005 certification
- SAS 70 Type I and II attestations (SOC)
- Sarbanes Oxley
- PCI DSS certification
- FISMA certification and accreditation
- And more …

Microsoft's Cloud Infrastructure: Stacked ISMS



Benefits Of Tiered ISMS

- Tiered ISMS allows Microsoft to break down security operations into manageable pieces
  - Core security operations in GFS are used and shared by business groups, and save money
  - Shared security infrastructure in a multi-tenanted environment makes it easier to detect malicious activity at the server and network level and deal with it
- Tiered approach allows internal customers to tailor their ISMS to their customer base JH7

Slide 11

JH7 John Howie, 2/10/2012

Compliance Framework

Industry Standards and Regulations

- Payment Card Industry Data Security Standard
- Health Insurance Portability and Accountability Act
- FISMA (NIST 800-53 r3)
- Business requirements, Sarbanes-Oxley, privacy laws, etc.

Controls Framework

- Identify and integrate:
  - Regulatory requirements
  - Customer requirements
- Assess and remediate:
  - Eliminate or mitigate gaps in control design

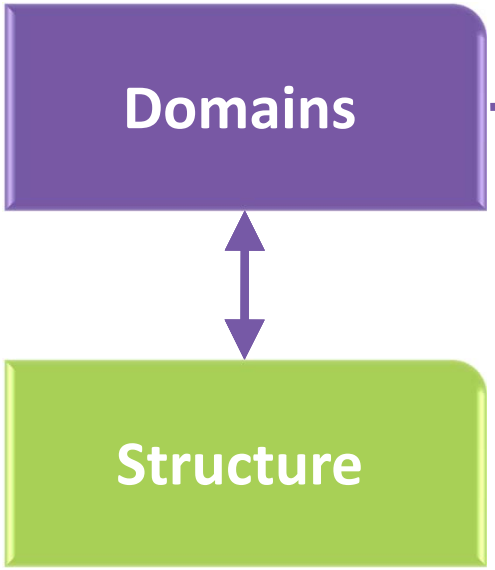
Predictable Audit Schedule

- Test effectiveness and assess risk
- Attain certifications and attestations
- Improve and optimize:
  - Examine root cause of non-compliance
  - Track until fully remediated

Certification and Attestations

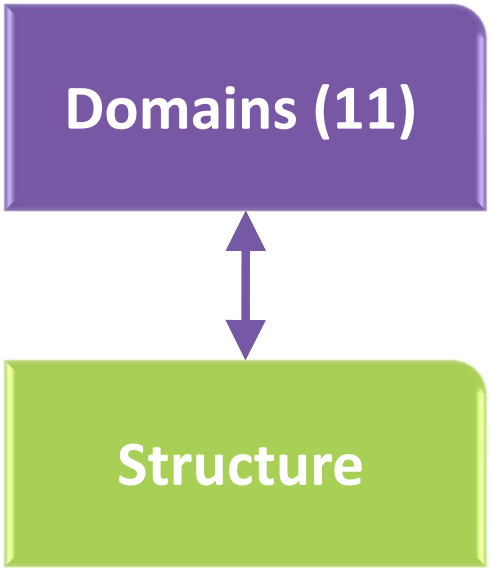
- ISO/IEC 27001:2005 certification
- Statement of Auditing Standard 70 type II attestation (SOC)
- PCI DSS certification
- FISMA certification and accreditation, etc.

