Trustworthy Computing

TwC Governance- Unified Incident Response

Private Sector Governance- Accountability and Decisioning for Success

Michele L. Turner, MBCP, FBCI, ITIL, CISA, CRISC, GRCP

Microsoft

Agenda

- Microsoft
  - Corporate Background
  - Trustworthy (TwC) Computing Background
  - TwC Governance
- What Is Governance?
  - Industry: IT, OCEG
  - TwC
  - Example(s)
- Lessons Learned
- Key Takeaways

Brain Teaser

FINISHED FILES ARE THE RESULT OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS.

How Many “F’s” do you see in the above sentence?
Answer in the Appendix of this deck.

Microsoft

Microsoft Mission:
"to create a family of devices and services for individuals and businesses that empower people around the globe at home, at work and on the go, for the activities they value most".

- Founded in 1975
- Corporate headquarters – Redmond, WA (USA)
- Over 100 subsidiaries worldwide
- Over 91,000 employees worldwide
- Core businesses with diverse and distinct focuses

Governance Statement

- *"Long-term thinking guides everything we do to sustain Microsoft's success and create value for shareholders, now and for future. Good corporate governance encourages accountability and transparency, and promotes good decision-making to support our business over decades".*

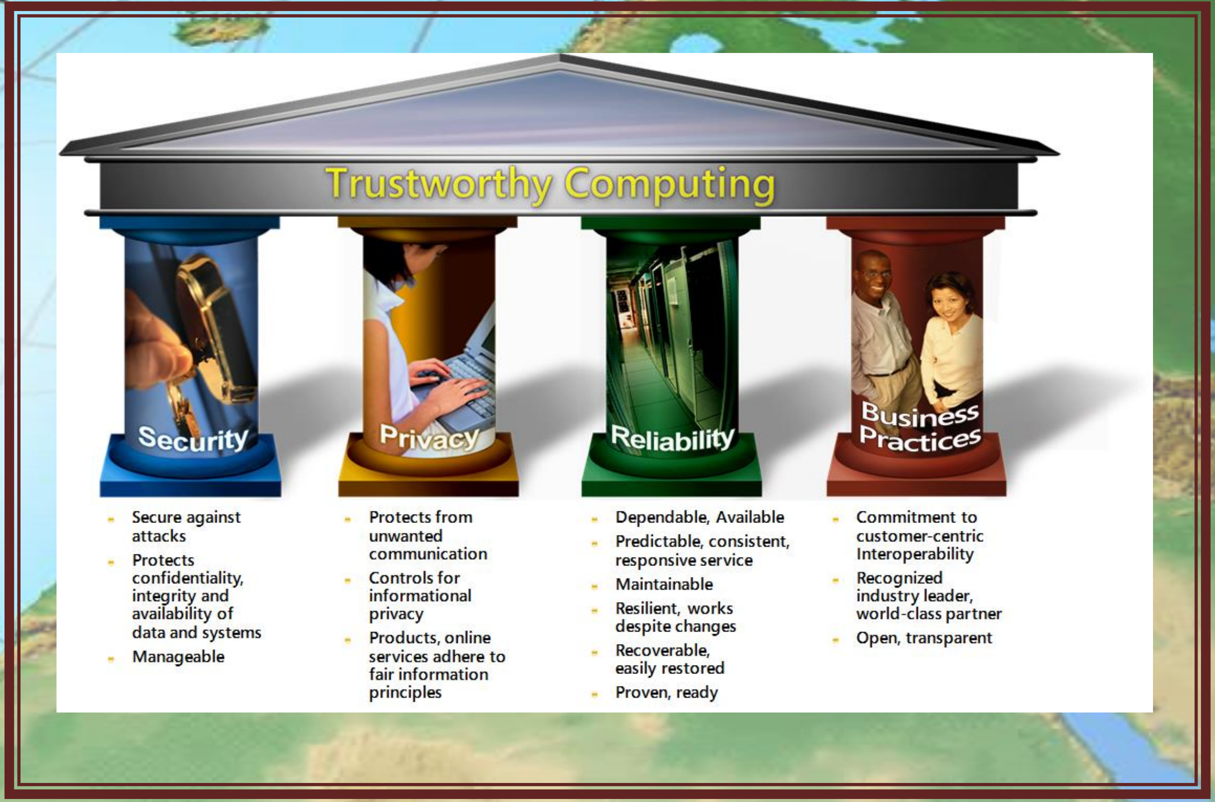
Challenges

- Geography, culture
- Business priorities
- Implementation of enterprise programs

Trustworthy Computing (TwC) Background

2002- Malicious Software

2002- Memo from Bill Gates



Security
- Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable

Privacy
- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

Reliability
- Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready

Business Practices
- Commitment to customer-centric Interoperability
- Recognized industry leader, world-class partner
- Open, transparent

