IT Governance

Real Security from Leadership and Process

Bill Stackpole, CISSP/ISSAP, CISM
Senior Security Consultant
Microsoft Corp.

“Information security is not a technical issue that can be delegated to the CIO, but a core governance issue that demands the attention of the CEO and boards”

Source: National Cyber Security Partnership

- **Technology is not the problem**
- **Current technology can secure our systems**
- **Emerging technologies continue to improve system security**
- **New technologies are making security easier to administer**

Session Objectives

Ammunition and Approaches

- Value and benefits of sound security leadership and processes
- Evaluate weaknesses in existing governance structure
- Develop IT Governance strategy
- Establish metrics for measuring the effectiveness of security processes
- Use Microsoft lessons learned to address governance issues and failures

What is Security Leadership?

Information Security Governance (ISG)

- Begins at the Board of Directors
- A integral part of corporate governance
- Same policies and controls used to direct and manage the organization as a whole
  - Risk management
  - Reporting
  - Accountability
- Responsibility for ISG is being redefined by new laws and regulations

The Goals of ISG

- Make information security a fundamental business issue at the CEO and Board level
- Align information security efforts with business objectives
- Balance IT investments with business risk decisions
- Create Security Enabled Organizations

Drivers for ISG

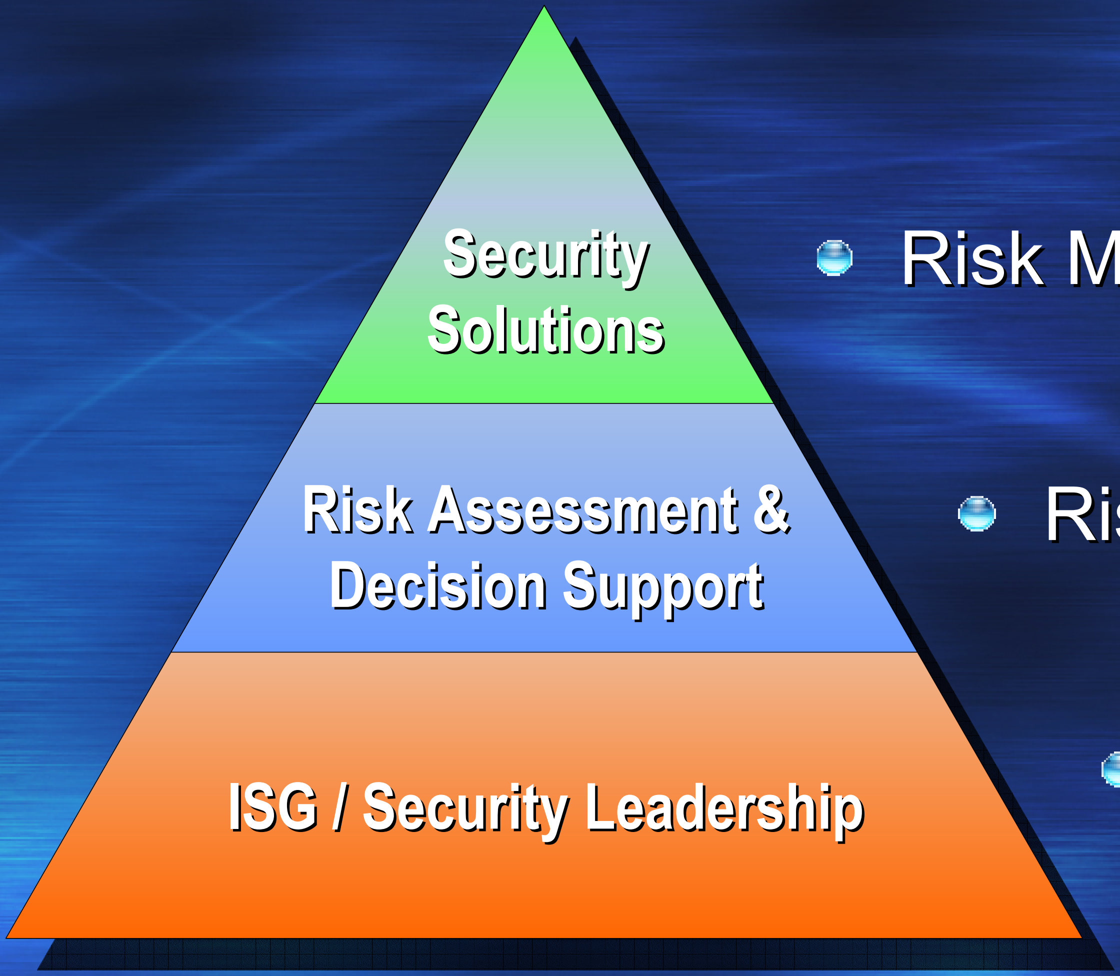
- Laws and Regulations
  - US – Sarbanes-Oxley
  - UK – Data Directive
  - Canada - Personal Information Protection and Electronic Documents Act
- Threat of increased regulation
- Extended Organization