Control Framework: Domains



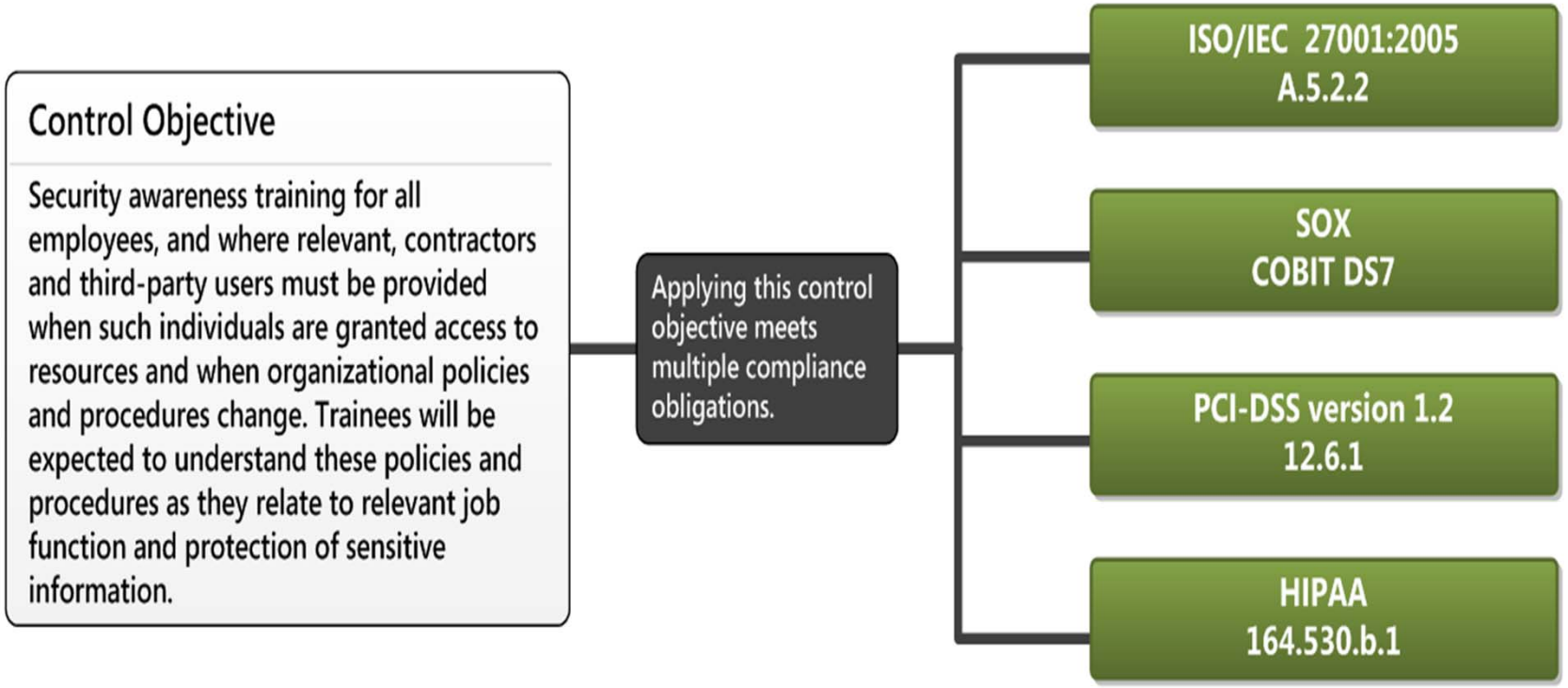
1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development, and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Control Framework: Structure



- Policy Objectives (62)
- Control Activities (612)
- Audit Requirements
  - 1,587
  - 8 Sources
- Control Owner
- Documents / Records
- Testing Procedures
- Cost Data
- Historical Health Data
- Importance Data
- Maturity Data