TwC Governance Organization

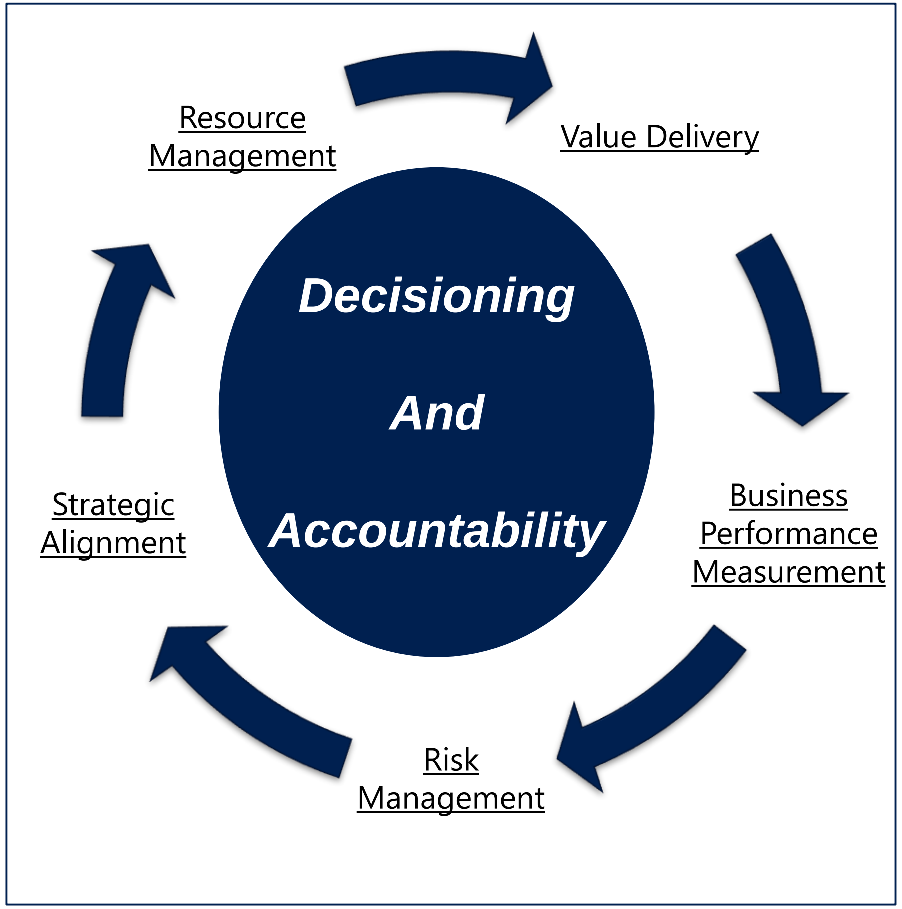
- Privacy
- Accessibility
- Global Readiness
- Online Trust and Safety
- Policy and Compliance Management
- Risk Management
- Unified Incident Response

What Is Governance, GRC, etc….

Industry: Information Systems Audit and Control Association (ISACA)

Resource Management:
Right Skills in the Right place at the Right time

Value delivery:
Delivering expected and agreed upon benefits



Performance Measurement:
Setting measurable targets and progress statements

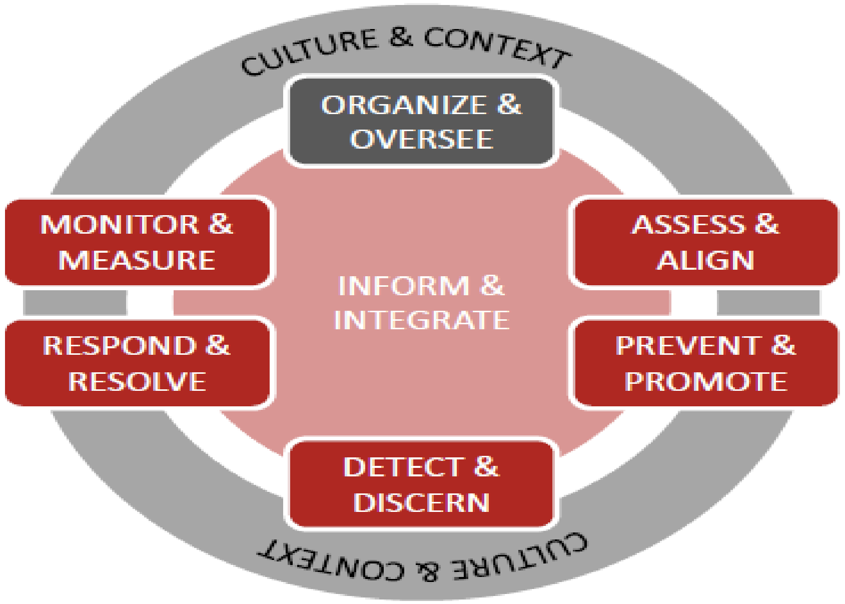
Risk management:
Framework to identify, monitor and manage risk

Strategic alignment:
Aligning strategy to the business for success

The decision rights and accountability framework for encouraging desirable behavior in the use of IT.

Industry: Open Compliance and Ethics Group (OCEG)- GRC

8 INTEGRATED COMPONENTS

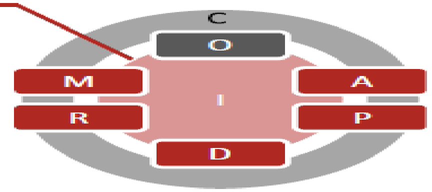


MONITOR & MEASURE
M1 — Context Monitoring
M2 — Performance Monitoring
M3 — Systemic Improvement
M4 — Audit & Assurance

INFORM & INTEGRATE
I1 — Info Management & Documentation
I2 — Internal & External Communication
I3 — Technology & Infrastructure

RESPOND & RESOLVE
R1 — Internal Review & Investigation
R2 — Third-Party Inquiry &Investigation
R3 — Corrective Controls
R4 — Crisis Response & Recovery
R5 — Remediation & Discipline

CONTEXT & CULTURE
C1 — External Business Context
C2 — Internal Business Context
C3 — Organizational Culture
C4 — Values & Objectives



DETECT & DISCERN
D1 — Hotline & Notification
D2 — Inquiry & Survey
D3 — Detective Controls