Benefits of ISG

- Avoid IT failures and resulting impacts on enterprise's value, reputation and competitive position
- Leverage IT's enabling capacity for new business innovations and practices
- Integrate with partners and connect with customer safely
- Measure IT security performance and ROI
- Incorporate and leverage new technologies

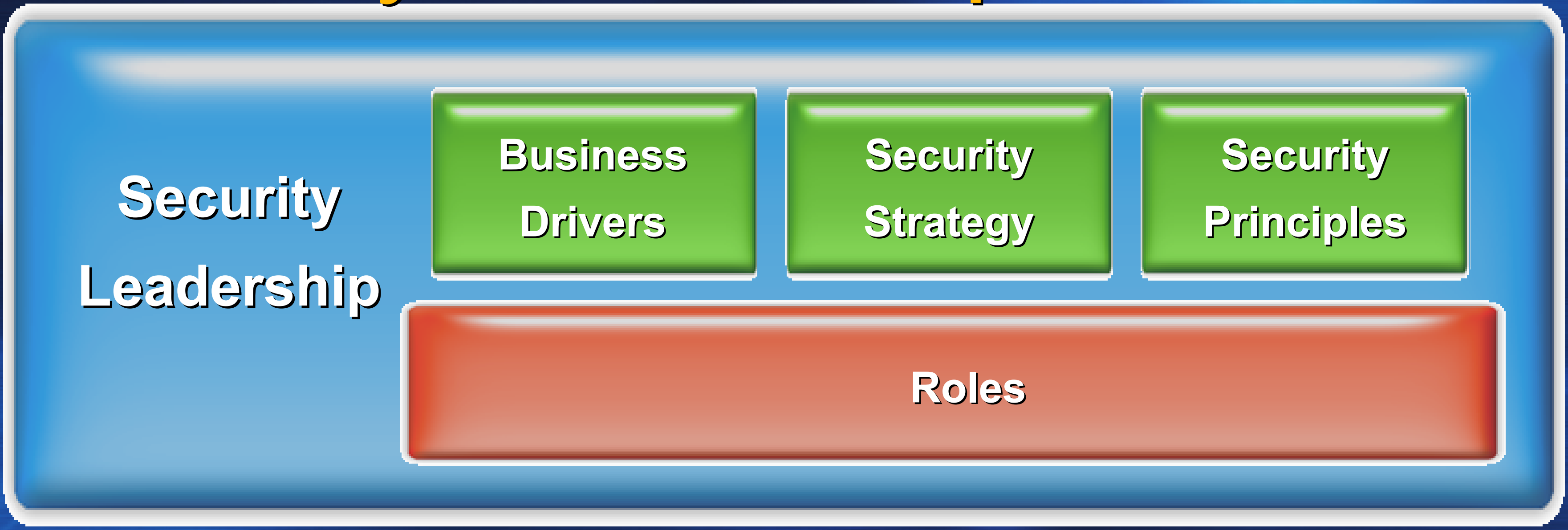
Security Enabled Business

Framework



- Risk Mitigation
- Risk Identification
- Risk Definition

Security Leadership



Security Leadership

Business Drivers

Security Strategy

Security Principles

Roles

- Business Drivers
  - Regulatory Compliance
  - Industry Standards
  - Partner/Vendor Connectivity
  - Customer Confidence

Business Drivers - Regulation

Tone at the Top

- **Documentation**
- **Training**
- **Communications**

‘CEOs and CFOs must ensure that their “tone at the top” is carried to <u>every corner of the company</u>. . . executives must be able to prove not only that policies, guidelines, and critical communications are sent out company-wide but that those policies have been read, understood, and agreed to by all employees.’

The Sarbanes-Oxley Act: Impact on Human Capital Management
Peoplesoft, Inc.

