CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

In conjunction with WIF-KL 2012

WIF KL WORLD INNOVATION FORUM KUALA LUMPUR

csm-ace 2012

CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

CYBERSECURITY RISK & COMPLIANCE FOR ECONOMIC TRANSFORMATION

www.csm-ace.my

Should Standards be Mandated?

Thaib Mustafa

Chairman, Technical Committee on Information Security Standard Development, Malaysia

7th November 2012

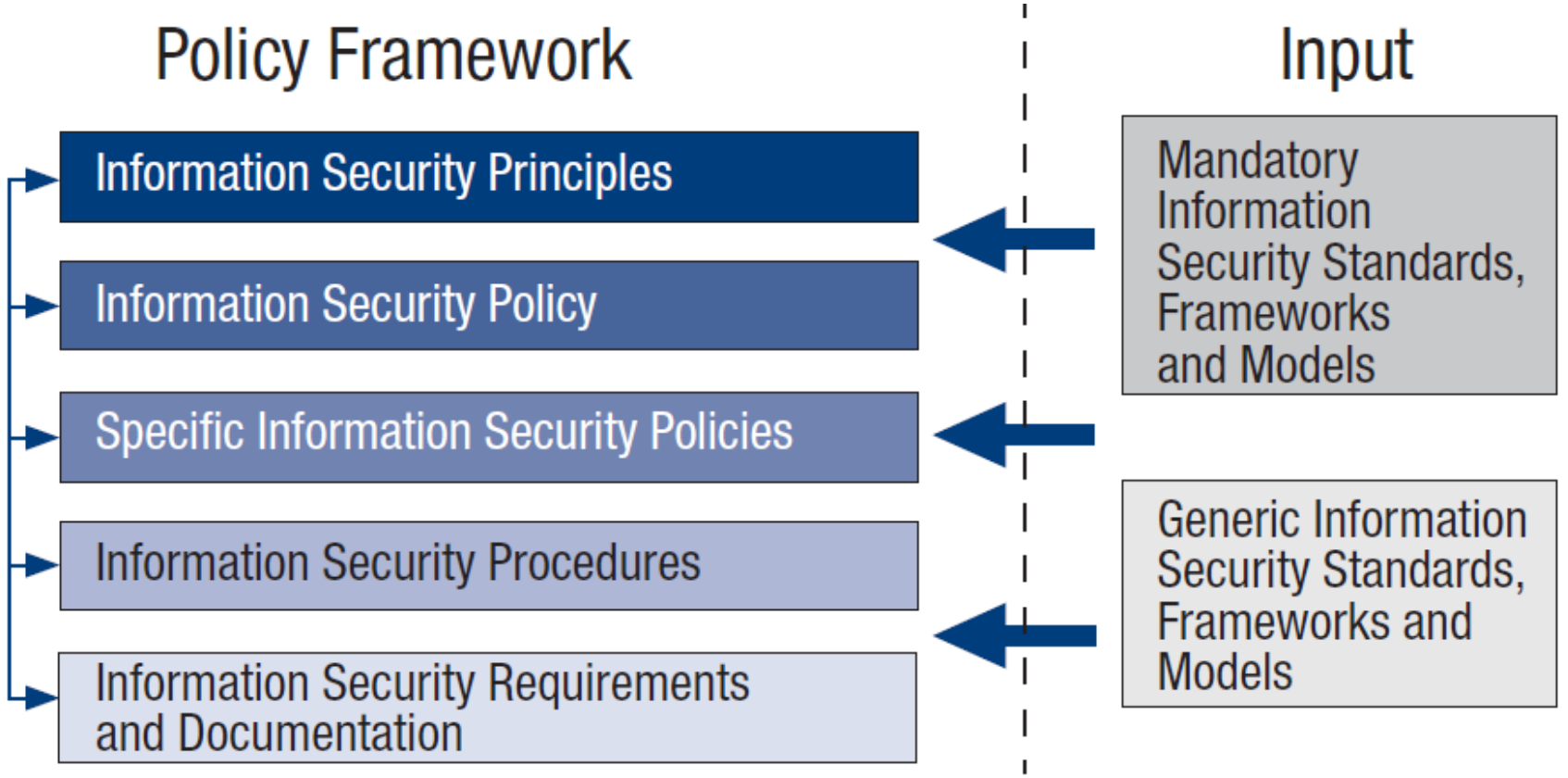
Why Mandated?