ORGANIZE & OVERSEE
O1 — Outcomes & Commitment
O2 — Roles & Responsibilities
O3 — Approach & Accountability

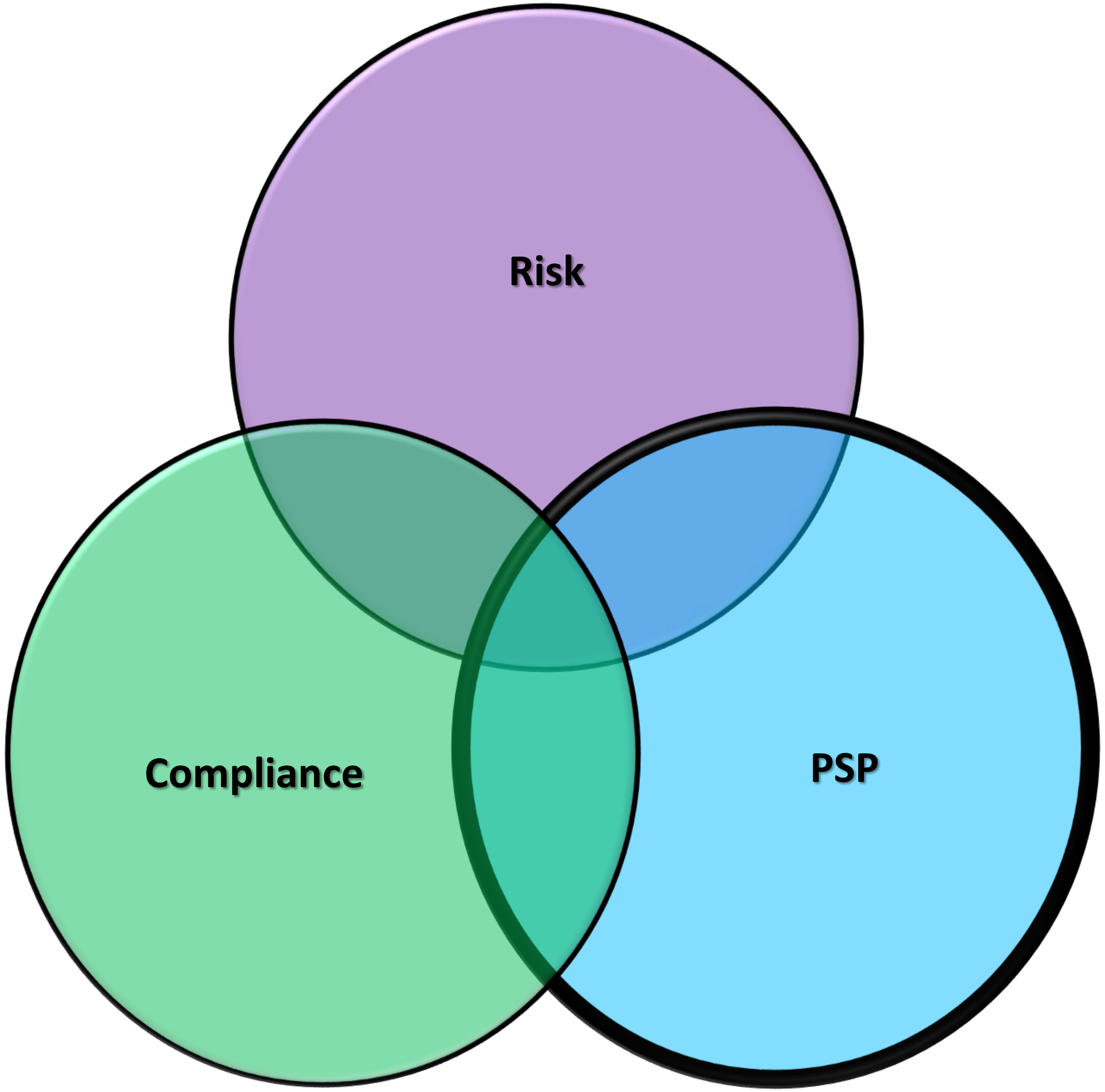
ASSESS & ALIGN
A1 — Risk Identification
A2 — Risk Analysis
A3 — Risk Optimization

PREVENT & PROMOTE
P1 — Codes of Conduct
P2 — Policies
P3 — Preventive Controls
P4 — Awareness & Education
P5 — Human Capital Incentives
P6 — Stakeholder Relations
P7 — Risk Financing & Insurance