Business Drivers

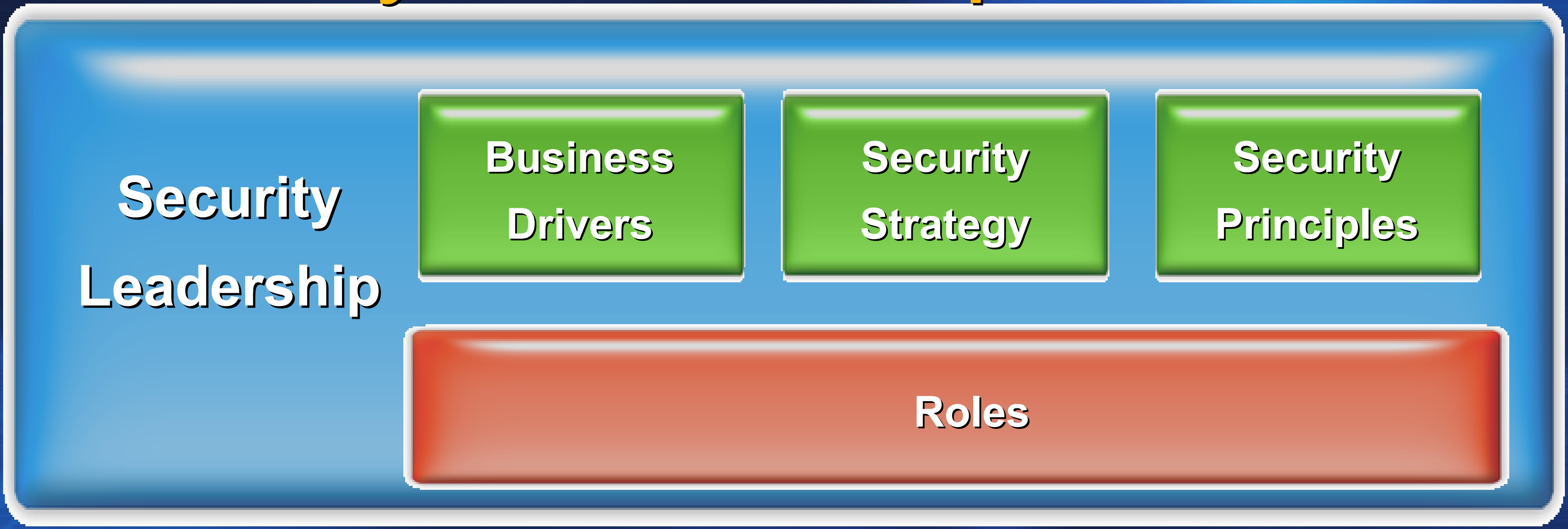
Industry Standards

- **COSO** - Internal controls and risk management
- **ISO 17799 -** Information security management
- **ISO/IEC TR 13335** - Security planning, implementation and maintenance
- **ITIL** - IT service processes and management
- **ISO/IEC 15408 – Security** products/services evaluation
- **TickIT -** Software quality management
- **NIST 800-14 -** IT security program
- **COBIT**- IT governance

