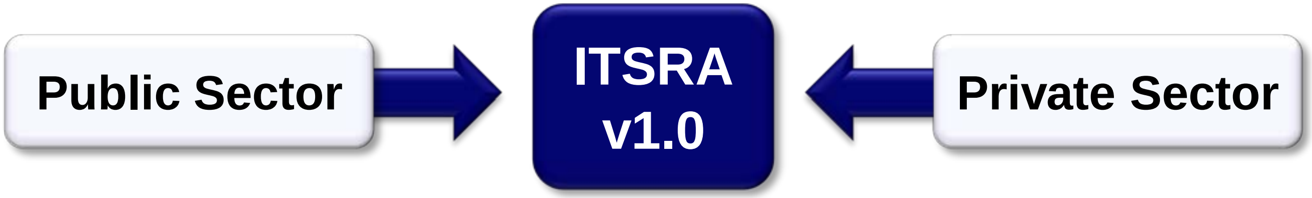
Information Technology Sector Baseline Risk Assessment

June 2010

Jerry Cochran
Principal Security Strategist
Trustworthy Computing
Microsoft Corporation

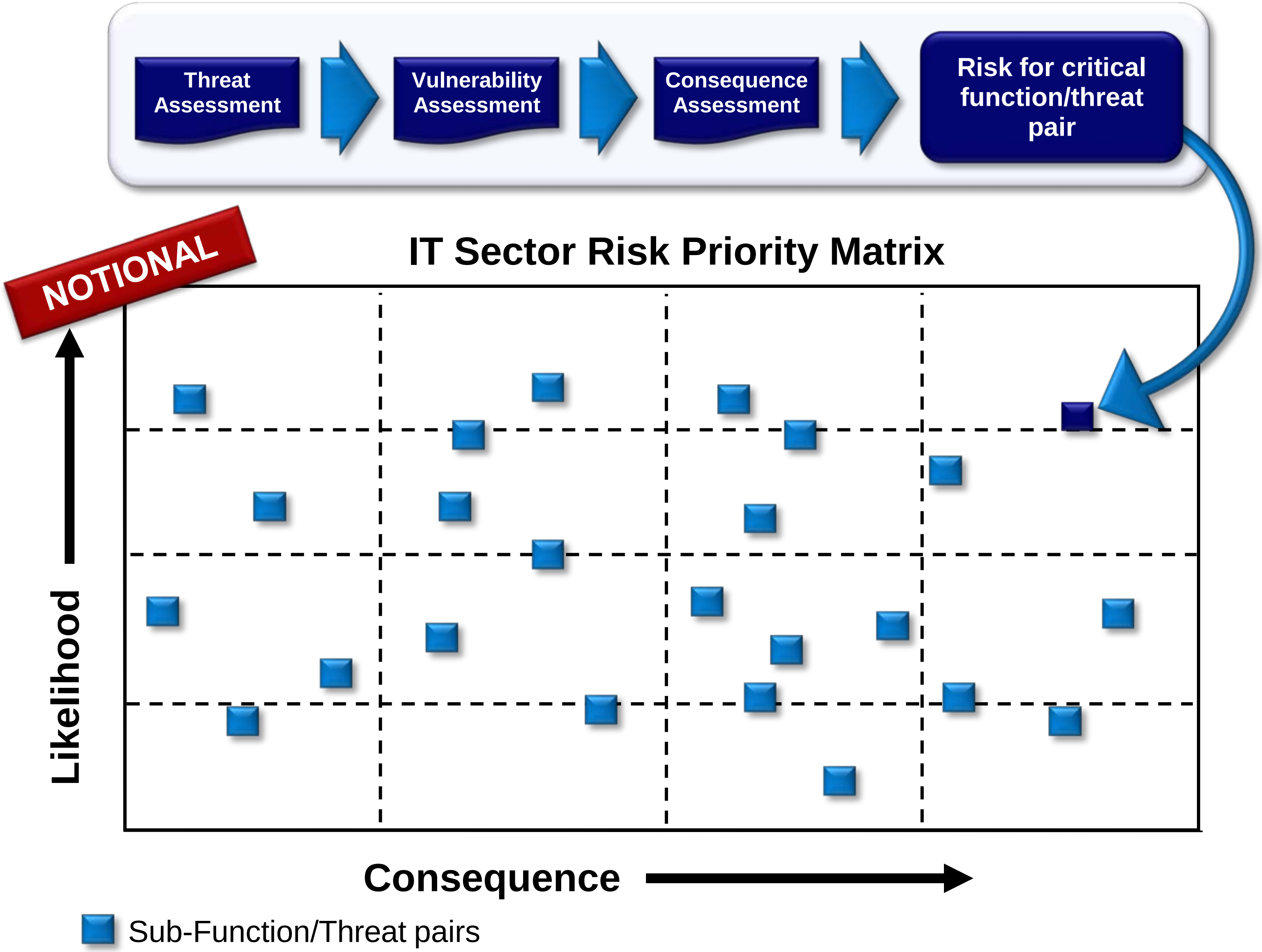
Scott Algeier
Executive Director
Information Technology - Information Sharing and Analysis Center (IT-ISAC)