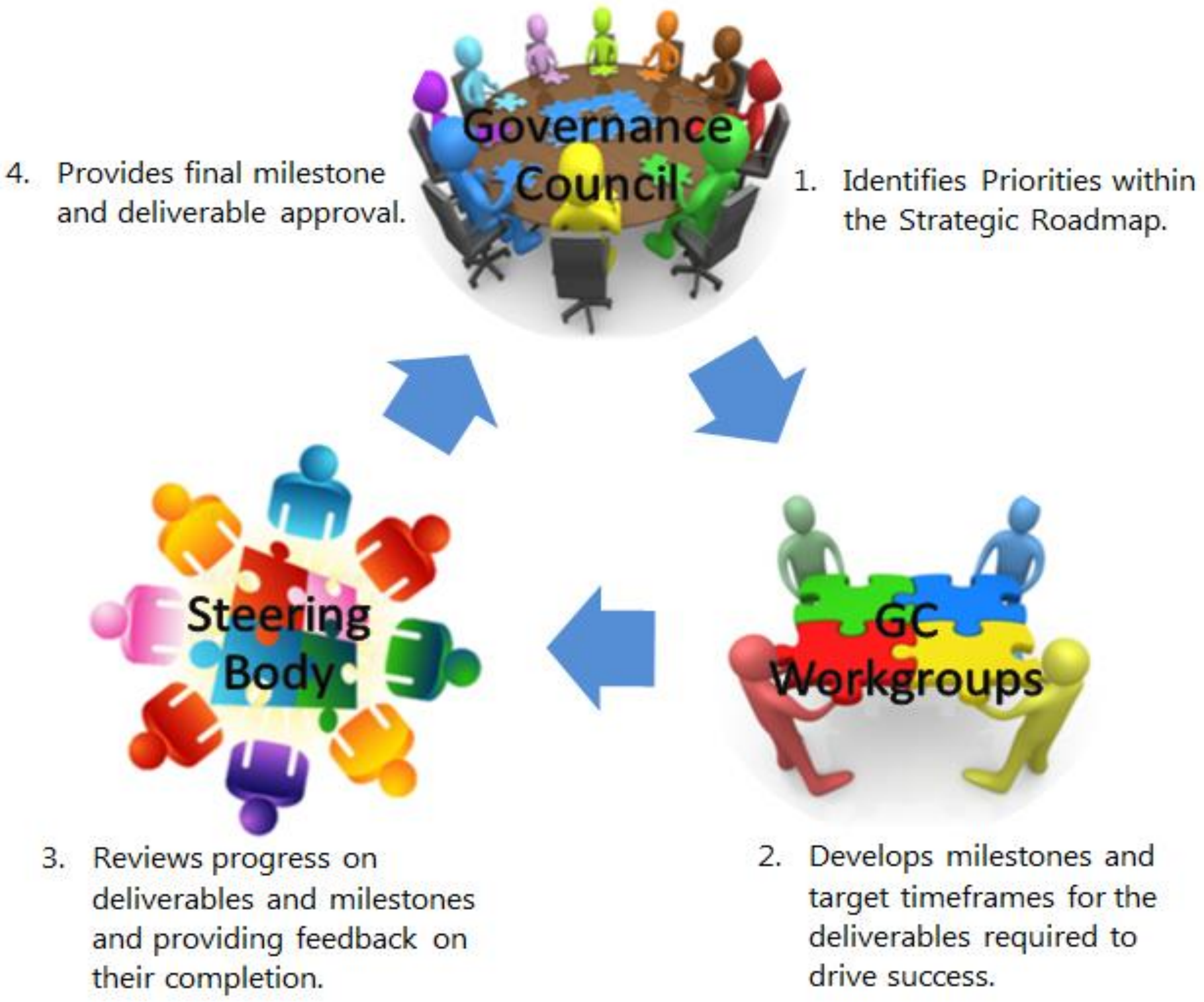
What Drives the Need: Culture, Competition and/or Competitive Advantage, etc….

MS: TwC Governance Function

- ❑ *Policies, Standards and Procedures (PSP)-*
  - ❑ Policy “Why”- A statement of intent from a governing authority that guides business decisions in order to direct an organization's actions in pursuit of long term objectives
  - ❑ *Standard “What”*-A documented requirement, rule, or practice monitored for compliance, and used to direct actions to satisfy the intent of a policy in whole or in part.
  - ❑ *Procedure “How”*- A description of specific steps or a process that, when completed, satisfies in whole or in part one or more Standards.
- ❑ *Risk- **“What** are the Challenges”*
- ❑ *Compliance- **“How** Well are they being managed”*