Evaluation Points

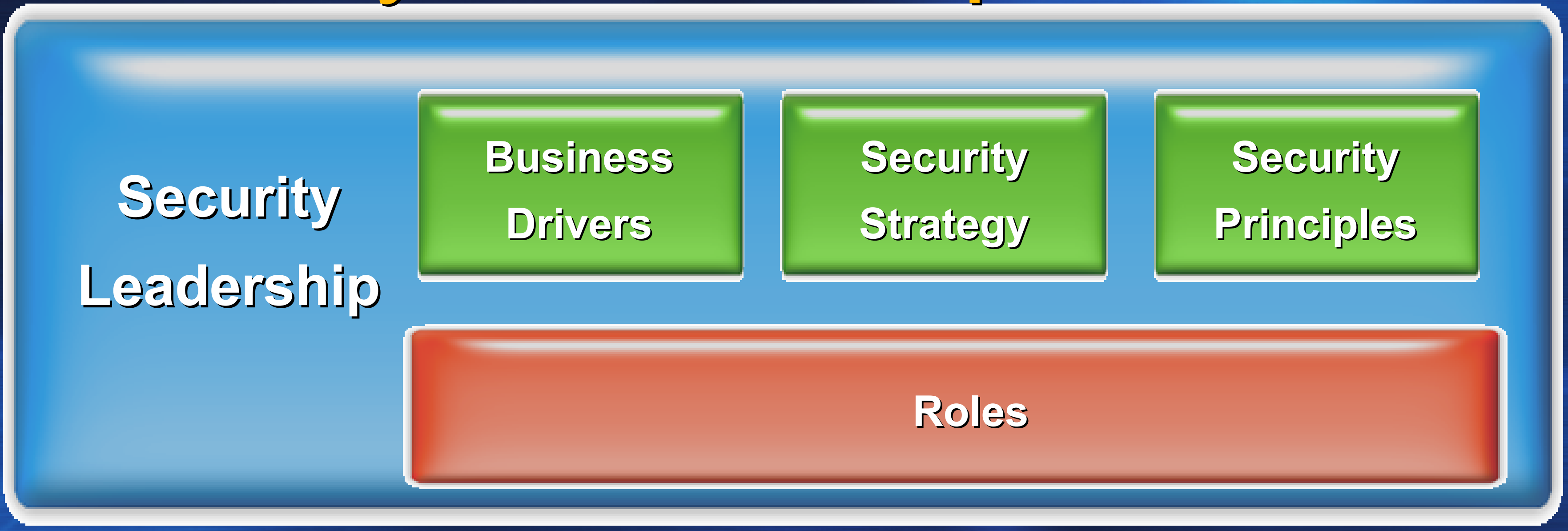
- What standards are activity used in your security management program?
- Are your policies and standards aligned with industry standards?
- How well do your operations, maintenance and monitoring practices align with industry best practices?

Security Leadership



- Security Strategy – Proactive vs. Reactive
  - Management commitment/sponsorship
  - Security defined in terms of value to business objectives
  - Clearly defined vision, mission and scope

Security Leadership



Security Leadership

Business Drivers

Security Strategy

Security Principles

Roles

- Security Principles
  - Confidentiality, Integrity, Availability
  - Isolation
  - Identity Assurance
  - Defense in Depth
  - Engineering Excellence
  - Least Privilege
  - Operations Excellence
  - Separation of Duties