IT Sector Baseline Risk Assessment (ITSRA v1.0)



- Completed in Dec 2009, result of an 18-month effort
- First-ever national-level sector risk assessment
- Attack-tree focused, all hazards methodology
- Subject matter experts from each “critical function”
- Results now driving national-level risk management policy development
  - National Infrastructure Protection Plan (NIPP)
  - IT Sector-Specific Plan (SSP)

Output: Prioritized IT Sector Risks



Threat Assessment

Vulnerability Assessment

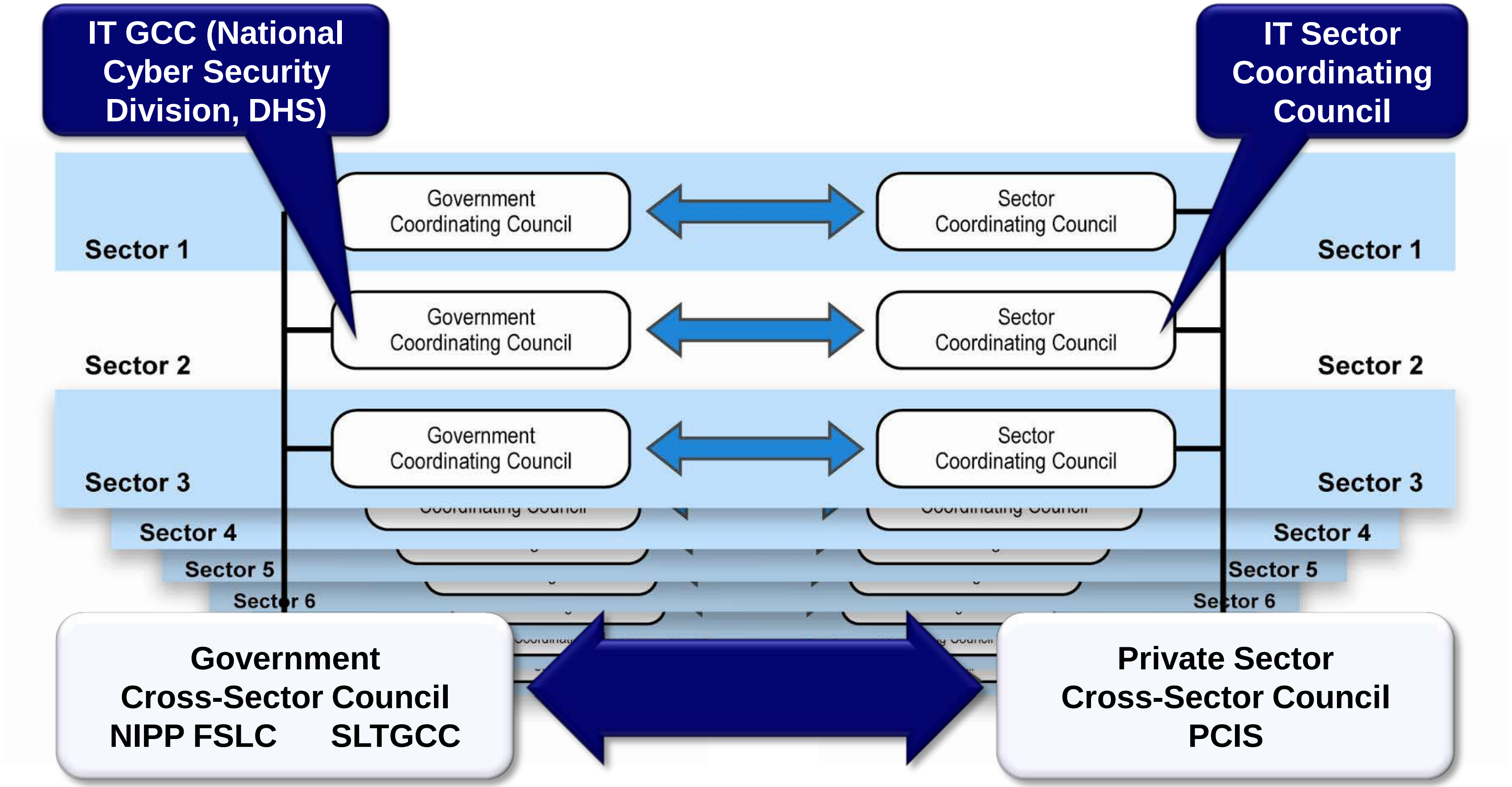
Consequence Assessment

Risk for critical function/threat pair

IT Sector Risk Priority Matrix

NIPP Partnership Framework

Critical Infrastructure Partnership Advisory Council (CIPAC)



IT GCC (National Cyber Security Division, DHS)

IT Sector Coordinating Council

Sector 1
Government Coordinating Council
Sector Coordinating Council
Sector 1
Sector 2
Government Coordinating Council
Sector Coordinating Council
Sector 2
Sector 3
Government Coordinating Council
Sector Coordinating Council
Sector 3
Sector 4
Sector 4
Sector 5
Sector 5
Sector 6
Sector 6