MS: TwC Governance Function, cont

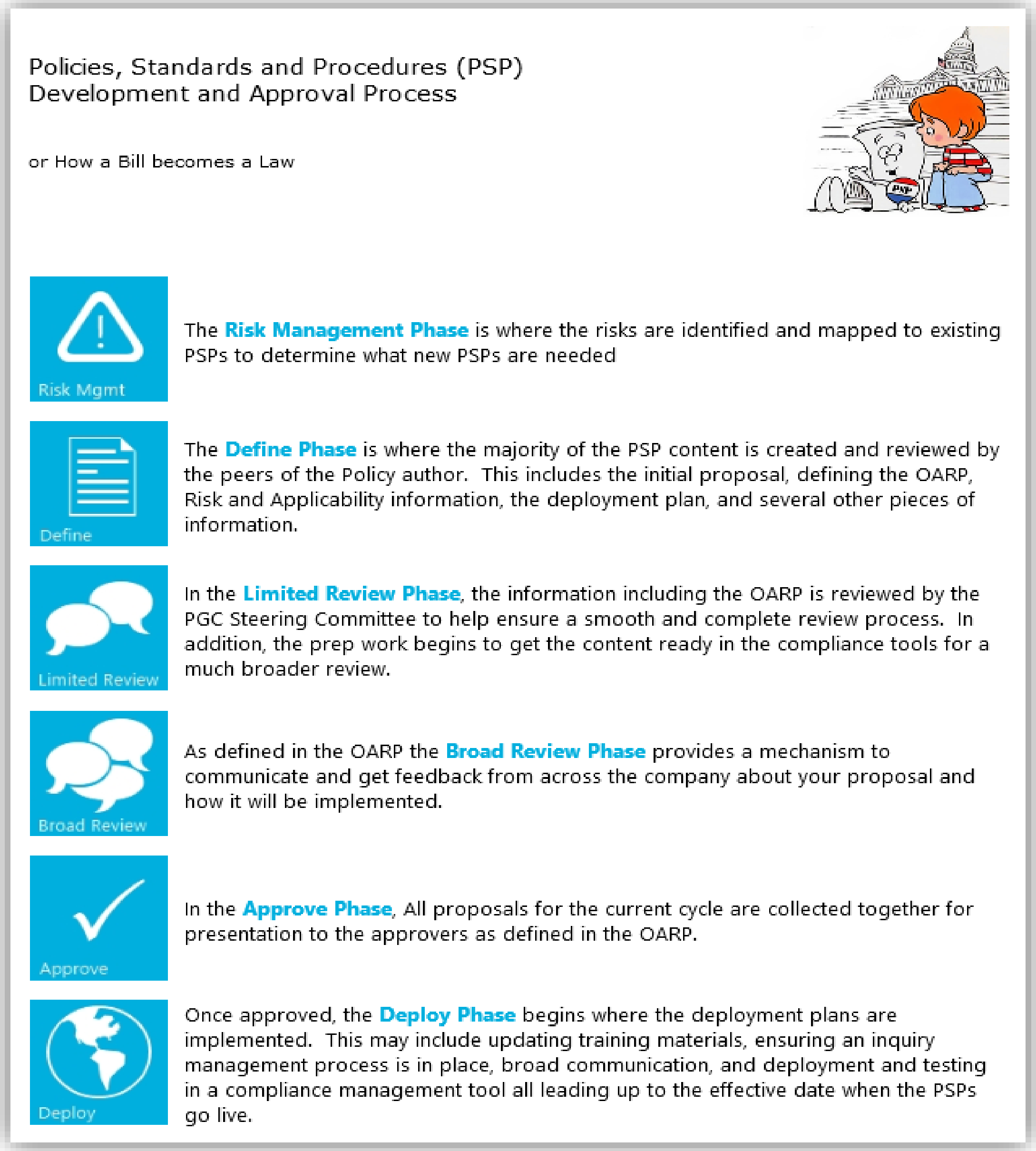


1. Identifies Priorities within the Strategic Roadmap.
2. Develops milestones and target timeframes for the deliverables required to drive success.
3. Reviews progress on deliverables and milestones and providing feedback on their completion.
4. Provides final milestone and deliverable approval.

Partnership: Cross org, collaborative Council leveraging multiple teams' talent to define and make operational an appropriate governance model.

Priorities and Process: Strategic Roadmap Development, Work Group Activities and Steering Body review.

MS: TwC Governance Function, cont



Policies, Standards and Procedures (PSP)
Development and Approval Process

or How a Bill becomes a Law

Risk Mgmt

The **Risk Management Phase** is where the risks are identified and mapped to existing PSPs to determine what new PSPs are needed

Define

The **Define Phase** is where the majority of the PSP content is created and reviewed by the peers of the Policy author. This includes the initial proposal, defining the OARP, Risk and Applicability information, the deployment plan, and several other pieces of information.

Limited Review

In the **Limited Review Phase**, the information including the OARP is reviewed by the PGC Steering Committee to help ensure a smooth and complete review process. In addition, the prep work begins to get the content ready in the compliance tools for a much broader review.

Broad Review

As defined in the OARP the **Broad Review Phase** provides a mechanism to communicate and get feedback from across the company about your proposal and how it will be implemented.

Approve

In the **Approve Phase**, All proposals for the current cycle are collected together for presentation to the approvers as defined in the OARP.

Deploy

Once approved, the **Deploy Phase** begins where the deployment plans are implemented. This may include updating training materials, ensuring an inquiry management process is in place, broad communication, and deployment and testing in a compliance management tool all leading up to the effective date when the PSPs go live.

Note: Compliance and Sustain Phases also included

Examples

Business Continuity Laws, Regulations and Standards

Pre-9/11

Consumer Credit Protection Act
OMB Circular A-130
FEMA Guidance Document
Paperwork Reduction Act
ISO 27002 (Previously ISO17799)
FFIEC BCP Handbook
Computer Security Act
12 CFR Part 18
Presidential Decision Directive 67
FDA Guidance on Computerized Systems
used in Clinical Trials
ANSI/NFPA Standard 1600
Turnbull Report (UK)
ANAO Best Practice Guide (Australia)
SEC Rule 17 a-4
FEMA FPC 65
CAR
JHACO
NFPA:2007

Post-9/11

Sarbanes-Oxley Act of 2002
HIPAA, Final Security Rule
FFIEC BCP Handbook -2003/ 2008
Fair Credit Reporting Act
NASD Rule 3510
NERC Security Guidelines
FERC Security Standards
NAIC Standard on BCP
NIST Contingency Planning Guide
FRB-OCC-SEC Guidelines for
Strengthening the Resilience of US
Financial System
NYSE Rule 446
California SB 1386
Australia Standards BCM Handbook
GAO Potential Terrorist Attacks
Guideline
Federal and Legislative BC
Requirements for IRS
Basel Capital Accord
MAS Proposed BCP Guidelines (Singapore)
NFA Compliance Rule 2-38
FSA Handbook (UK)
BCI Standard, PAS 56 (UK)
Civil Contingencies Bill (UK)%

Sarbanes-Oxley
2002 Safety Act
FCD-1/2
NYS Circular Letter 7
ASIS
State of NY FIRM White Paper on CP
NISCC Good Practices (Telecomm)
Australian Prudential Standard on BCM
HB221
HB292
BS25999
SS507 – SS540
TR19
CA Z1600
ISO/PAS 22399
HiTech Act of 2009
NZ 5050
ISO22301
FINRA 4370
SEC - Compliance Programs
Dodd-Frank Wall Street Reform Act
ISO22301
NFPA:2010-2013