- In general, security standards are developed based on best practices and to be adopted on a voluntary basis
- Mandatory compliance to standards are mainly for certification purposes
- Mandatory compliance to security standards only applicable as the last resort after voluntary and directive order

Regulatory Challenges

- Regulatory Framework
  - Clear goals, objectives, fit for purpose, regulators, review process/acts
- Security Standards
  - What & which standards, local & International
- Stakeholders
  - Ownership, accountability & responsibility, cost & benefits
- Political
  - Political will to enforce, time, budget & resources
- Technology
  - Rapid changes of technology, availability & cost of supporting tools
- Social
  - Customer & user acceptance, role & responsibility
- Environmental
  - Changes in environmental control, green technology, cloud, BYOD

IT Security Policy Framework (COBIT5 for Information Security)



Security Governance

"Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.“

– IT Governance Institute

Security Governance Challenges (1/2)

- Board members do not understand that information security is their responsibility and focus solely on corporate governance and profits
- CEO, CFO, and business unit managers think that information security is the responsibility of the CIO, CISO and IT department and do not get involved
- CISO use general security policies, inserted his company's name and get the CEO approval
- All security activity takes place within the security department, thus security works in silo and is not integrated throughout the organization

Security Governance Challenges (2/2)

- Business processes are not documented and not analyzed for potential risks that can affect operations, productivity and profitability
- Policies and standards are developed, but no enforcement or accountability practices have been envisioned or deployed
- Security products, managed services and consultants are deployed without any specific research or targeted performance metrics to evaluate the ROI or effectiveness lead to the false sense of security
- Organization does not analyze its performance for improvement, but continually move forward and repeatedly makes the same mistakes

Effective Security Governance

1. Board members must understand that information security is critical to the company and being updated on security performance
2. Executive management participate in a risk management committee and set an acceptable risk level and security policies
3. Business unit managers responsible for carrying out risk management activities and document critical business processes
4. Employees are held accountable for any security breaches
5. Security products, managed services and professional services are deployed in an informed manner and reviewed for cost effectiveness
6. Continuously review the business processes, including security for improvement

Mandated Security Governance

1. Dedicated Security Organization & CISO
2. Clear Security Policy
3. Adoption of Security Standards
4. Declaration of Security Policy
5. 3rd Party Security Audit
6. Annual Security Report

Example: Clear Security Policy

- Recognize the importance of protecting customer privacy and security.
- Understand that secure products/services are instrumental in maintaining the customer trust and confidence.
- Strive to create innovative products that both serve the customer needs and to operate in the customer best interest.
- Commitment to keep the information safe and secure.
- Provide layered security strategy throughout the organization.
- Provide controls at each level of data storage, access, and transfer.
- Assurance on data privacy, confidentiality, integrity and availability at all times.

Example: Declaration of Security Policy

- Corporate Security Policy (Security Commitment)
- Organizational Security (CISO, Dedicated Security Team)
- Asset Classification & Control (Access, Deletion, Disposal)
- Personnel Security (Security Scanning)
- Physical & Environmental Security (Secure Area, Facility)
- Operational Security (Malware Prevention, Monitoring, VM, Incident)
- Access Control (Authentication, Authorization, Accounting)
- Systems Development & Maintenance (Design, Testing, Review)
- Disaster Recovery & Business Continuity (Replication, Backup)
- Regulatory Compliance (Legal Info Access, Privacy, 3rd Party Audit)
- Apps Security & Compliance (2 Factor Authentication, HTTPS)

CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

In conjunction with WIF-KL 2012

WIF KL WORLD INNOVATION FORUM KUALA LUMPUR

csm-ace CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION 2012

CYBERSECURITY RISK & COMPLIANCE FOR ECONOMIC TRANSFORMATION

www.csm-ace.my

THANK YOU

Thaib Mustafa

thaibmus@tm.com.my

Chairman,

Technical Committee on Information Security Standard Development, Malaysia