Government Cross-Sector Council
NIPP FSLC SLTGCC

Private Sector Cross-Sector Council
PCIS

The scope of the IT Sector's approach analyzes risk to the critical IT Sector functions…

Produce and provide IT products and services

Provide incident management capabilities

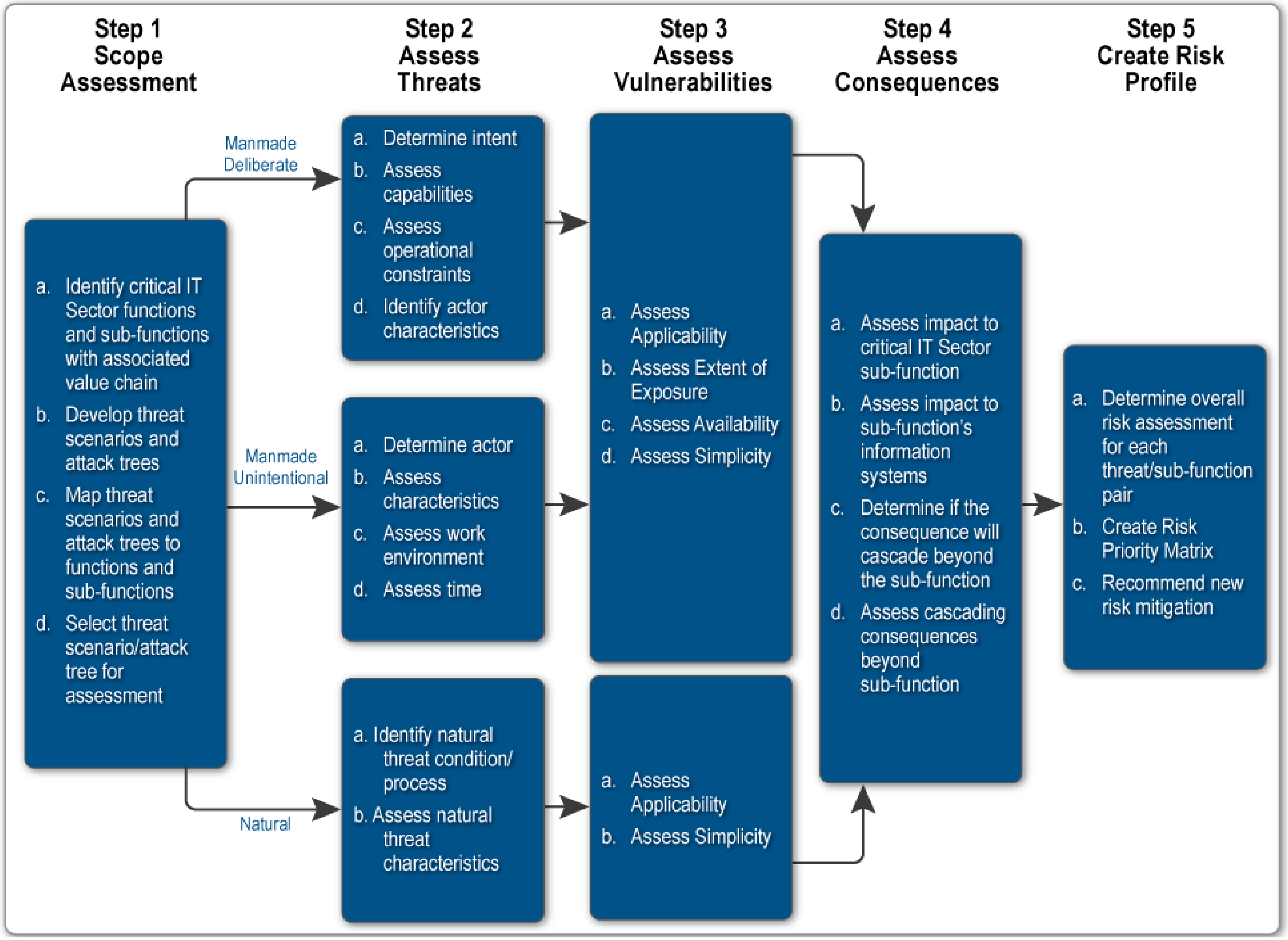
Provide domain name resolution services

Provide identity management and associated trust support services

Provide Internet-based content, information, and communications services

Provide Internet routing, access, and connection services

Risk Assessment Methodology



Step 1 Scope Assessment

a. Identify critical IT Sector functions and sub-functions with associated value chain
b. Develop threat scenarios and attack trees
c. Map threat scenarios and attack trees to functions and sub-functions
d. Select threat scenario/attack tree for assessment

Step 2 Assess Threats

Manmade Deliberate

a. Determine intent
b. Assess capabilities
c. Assess operational constraints
d. Identify actor characteristics

Manmade Unintentional

a. Determine actor
b. Assess characteristics
c. Assess work environment
d. Assess time

Natural

a. Identify natural threat condition/ process
b. Assess natural threat characteristics