DRI International 10pp

Title IX – 110-53

1991-2001

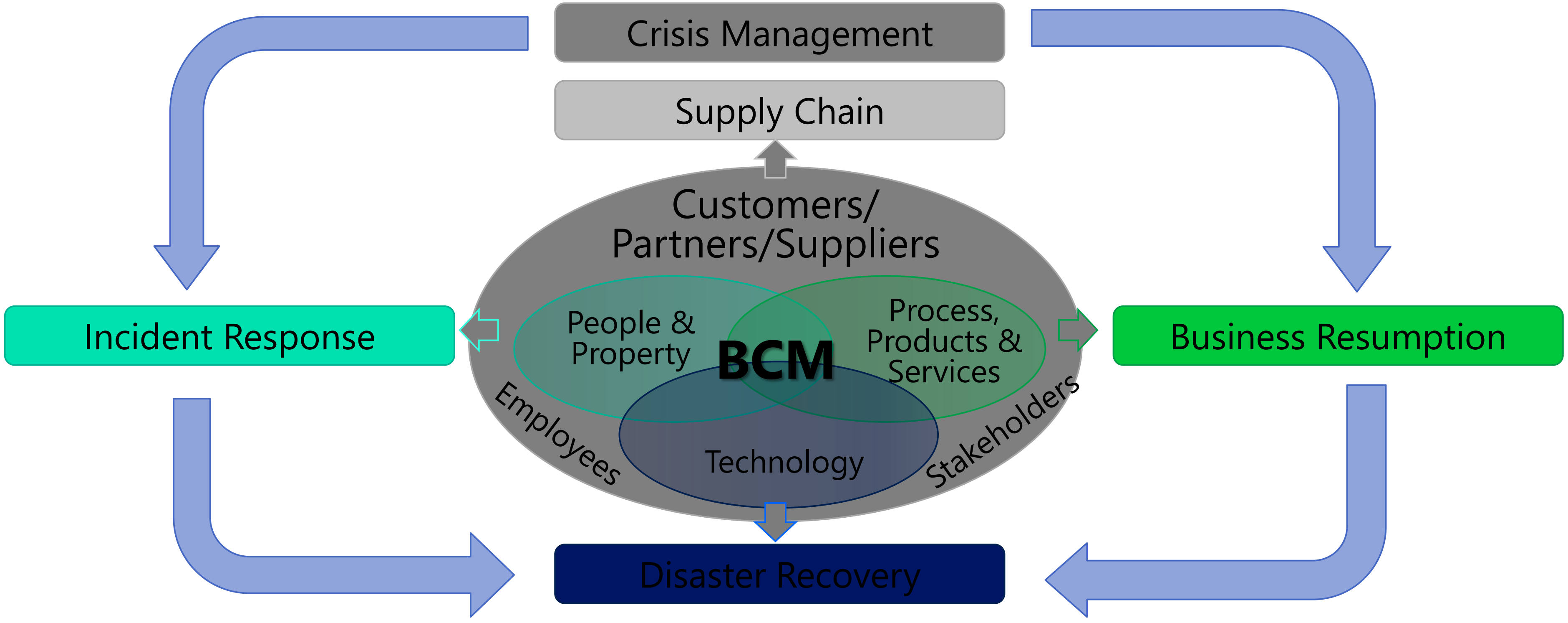
2002-2013

- Information above leveraged from the DRII communicated deck.
- Additional insights on Disaster Recovery journal site here.

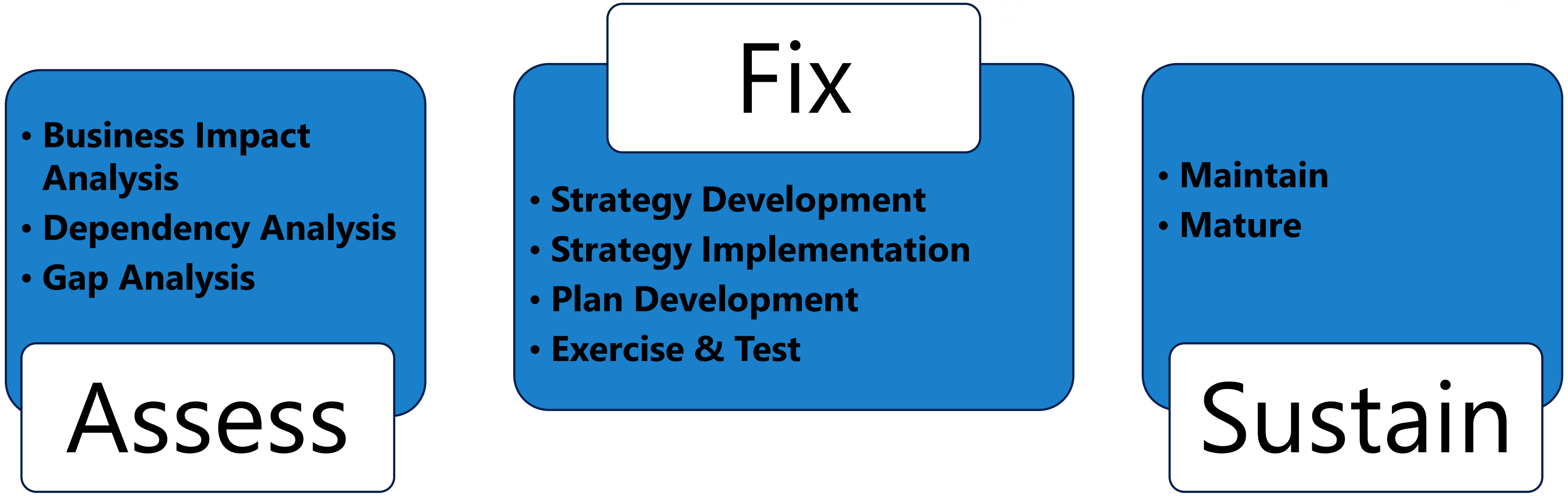
Business Continuity, Disaster Recovery, Incident Response