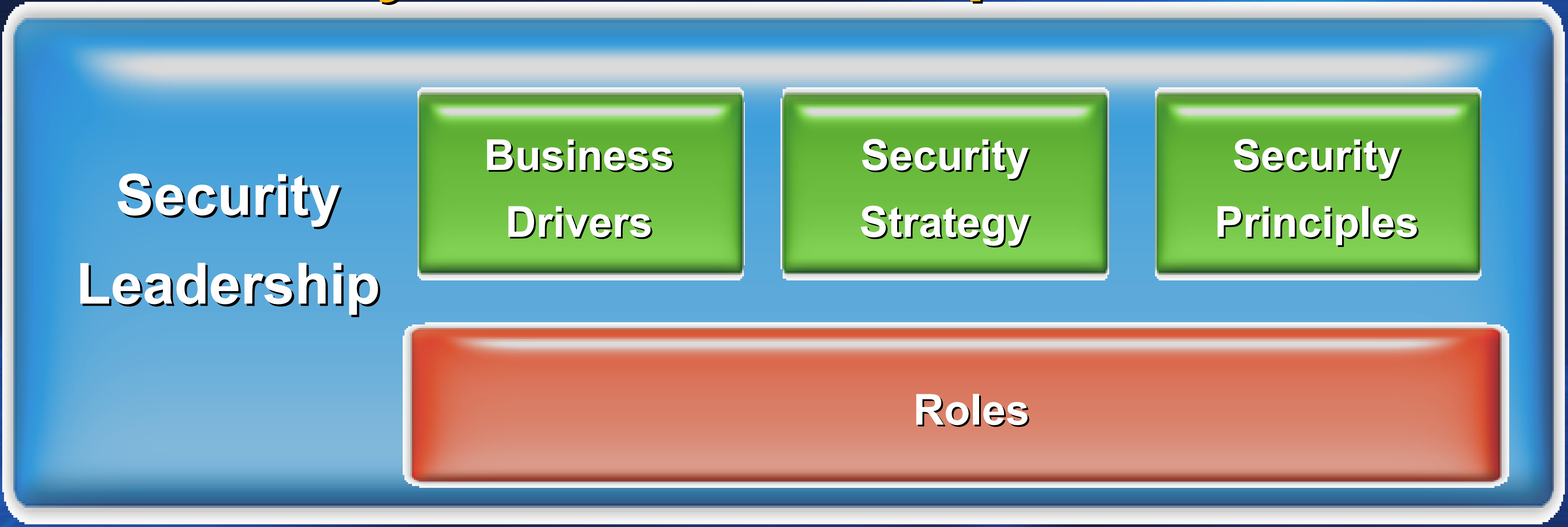
Security Principles

Security Principles	Description
Isolation: manage risk across the full suite of technical control points	Securing the network Secure application operation Locking down clients and servers Data security and privacy Physical security
Identity Assurance: includes authentication, user privacy, and data access authorization	Manage to practice of least privilege Base decision on data classification and use Enforce privacy and privacy rules Monitor identity assurance
Engineering Excellence: dedicated to the design and development of secure systems	Secure application development Build security into the life cycle Secure systems architecture Reduce attack surface Ensure availability
Operations Excellence: people, processes, and technology to maintain and operate secure systems	Plan for system maintenance and updating Enforce security configuration and hardening Monitor and audit Practice incident response Awareness and training

Evaluation Points

- Does your program have a clearly defined vision, mission and scope?
- Is it aligned with your company's business objectives?
- What are the key security principles that govern your program?
- Can you identify them? Articulate them?