Step 3 Assess Vulnerabilities

a. Assess Applicability
b. Assess Extent of Exposure
c. Assess Availability
d. Assess Simplicity

a. Assess Applicability
b. Assess Simplicity

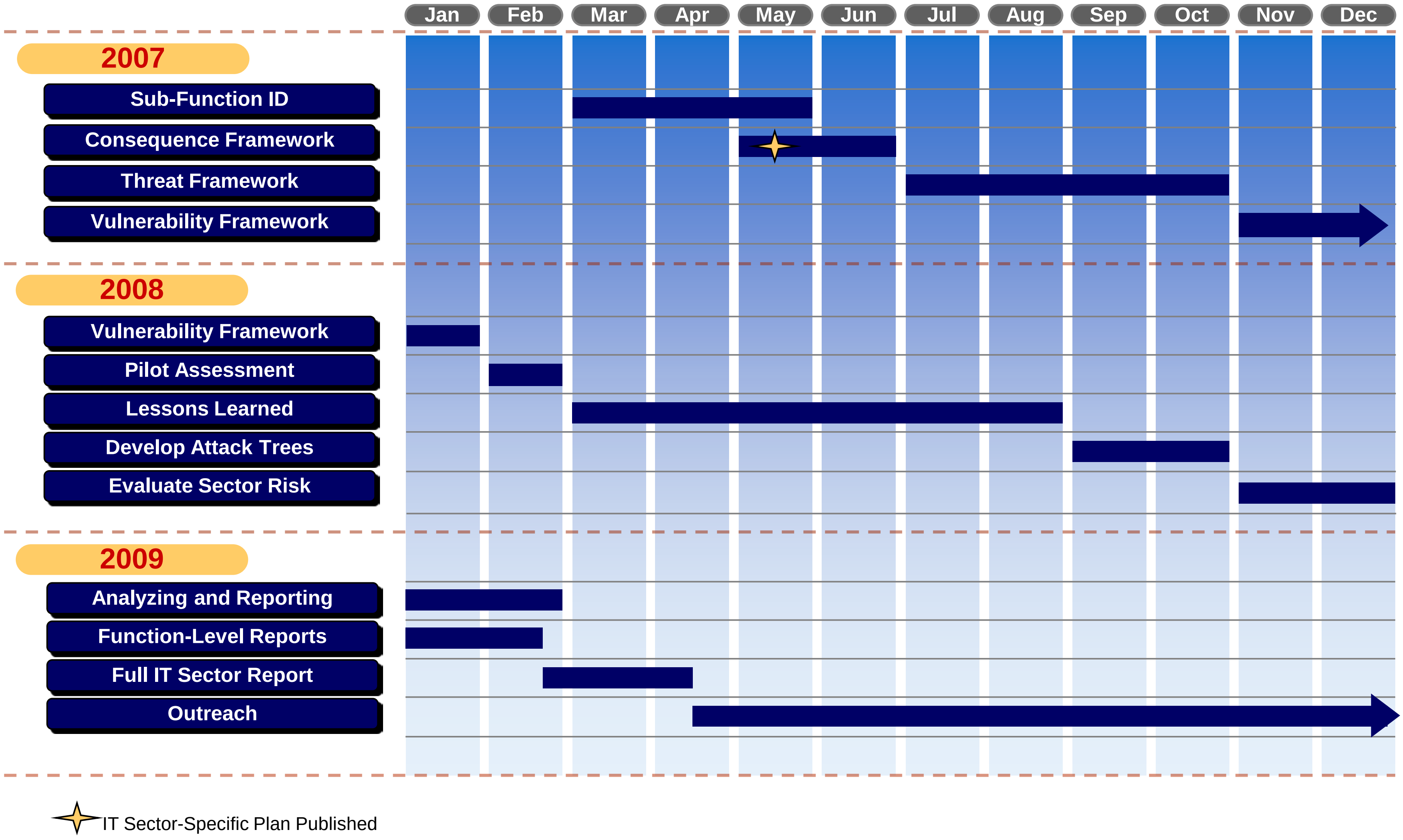
Step 4 Assess Consequences

a. Assess impact to critical IT Sector sub-function
b. Assess impact to sub-function's information systems
c. Determine if the consequence will cascade beyond the sub-function
d. Assess cascading consequences beyond sub-function

Step 5 Create Risk Profile

a. Determine overall risk assessment for each threat/sub-function pair
b. Create Risk Priority Matrix
c. Recommend new risk mitigation

The IT Sector Baseline Risk Assessment was developed in an evolutionary process and a collaborative manner among public and private sector partners



Three key risks were identified as a result of the ITSRA

1

Produce and Provide IT Products and Services

Supply chain risk to hardware, software and services is an integrity issue as well as an availability issue

- Global nature of supply chain means attacks can happen anywhere at any time
- Global nature also provides resiliency
- Corporate quality control processes and procedures also mitigate risks

2

Provide Internet-based Content, Information, and Communications Services

Impacts to the *Provide Internet-based Content, Information, and Communications Services* function are usually symptomatic of threats (manmade or natural) to other parts of the IT Sector infrastructure

- Highly dependent on DNS and Internet Routing functions
- Unintended Border Gateway Protocol (BGP) changes, or improperly updated BGP tables can cause impacts to the availability of Internet content.
- People, process and technology mitigations such as training and terminating access controls for former employees typically minimize the vulnerabilities or limit the consequences associated with successful exploitation.