Enterprise Risk Management (ERM) ← **Governance**

Compliance → **Internal Audit**



Business Continuity, Disaster Recovery, Incident Response



Assess

- **Business Impact Analysis**
- **Dependency Analysis**
- **Gap Analysis**

Fix

- **Strategy Development**
- **Strategy Implementation**
- **Plan Development**
- **Exercise & Test**

Sustain

- **Maintain**
- **Mature**

Key Characteristics

- Common taxonomy enhances enterprise wide decision making and reporting
- Layered Approach – Rank processes to align activity/resources with the greater operational risk

Business Continuity, Disaster Recovery, Incident Response

Today's Challenges	Best Practices
Business Unit Engagement	• Top down sponsorship • Standards based methodology • Enterprise wide scorecard
Program Scalability	• Embed BCM professionals in key business units • Prioritize activity • Use familiar tools (Microsoft Office, SharePoint)
Program vs. Project Mentality	• Integrate BCM into company culture • Develop relationships with key stakeholder groups • Provide business unit participation opportunities in governance and critical decisions

Culture- MS Corporate Vulnerability and Disclosure

- Appropriately engaging Community in identification of vulnerabilities.

"We want to make it more costly and difficult for criminals to exploit vulnerabilities,"… "We want to inspire researchers to focus their expertise on defensive security technologies". Katie Moussouris- MS Security Research Center

Lessons Learned

Worked Well

1. Buy-in and Visible Sponsorship as noted through Charter sign-off, Policy Governance Council engagement, etc…
2. Working Group Development to drive action on key strategic roadmap items across TwC and the Business Units. Acknowledgement that Risk Management is the common thread that needs to be consistently applied.
3. Leveraging existing work and process vs. building brand new and not acknowledging those that "had come before".

Challenges

1. Driving change across a Global organization
2. Taxonomy Differences

Looking Back….

1. Do early research and acknowledge existing GRC Community- cosponsor knowledge transfer sessions and Industry best practices Bootcamps (example: www.oceg.org)
2. Identify existing taxonomy challenges early- work to find the commonalities and begin efforts to agree and/or document differences early on
3. Clearly identify and document roles and responsibilities as a first step.
4. Exception Handling Process- Gain agreement and document early on

Key Takeaways

- ❑ Agreed Upon Governance Model
- ❑ Method to Implement the Model
- ❑ Leverage and Celebrate Successful areas/Proven practices
- ❑ Transparency, Transparency, Transparency…

Thank you!

❑ Michele Turner (michelet@microsoft.com)

Appendix

Brain Teaser- Answer:

There are six F's in the sentence. Many people forget the OFs. The human brain tends to see them as "V's" or the acronym “vs.” instead of "F's” or “ofs".

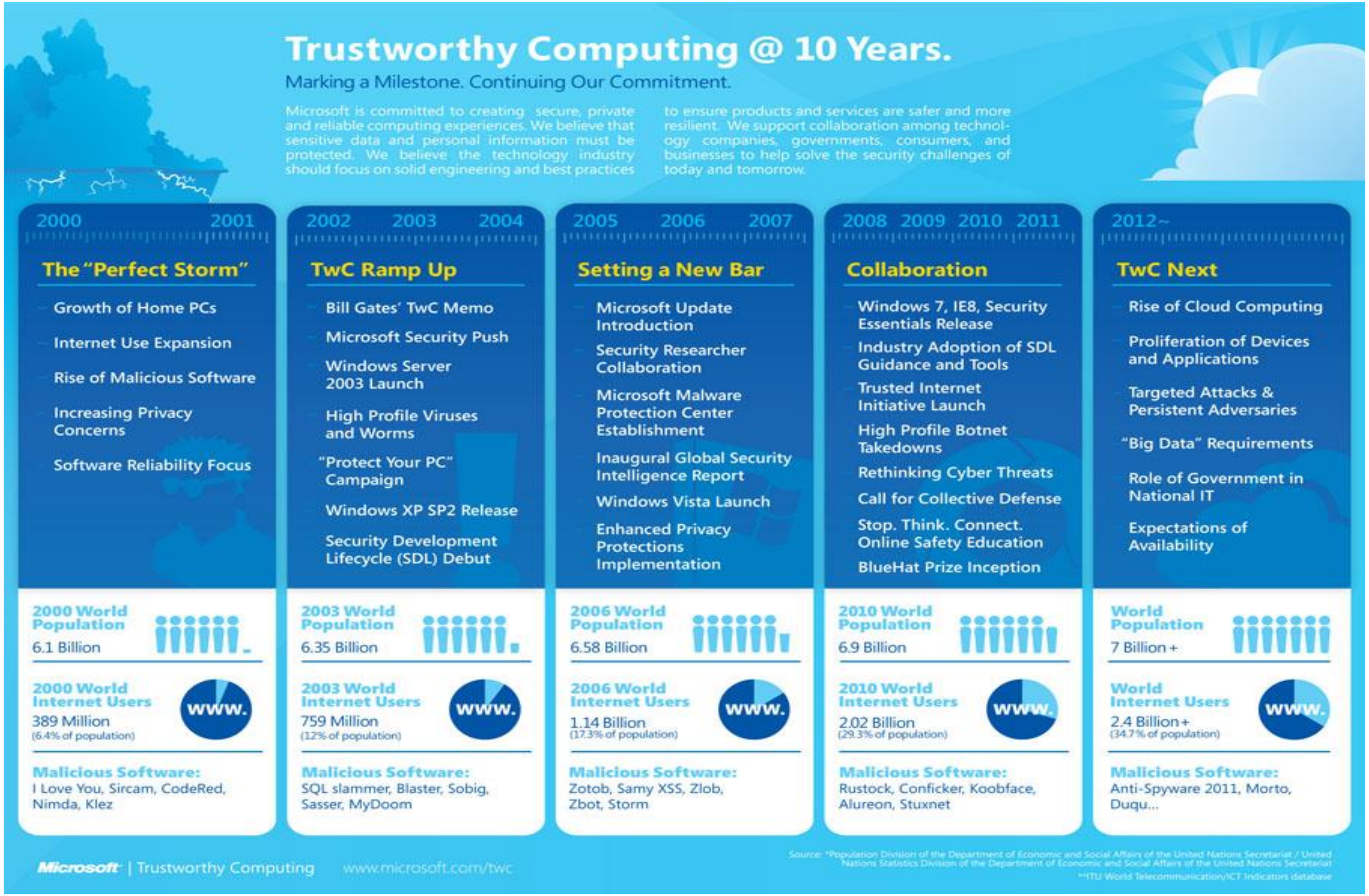
- At times, especially in Governance, we are so focused on one aspect, that we have tunnel vision and cannot see the others.
- For subject matter experts in risk, leverage your partners expertise in policy or compliance, to broaden your understanding and clear the spots that you may overlook. The same is true for those in policy and compliance in leveraging risk.
- Governance is about decisioning and accountability, all working together to complete the story ☺.