Security Leadership



Security Leadership

Business Drivers

Security Strategy

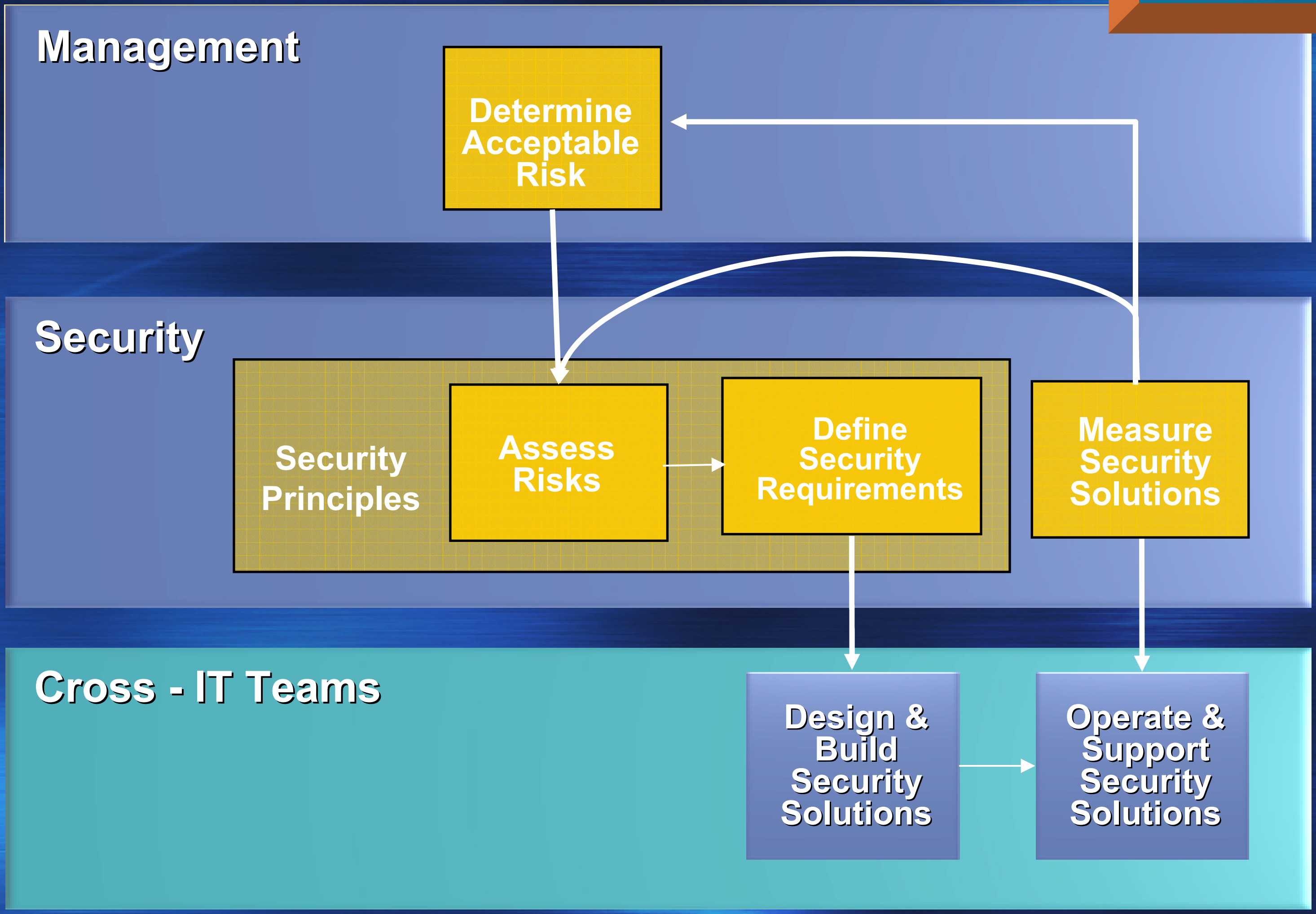
Security Principles

Roles

- Security Roles
  - Management
  - Administration
  - Audit
- Filling the Gaps

Roles (Organizations)

Security Leadership
Risk Management
Security Solutions



Management

Determine Acceptable Risk

Security

Security Principles

Assess Risks

Define Security Requirements

Measure Security Solutions

Cross - IT Teams

Design & Build Security Solutions

Operate & Support Security Solutions

Evaluation Points

- Does your ISG have a clearly defined roles and responsibilities?
- Are they part of HR job descriptions?
- Have competency requirements been defined?
- Are skill actively managed?

Lessons Learned at MS IT

- Executive sponsorship
- Stakeholder consensus
  - Corporate Security
  - IT Operations and Support groups
  - Line-of-Business Application owners
- Well-established lines of communication
- Clear expectations
- Well-defined roles and responsibilities
  - Document work flow and procedures
  - Document minimum requirements
- Continuous improvement