Three key risks were identified as a result of the ITSRA (continued)

3

Provide Incident Management Capabilities

Attacks against the *Provide Incident Management Capabilities* function could be force multipliers. This effect could increase the consequences of more traditional attacks against the IT Sector by inhibiting an effective response

- Threats typically occur in parallel to attacks on other elements of the IT infrastructure
- For example, attacks against the incident management function could be force multipliers, which could result in more sever impacts to the infrastructure than typical attacks
- Organization- and national-level incident response capabilities typically mitigate the risks associated with threats to this function
- Infrastructure and workforce location diversity results in more resilient incident response capabilities
- Enhanced information sharing processes and mechanisms has also resulted in improved response to incidents

In addition, IT sector partners identified function-specific risks to inform the Sector’s protective program and R&D efforts

IT Sector Function	Risks	Mitigations (Existing, Being Enhanced, or Potential Future)
Produce and Provide IT Products and Services	▪ Global nature of complete supply chain ▪ Integrity and availability of products	▪ Diversity of supply chain ▪ Quality control processes and procedures
Provide Domain Name Resolution Services	▪ Policy and governance failures that result in a decrease in interoperability ▪ Cascading consequences due to failure of Internet Routing function	▪ Provisioning of Anycast ▪ Incorporation of diverse infrastructures ▪ Enhanced quality assurance processes that mitigate risks associates with human error
Provide Internet-based Content, Information, and Communications Services	▪ Dependent on DNS and Internet Routing functions ▪ Unintended Border Gateway Protocol (BGP) changes or improperly updated BGP tables can impacts the availability of Internet content ▪ Disruptions in the DNS function can cascade to the Internet Routing and Internet Content functions	▪ People, process and technology mitigations such as training and terminating access controls for former employees typically minimize the vulnerabilities or limit the consequences associated with successful exploitation. ▪ End Users/customers can also help mitigate

In addition, IT sector partners identified function-specific risks to inform the Sector's protective program and R&D efforts (Continued)

IT Sector Function	Risks	Mitigations (Existing, Being Enhanced, or Potential Future)
Provide Internet Routing, Access and Connection Services	▪ The concentration of physical assets supports a narrow range of physical threats to the function ▪ Threats to BGP and other interdomain router operating systems, and intra-domain protocols are the primary vulnerabilities	▪ Enhanced technologies and processes ▪ Information sharing and communities of practice
Provide Incident Management Capabilities	▪ Threats are varied and typically occur in parallel to attacks on other elements or functions of the IT infrastructure ▪ Depending upon their severity, attacks on IT Sector critical functions have the potential to deny or degrade the Sector's ability to detect, respond to, or recover from an incident	▪ Infrastructure and workforce location diversity results in more resilient incident response capabilities ▪ Integrating lessons learned into future incident response procedures, policies, and prevention activities facilitates continuous improvement and fosters improved prevention and protection practices

Interdependencies across the critical IT Sector functions illustrate the level at which they are integrated

First Order - Exploited Function	Cross-Functional Impact					
	Products & Services	Internet Routing	DNS	Identity Mgmt	Internet Content	Incident Mgmt
Products & Services	X	High	High	High	High	High
Internet Routing	Medium	X	High	High	High	High
DNS	Low	High	X	High	High	Medium → High
Identity Mgmt	Medium → High	Low	Low	X	High	Low → Medium
Internet Content	Medium	Low	Low	Low	X	Medium → High
Incident Mgmt	Low → High	Low → High	Low → High	Low → High	Low → High	X

Highlighted Interdependencies

All functions depend on **Products and Services**

Internet Routing is the most basic function of the internet, thus **DNS** is highly reliant on it

DNS makes **Internet Content** accessible to the average user

Identity Management provides security for **Internet Content**

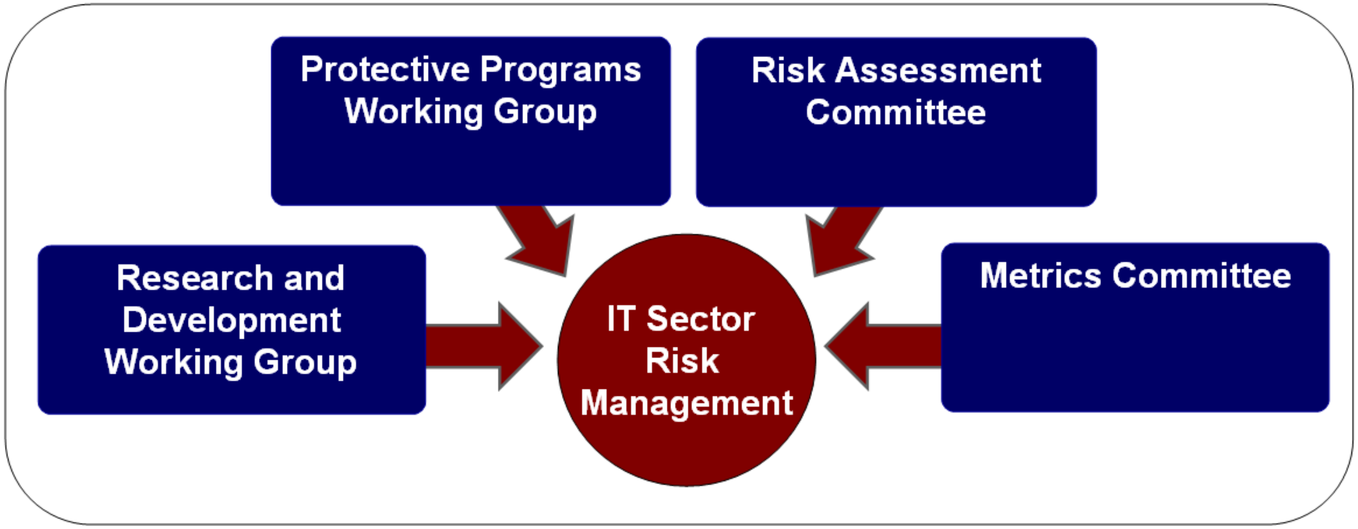
Incident Management relies on **Internet Content** to provide critical communication and collaboration services

