



WIPO Information Security Program

Lilia Vogt

SCIT, June 2002

Components

- Confidentiality
 - sensitive business objects (information & processes) are disclosed only to authorized persons
- Integrity
 - safeguarding the accuracy and completeness of information and processing methods
- Availability
 - ensuring that authorized users have access to information and associated assets when and where required

Information Security is about ...

- People
- Technical controls
- Risk Management
 - Mitigate, transfer or accept
 - No 0% risk
 - Risk that is well understood

The Challenge

- Increased dependence on IT
 - Increased accessibility
 - New risks and scope
- Increased reliance on public systems and networks
- New business areas (Online Arbitration, WIPOnet, E-filing, EDMS, etc.)
- General increase in the value of information
- Increase in cyber attack activities

The Approach

- Assurance
 - To sustain Business Continuity despite power outages, natural disasters, human error, hardware failures, etc.
 - To maintain availability and quality of information
 - To increase control and stability through Change Management processes
- Security
 - To enable access for user community to needed services
 - To protect the user community from malicious acts
 - To protect the Organization from embarrassment and financial losses

Implementation guidelines

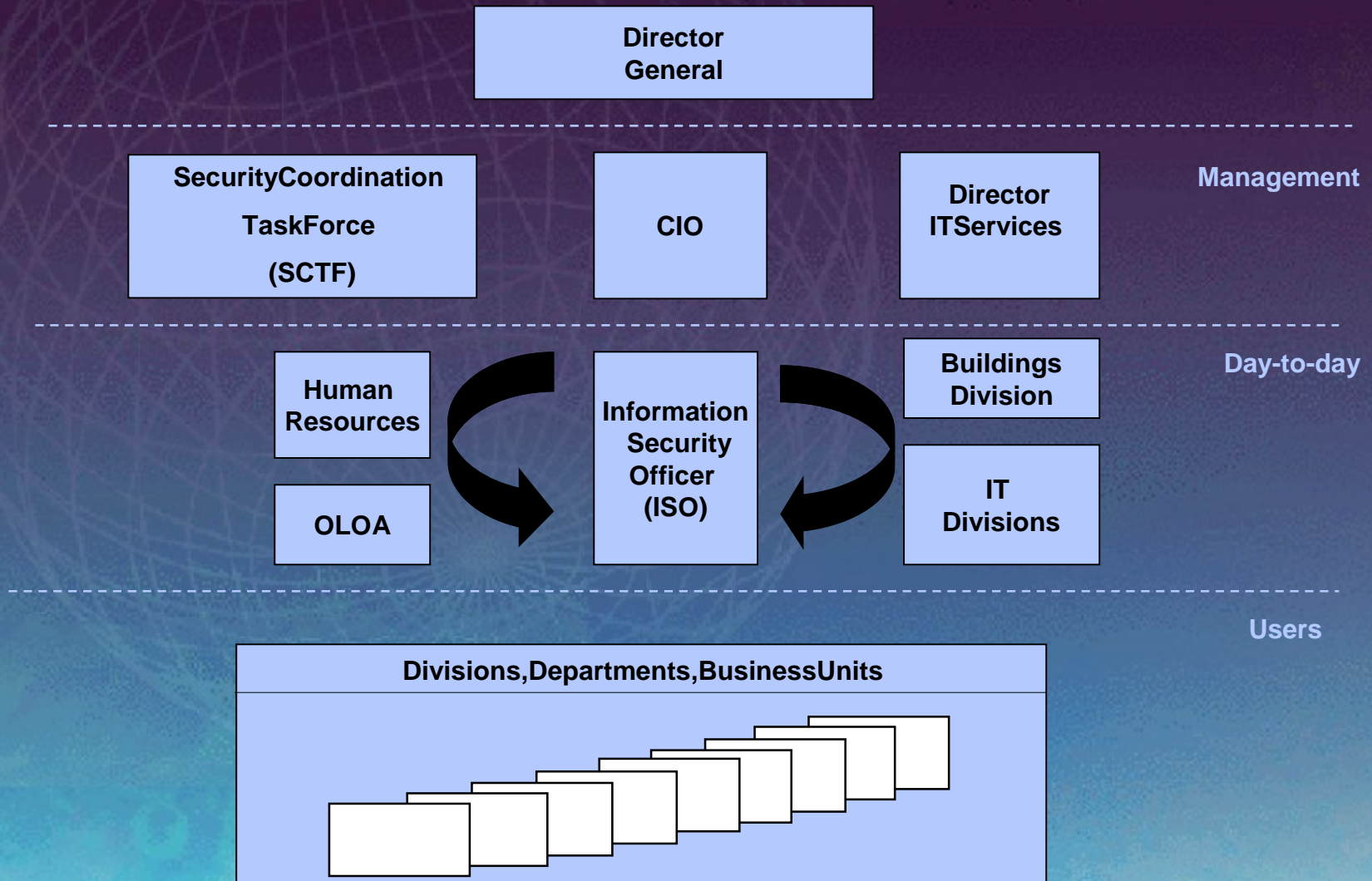
- Aligned with WIPO business objectives
 - Not security for security
- Cost-effective
 - Not security at any cost
- Layered
 - Physical, network, system, application, interface and procedural security
- Commensurate with the threats and objectives
 - Not total security
- Consistent and followed
 - Not a one-time event