Rationalized Requirements



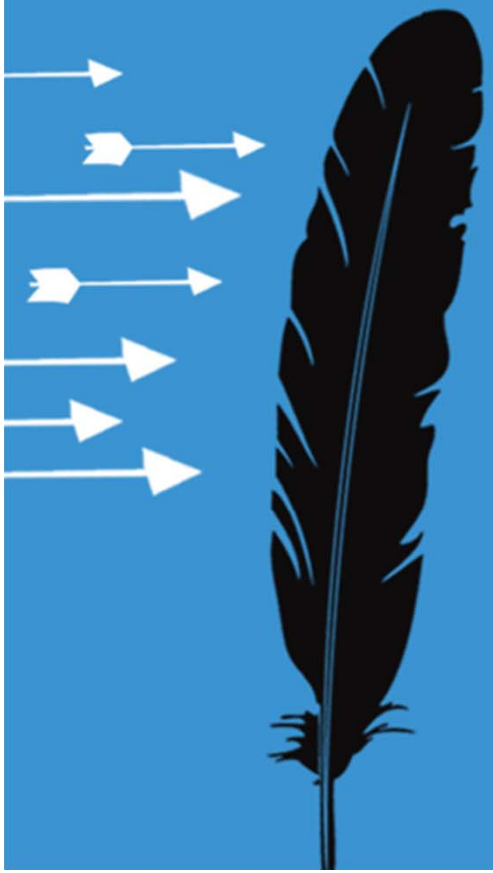
Benefits Of Compliance Framework

- The compliance framework and rationalized obligations approach:
  - Eliminates confusion over conflicting compliance obligations and time spent explaining decisions to internal customers and auditors
  - Drastically reduces time spent preparing for audits by reducing number of times audit evidence is collected

Slide 16

JH8 Re-iterated that this is all for internal customers, not external customers
John Howie, 2/10/2012

Integrated Control Monitoring and Incident Response



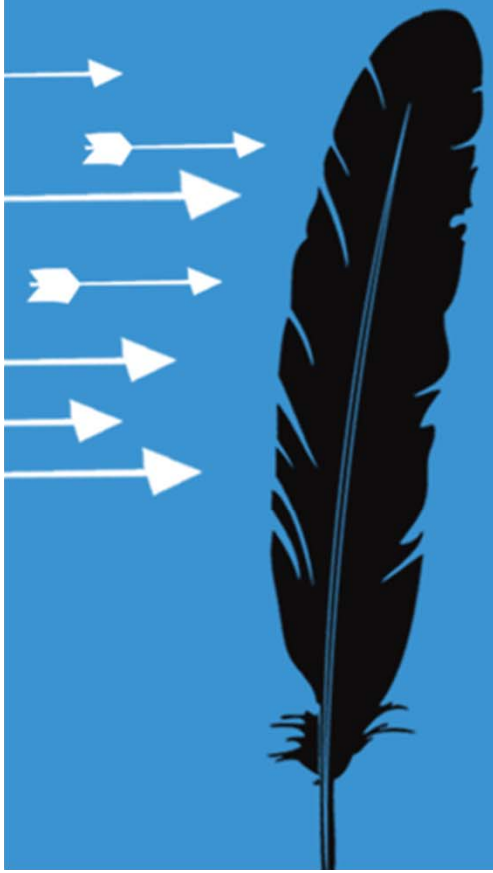
Incident Response

- Security Incident Response is a Tier 2+ function
  - Tiers 0 and 1 are handled by the Microsoft Operations Center (MOC) – a fully staffed 24x7 function
    - Initial alarms are handled by trained technicians using documented Trouble Shooting Guides (TSGs)
    - Alarms that cannot be handled by the MOC are escalated to the on-call Security IR team members
- Security Incident Response follows documented processes that are based on ISO/IEC 18044 and NIST SP800-61
  - ISO/IEC 27035:2011 not used (yet)

Integrated Monitoring

Benefits Of Integrated Monitoring

- Many incidents can indicate a security problem:
  - Network outage
  - Server crash
  - Running out of disk space
- Integrated monitoring provides a more holistic overview of the state of the environment
  - MOC staff can make connections and report suspicions on to Tier 2 Security Incident Response
  - Shift patterns can be adjusted to handle extraordinary events
- Having Security Incident Response at Tier 2 frees them up from monitoring controls and allows them to pursue qualified events



Bringing it all together

Apply Learning To Minimize Distractions

- Create an Information Security Management System if you do not already have one
  - If you do not know where to start begin with ISO/IEC 27001:2005
- Create a control framework
  - Bring together all your compliance obligations together, reconcile conflicts, and design controls
  - Make sure control framework is covered by ISMS
- Integrate security monitoring with other system and network monitoring
  - Optimize engagement of your deep security subject matter experts