All functions rely on **Incident Management** for passive and active risk mitigation

High, Medium, and Low are used to indicate the relative level of dependency across the critical IT Sector functions.

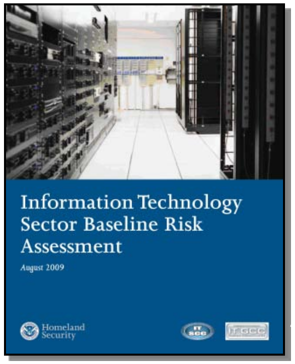
ITSRA will inform the Sector's R&D, protective programs, and metrics activities

- ITSRA identifies key risks that require national-level mitigation
- IT public and private sector partners have established a process for informing risk mitigation activities
- IT Sector will prioritize and refine the risks and mitigations identified in the ITSRA
- Organizations not involved in the ITSRA are welcome to join the risk management process and provide additional expertise


Protective Programs Working Group
Risk Assessment Committee
Research and Development Working Group
IT Sector Risk Management
Metrics Committee

The result of the IT Sector's mitigation efforts will include identification of gaps in R&D and protective programs that are needed to reduce risks identified in the IT Sector Baseline Risk Assessment

Value to industry and government: baseline to determine the security and resiliency of the critical functions



Information Technology Sector Baseline Risk Assessment

August 2009

Homeland Security

National Level

- Prioritizes national level risks to:
  - — Inform R&D resource allocation
  - — Identify, develop, and deploy innovative and flexible protective measures to enhance the security of the critical functions
  - — Creation of outcome based metrics to measure effectiveness of existing and future mitigations
- Provides a new way of thinking about threat actors, vulnerabilities, and risks

Corporate Level

- Provides a baseline for how secure the environment, allowing companies to refine security policies, practices, business continuity, and preparedness planning
- Identifies challenges that private sector participants could help mitigate through development of products and services
- Anchors security measures to a concrete data set that will better support their business operations and be the basis of meaningful infrastructure protection metrics

IT Sector Risk Assessment Version 2.0

- **Use existing, proven methodology to build off of the foundations of the Baseline ITSRA**

- **Leverage the expertise of function specific subject matter experts**

- **Main areas of focus**
  - Identity Management
  - Dependency Analysis (Communications and Electricity)

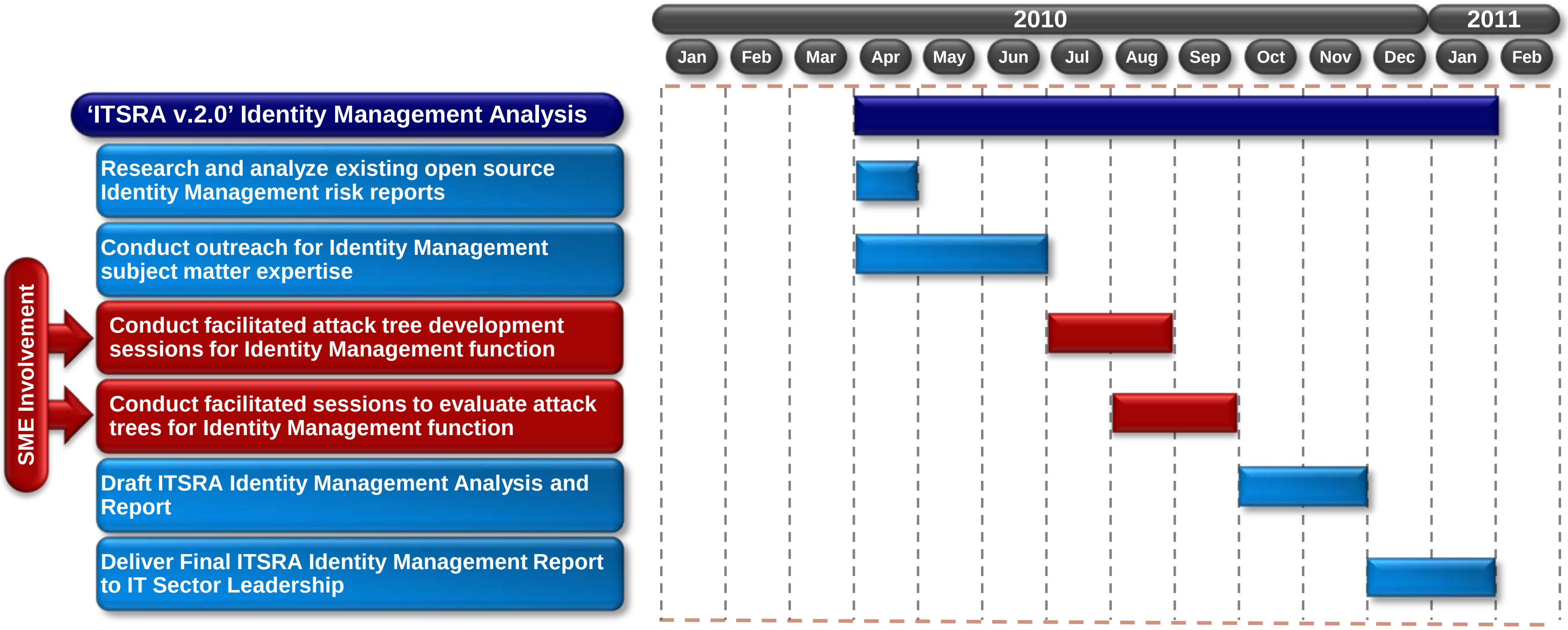
IT public and private sector partners identified dependency and interdependency analysis as an area for further study (1 of 2)