Main functions

- Coordination of information security activities on Organizational level
- Security policies, standards and procedures
- Risk Management
- Access control & compliance
- Awareness and training
- Business continuity and disaster recovery
- Incident handling
- Physical security of information and systems

WIPO Information Security Program

IS Reporting



Responsibilities in the Information Security Administration

Information Security Administration

Overall Security Planning and Management

- Work with management on policies, standards and procedures
- Advertising the Security Program
- Risk Assessment and Management
- DRP & BCP
- Compliance monitoring
- Security Training and Awareness

Information Security Officer

Day-to-day System Administration

- Keeping the systems running
- Logs monitoring
- Doing daily backups
- Applying patches

System Administrators

Day-to-day Security Administration

- Accounts Management
- Security profiles
- Passwords and password controls

- Security Health checking
- Vulnerabilities testing

Information Security Officer

Security Administrators

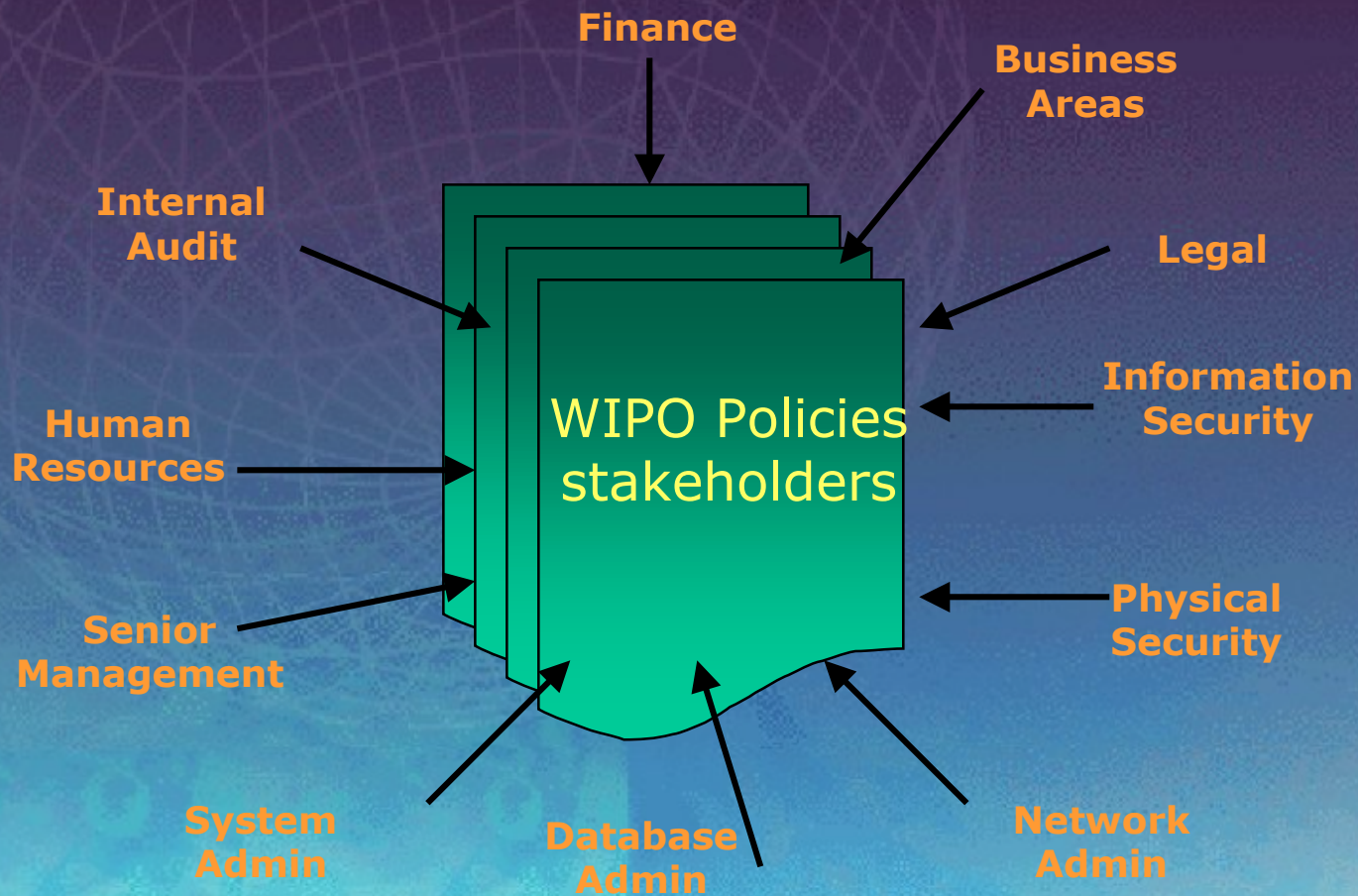
What has been achieved

- Management structures in place
- Main roles and responsibilities defined
- Central coordination established
- Security policies developed and approved
- Security standards, baselines and procedures
- Awareness program initiated