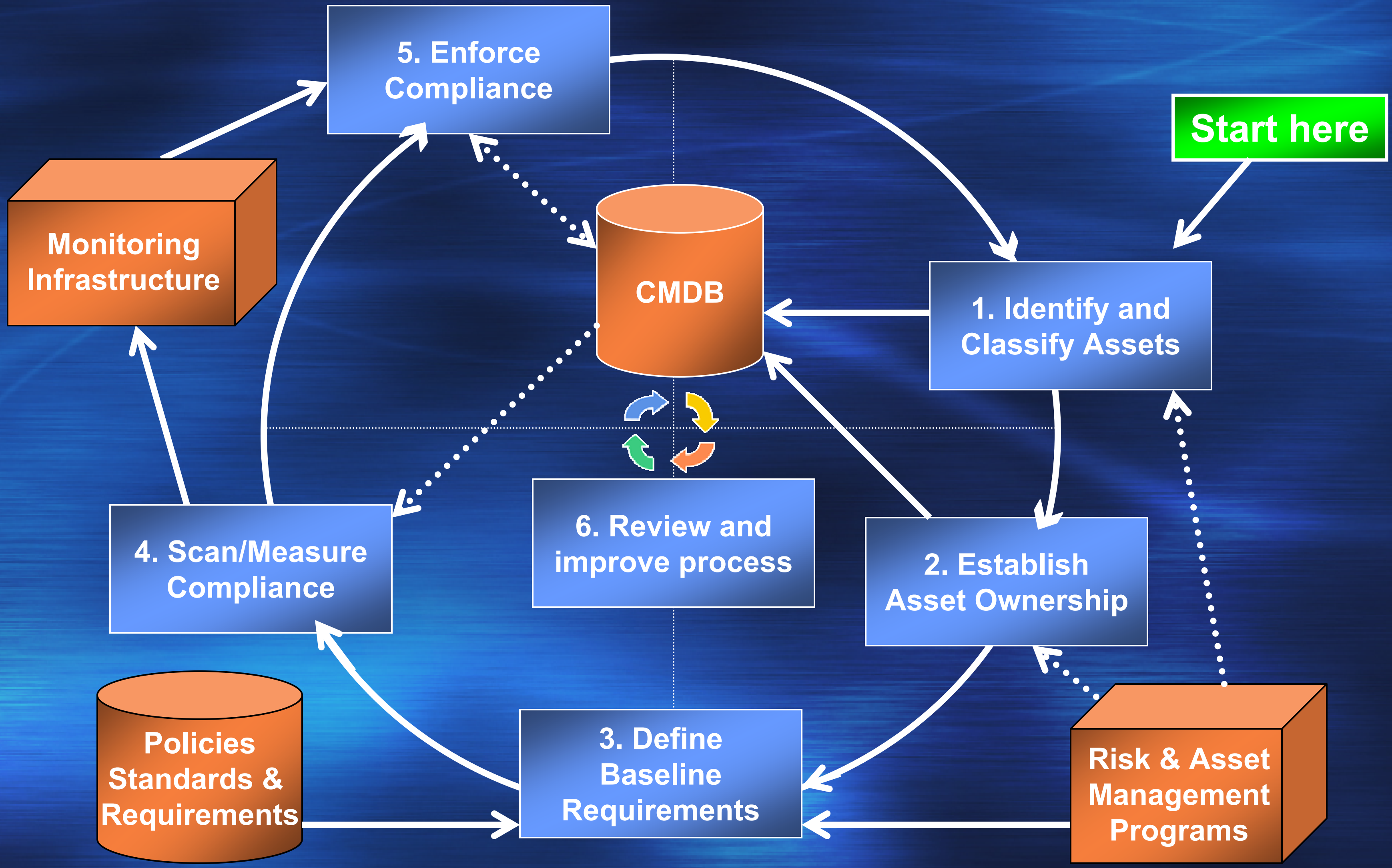
Key ISG Processes

- Risk Management
- Data Management
- Change Management
- Configuration Management
  - Build/Rebuild
  - Patch/Update
- Security Operations Management
  - Administration
  - Monitoring
  - Incident response
- Compliance Management

Processes and Practices

- Comprehensive
- Documented
- Consistent and repeatable
- Decision support
- Flexible
- Accommodating
- Continuous evaluation and improvement

Compliance Process Example



Start here

1. Identify and Classify Assets

2. Establish Asset Ownership

3. Define Baseline Requirements

4. Scan/Measure Compliance

5. Enforce Compliance

6. Review and improve process

CMDB

Monitoring Infrastructure

Policies Standards & Requirements

Risk & Asset Management Programs

Lessons Learned at MS IT

Program Operations

- Communicate, Communicate, Communicate
  - Consistent format
  - Requirements and Timeframes
  - Enforcement actions for non-compliance
- Make the process visible to users
- Coordinate, Coordinate, Coordinate

"The process only works when everyone is tracking on their tasks"

Lessons Learned

- Repeatable & sustainable process
  - Document templates, work flow, checklists
  - Continuous evaluation and improvement
- Build process with key stakeholders
  - Establish clear roles and responsibilities
    - Who is responsible
    - Who is accountable
    - Who is consulted (management, other teams…)
    - Who do you inform (management, other teams…)

Lessons Learned

- Maintain a list of the minimum requirements
- Give the user base a voice
  - Provide a clear escalate path
  - Provide a feedback loop
- Only make short term exceptions

Benefits

MS IT Results

- 2 years ago
  - 85% Compliance
  - Two week timeframe
  - Several long term exemptions
- Today
  - 99% Compliance
  - Four day timeframe
  - Handful of short term exemptions

Roadmap

- Q1 - Risk Assessment
  - Develop your security leadership model
  - Review program policies, standards & roles
  - Classify findings as red/yellow/green
- Report findings to BOD Governance Committee and get support for ISG
- Q2 – Fill the gaps

Roadmap – Q3

- Review general practices
  - Minimize business unit involvement
- Clarify red/yellow/green evaluation criteria and identify gaps
- Identified business critical systems and dependences
- Create and present a Risk Scorecard to the BOD

Roadmap – Q4

- Perform simple subjective risk analysis with business unit stakeholders
- Express risk using the formula: vulnerability x threat x impact

For example - “Inconsistent account provisioning grants malicious users the ability to delete critical data that could result in loss productivity or the loss of intellectual property.

Roadmap

- Improve processes
  - Involve business unit stakeholders
  - Define requirements
  - Built consensus
- Improve measurement
  - Define baselines
  - Automate monitoring & reporting tools
- Improve controls

Microsoft®

Your potential. Our passion.™

Questions?

Bill Stackpole, CISSP/ISSAP, CISM wstack@microsoft.com

Resources

- IT Governance Institute http://www.itgi.org
- Tools and Resources for Security Management www.theiia.org
- **Corporate Governance Task Force of the** National Cyber Security Partnership www.cyberpartnership.org
- Information Security Roles & Responsibilities Made Easy – Charles Cresson Wood
- **Information Security Policies and Procedures: A Practitioner's Reference – Thomas Peltier**