Sector	Example (The ITSRA provides additional details)
Communications	• Share many collocated facilities for switching and routing functions • Dependence on carrier cable networks and satellite communications for delivery and distribution of critical IT functions
Energy	• Require constant electrical power for sustained operation of data centers, production facilities, carrier hotels, and other physical assets • Sustained interruption of electrical power would inevitably cause a denial-of-service
Banking and Finance	• Safe and stable capital and financial markets allow the IT sector to acquire raw materials, maintain workforces, and purchase • Conduct financial transactions and safe capital is required for many of the supply chain dependent processes of IT Sector entities to continue
Chemical	• Provides an array of raw and synthetic materials for use in manufacturing of IT products • Degradation of these materials can a denial-of-service, damage to equipment, or injury to personnel

IT public and private sector partners identified dependency and interdependency analysis as an area for further study (2 of 2)

Sector	Example (The ITSRA provides additional details)
Healthcare and Public Health	• Supports a productive, innovative, and highly-skilled workforce • Protects the workforce from disease and pandemics promoting a healthy lifestyle so workers have limited time out of workforce due to illnesses, especially those that are preventable
Transportation Systems	• Physically transports IT materials and products associated with the supply chain • Supply chain interruptions could result in unreliable or untrustworthy delivery and impacts to the just-in-time-delivery practices
Water	• Provides potable water to operate HVAC systems that keep computer systems cool • Production plants require purified potable water for cogeneration of electricity and steam-driven processes • Sustained loss of water cause equipment shutdown or failure, resulting in a denial-of-service
Federal Government	• Supports the critical IT Sector functions in providing and operating specific root, top level, and lower level domain name servers

Identity Management Analysis Work Plan



‘ITSRA v.2.0’ Identity Management Analysis

Research and analyze existing open source Identity Management risk reports

Conduct outreach for Identity Management subject matter expertise

Conduct facilitated attack tree development sessions for Identity Management function

Conduct facilitated sessions to evaluate attack trees for Identity Management function