TwC- PSP “Story”

- ❑ ***Policy-*** Think of the policy as saying, “At Microsoft, we will Jump”. The reason we will jump is because we want to demonstrate our dedication to the principles of flexibility, athletic talent and prowess, and because we know our customers will not buy products from companies unless they jump.

- ❑ ***Standard-*** The related standards outline how high we must jump, how often we will jump, and whom must jump to demonstrate our enthusiastic dedication to the principles of flexibility, athletic prowess, and delighting our customers with jumps.”

- ❑ ***Procedure-*** The procedures derived from the standards tell us from what point we must jump, how and who will be measuring our jumps, what shoes we may wear, and whether our jumps are actually jumps vs hops, which are not allowed.



www.
www.
www.
www.
www.

Trustworthy Computing @ 10 Years.

Marking a Milestone. Continuing Our Commitment.

Microsoft is committed to creating secure, private and reliable computing experiences. We believe that sensitive data and personal information must be protected. We believe the technology industry should focus on solid engineering and best practices to ensure products and services are safer and more resilient. We support collaboration among technology companies, governments, consumers, and businesses to help solve the security challenges of today and tomorrow.

2000 2001

The "Perfect Storm"

- Growth of Home PCs
- Internet Use Expansion
- Rise of Malicious Software
- Increasing Privacy Concerns
- Software Reliability Focus

2000 World Population
6.1 Billion

2000 World Internet Users
389 Million
(6.4% of population)

Malicious Software:
I Love You, Sircam, CodeRed, Nimda, Klez

2002 2003 2004

TwC Ramp Up

- Bill Gates' TwC Memo
- Microsoft Security Push
- Windows Server 2003 Launch
- High Profile Viruses and Worms
- "Protect Your PC" Campaign
- Windows XP SP2 Release
- Security Development Lifecycle (SDL) Debut

2003 World Population
6.35 Billion

2003 World Internet Users
759 Million
(12% of population)

Malicious Software:
SQL slammer, Blaster, Sobig, Sasser, MyDoom

2005 2006 2007

Setting a New Bar

- Microsoft Update Introduction
- Security Researcher Collaboration
- Microsoft Malware Protection Center Establishment
- Inaugural Global Security Intelligence Report
- Windows Vista Launch
- Enhanced Privacy Protections Implementation

2006 World Population
6.58 Billion

2006 World Internet Users
1.14 Billion
(17.3% of population)

Malicious Software:
Zotob, Samy XSS, Zlob, Zbot, Storm

2008 2009 2010 2011

Collaboration

- Windows 7, IE8, Security Essentials Release
- Industry Adoption of SDL Guidance and Tools
- Trusted Internet Initiative Launch
- High Profile Botnet Takedowns
- Rethinking Cyber Threats
- Call for Collective Defense
- Stop. Think. Connect. Online Safety Education
- BlueHat Prize Inception

2010 World Population
6.9 Billion

2010 World Internet Users
2.02 Billion
(29.3% of population)

Malicious Software:
Rustock, Conficker, Koobface, Alureon, Stuxnet

2012~

TwC Next

- Rise of Cloud Computing
- Proliferation of Devices and Applications
- Targeted Attacks & Persistent Adversaries
- "Big Data" Requirements
- Role of Government in National IT
- Expectations of Availability

World Population
7 Billion +

World Internet Users
2.4 Billion +
(34.7% of population)

Malicious Software:
Anti-Spyware 2011, Morto, Duqu...

Microsoft | Trustworthy Computing www.microsoft.com/twc

Source: *Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat / United Nations Statistics Division of the Department of Economic and Social Affairs of the United Nations Secretariat
**ITU World Telecommunication/ICT Indicators database

Microsoft