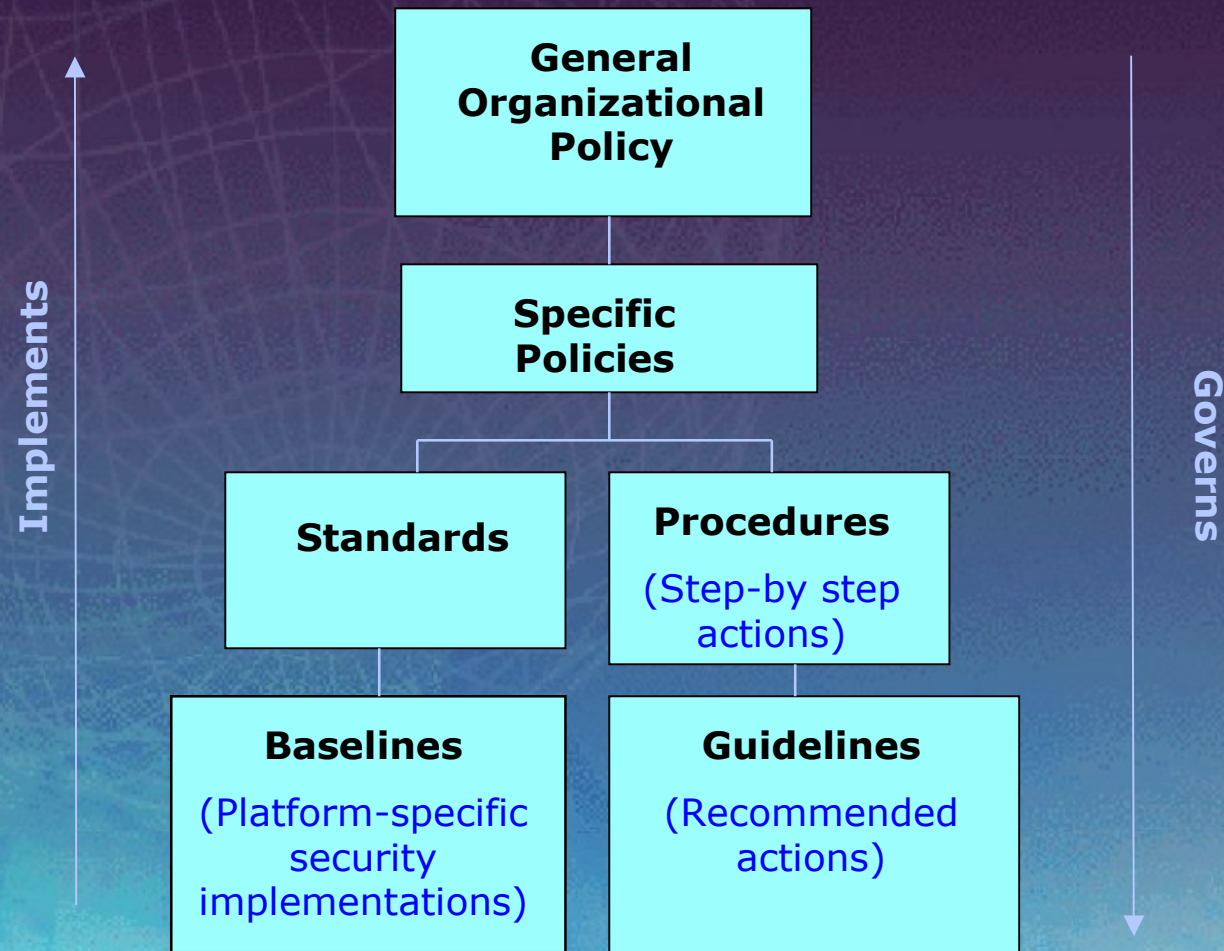
Why security policies

- Starting point of any Information Security Program
 - Define the general security framework
 - Set the stage in terms of what tools and procedures are needed
 - Provide guidance when incident occurs
- Policies define responsibilities and expectations
 - Requirements for protection of technology and information assets
 - Acceptable use for regular and privileged users
- Policies communicate consensus among all major sectors in the Organization

Who participated in the policies development



Policies, standards, procedures, baselines



Examples of WIPO IS Policies

- General Organizational Policy
- Acceptable Use Policy
- E-mail Policy
- Internet Access Policy
- Remote Access Policy
- Communications Policy
- Password Policy
- Privacy Policy

Next steps

- Information Security Policy implementation
- Extending the Information Security Awareness program
- IT Operations Risk Assessment
- Vulnerabilities Testing
- Reinforcing the resources
- Improving the monitoring
- Contingency Planning
- and the list goes on...

Key elements for success

- Management commitment
- Clearly defined and implemented security policies and principles
- Must be business driven
- A security awareness program that reaches everybody in the Organization

Thank you!

The image features a 3D, metallic-looking 'Thank you!' text that is slightly tilted. The background is a gradient of blue, transitioning from a darker purple-blue on the left to a lighter cyan on the right. A faint, wireframe globe is visible in the background, centered behind the text. The overall aesthetic is clean and professional.