Draft ITSRA Identity Management Analysis and Report

Deliver Final ITSRA Identity Management Report to IT Sector Leadership

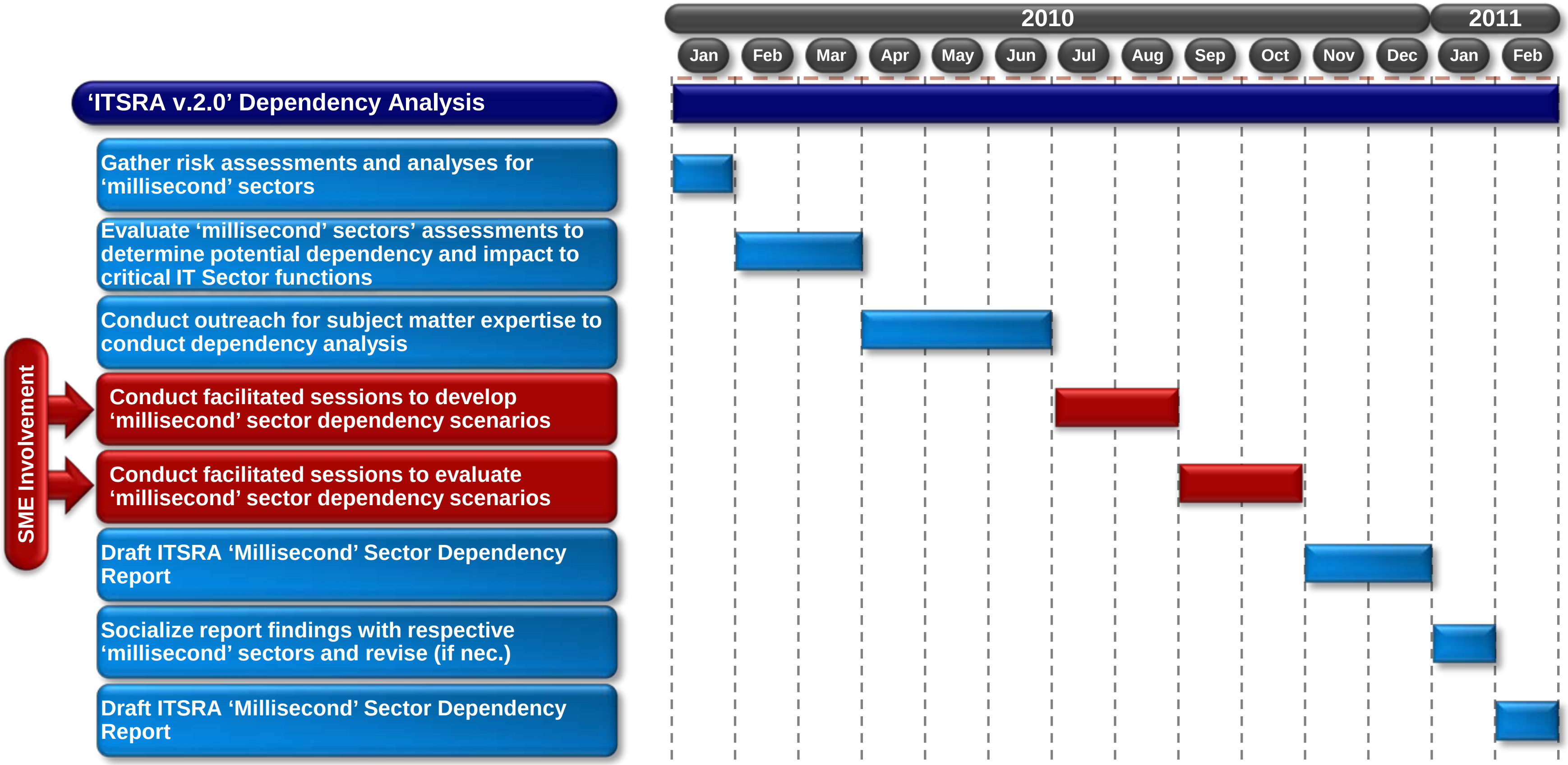
Scope: Shaped primarily by the sub-functions

Goal: Identify threats, vulnerabilities, and consequences to the function and/or its sub-functions

Recruiting: Subject matter experts knowledgeable in operations, policies (to include national level issues), procedures, standards or risks associated with the function and many of its sub-functions

Value Proposition: Inform the Nation’s strategy and planning efforts on identity management

Dependency Analysis Work Plan



‘ITSRA v.2.0’ Dependency Analysis

- Gather risk assessments and analyses for ‘millisecond’ sectors
- Evaluate ‘millisecond’ sectors’ assessments to determine potential dependency and impact to critical IT Sector functions
- Conduct outreach for subject matter expertise to conduct dependency analysis
- Conduct facilitated sessions to develop ‘millisecond’ sector dependency scenarios
- Conduct facilitated sessions to evaluate ‘millisecond’ sector dependency scenarios
- Draft ITSRA ‘Millisecond’ Sector Dependency Report
- Socialize report findings with respective ‘millisecond’ sectors and revise (if nec.)
- Draft ITSRA ‘Millisecond’ Sector Dependency Report

SME Involvement

Scope: Identify how critical IT Sector functions are impacted by disruptions in Communications and Energy

Goal: Determine the impact of disruptions on critical IT Sector functions

Recruiting: Subject matter experts knowledgeable in either:

- The operations, policies (to include national level issues), or risks associated with the critical IT Sector functions and many of its sub-functions; or
- Plausible disruptions in Communications or Energy

Three Ways to Participate

Activity	Description	Estimated Time Commitment
Facilitated Sessions	In person or remote attendance Two sessions per activity identified in the assessment work plan (or more as required)	No longer than 3 hours per session No more than 2 hours to review pre-meeting materials
Review Report Drafts	Synopses of each assessment Length and content determined by participants Facilitators and support team will draft reports in collaboration with participants	No more than 3 to 5 cycles of review Report length 20-40 pages Review times will depend on report length
Outreach and Communications	Voluntary assistance in presenting results Goal: Public documents Outreach/communications materials no longer than 10 pages; include guidance for speakers	No more than 8 hours

Contact Information

Jerry Cochran
Principal Security Strategist
Trustworthy Computing
Microsoft Corporation
Jerry.Cochran@microsoft.com

Scott Algeier
Executive Director
Information Technology Information Sharing and Analysis Center (IT-ISAC)
salgeier@it-isac.org

Timothy Casey
Senior Information Risk Management Analyst
Enterprise Information Security
Intel Corporation
Timothy.p.casey@intel.com