Microsoft
Trustworthy Computing

DRAFT WORKING DOCUMENT

A Framework for Critical Information Infrastructure Risk Management

Global Security Strategy and Diplomacy

Table of Contents

Executive Summary

Critical infrastructures (CIs) play a vital role in today's societies, enabling many of the key functions and services upon which modern nations depend. From financial networks to emergency services, energy generation to water supply, these infrastructures fundamentally impact and continually improve our quality of life.

Particularly vital in this regard are critical information infrastructures (CIIs), those vast and crosscutting networks of information and communications technologies that link and effectively enable the proper functioning of other key infrastructures. In fact, CIIs not only support *all* other critical infrastructures, they also enable the very "information age" at the heart of how modern citizens live, work, and play.

The non-physical—or logical—nature of information infrastructures, however, renders them particularly difficult to protect from potential disruption or attack. As a result, managing risk to critical information infrastructures requires a unique framework to be used to ensure the resiliency of traditional physical infrastructures.

In this guide, Microsoft puts forward a top-down, function-based framework for assessing and managing risk to critical information infrastructures. This framework consists of five sequential steps, described in detail in this guide. Specifically:

- Determining Risk Management Scope
- Identifying Critical Information Infrastructure Functions
- Analyzing Critical Function Value Chain and Interdependencies
- Assessing Critical Function Risk
- Prioritizing and Treating Critical Function Risk

The guide also discusses a key component of each step in this CII risk management framework: strong public-private partnerships among stakeholders. That is, public and private stakeholders must work together to conduct a top-down, function-based risk assessment, jointly identify and implement risk treatment options, and collaboratively monitor and evaluate these risks and treatments on a continuous basis.

Microsoft's Trustworthy Computing group offers this guide to help government and infrastructure stakeholders advance CII resiliency and security globally. We welcome comments, thoughts and suggestions on this evolving resource.

For more information about Microsoft's approach to critical infrastructure protection and its Global Security Strategy and Diplomacy team, visit http://www.microsoft.com/twc or contact cipteam@microsoft.com.

Introduction

Critical infrastructures (CIs) provide essential services that enable modern societies and economies, making their protection an important national and international policy concern. The complexity, interconnectedness and interdependency of these infrastructures only amplify those concerns.

Critical infrastructures—including energy, communications and banking networks, public health and safety mechanisms, and national security—are typically an aggregate of functions provided by a wide range of stakeholders. While CIs are generally privately owned and operated, governments, technology vendors, and service providers all have important roles in ensuring the smooth and reliable functioning of CIs. Managing risks to these infrastructures, as a result, is a shared responsibility, and one that requires close and sustained collaboration among stakeholders.

Critical Infrastructure Protection (CIP) is not an end state, but a continuum. It is an ongoing process of activities that draws upon the shared expertise of all the collaborating stakeholders. This form of close cooperation is particularly important when it comes to highly diffuse and interconnected **critical information infrastructures (CIIs)**—those crosscutting networks of **information and communications technologies (ICTs)** that support, link, and enable other critical infrastructures.

Critical information infrastructures (CIIs) are crosscutting networks of information and communications technologies **(ICTs)** that collectively support, link and enable other critical infrastructures.

Critical infrastructure protection (CIP) is a continuous set of risk management and operational response activities aimed at improving the security and resiliency of **critical infrastructures.** These are infrastructures that support essential services, public health and safety, the economy, and national security.

In contrast to physical critical infrastructure assets, such as buildings, dams, or power plants, critical information infrastructures are virtual, or "logical" in nature. That is, they are comprised of complex, widely scattered systems of software, hardware, and services working together to produce a desired outcome. For example, when a consumer conducts an online search using Bing, he is, in fact, accessing a wide array of independent, far-flung computer networks that together collect, organize, and disseminate the results of his search. The location of these networks is irrelevant to the consumer; what is important to him is the outcome of his search. The same is true for any number of important ICT functions regularly utilized by businesses, governments, and individuals.

Because of this highly diffuse nature of computer networks, managing risk to ICT-based infrastructures is fundamentally different from managing risk to traditional physical infrastructures. A framework specifically geared to the unique, virtual nature of critical information infrastructures is not only recommended, but also fundamental.

Microsoft has a broad history of experience in helping to manage risks to critical information infrastructures. In 2002, Microsoft established Trustworthy Computing as a top company priority. Microsoft's Trustworthy Computing group works closely with governments, infrastructure owners and operators, and technology vendors to understand and mitigate emergent risks to critical infrastructures.

This document provides readers with a detailed discussion of Microsoft's Critical Information Infrastructure Risk Management Framework. It leverages Microsoft's substantial experience working with governments and industries on risk assessment strategies that account for the unique characteristics of ICTs.

This strategic framework can be used to focus on the national, regional or sectoral levels. It is designed to complement and work alongside traditional organizational risk management frameworks, practices and standards. Microsoft's Trustworthy Computing group invites discussion and further collaboration on this framework, with the goal of continually improving and enhancing this resource for critical infrastructure protection efforts globally.

The Structure of this Guide

This resource is presented in three sections:

- **CIP Principles:** Provides a top-line overview of the principles commonly shared by effective critical infrastructure protection. That is, the guiding philosophy that forms the basis for successful efforts to improve resiliency, regardless of the critical infrastructure in question.
- **Risk Management Fundamentals:** Provides a primer on the core concepts of risk management.
- **Microsoft's Framework:** Provides a step-by-step guide to Microsoft's framework for CII risk management, including the tools needed for stakeholders looking to develop their own CII risk management processes, from conception to execution.

Key Principles for Critical Infrastructure Protection

Experience has shown that effective critical infrastructure protection efforts share key central principles: **trustworthy plans and policies; resilient operations; and investments in innovation**. And importantly, all of these principles are linked together by the existence of **trusted collaboration** and **information sharing.**

Figure 1 – The Microsoft Critical Infrastructure Protection Continuum

Trustworthy Plans and Policies

A central principle of effective CI protection is the need to **create and sustain trustworthy policies and plans** that guide and inform stakeholders' work across the full spectrum of critical infrastructure protection activities, including risk management. In order to be trustworthy, policies and plans must be **collaborative, flexible, and measurable.** That is, they must:

- **Build and reinforce strong, cooperative partnerships** among stakeholders;
- **Be adaptable and scalable**, responding to ongoing changes in threat profiles; and
- **Contain milestones and metrics** that track the progress of a CI protection program.

In essence, trustworthy policies and plans articulate stakeholders' priorities and guide subsequent CIP activities in adherence to those priorities. Not surprisingly, then, these policies and plans are not developed by happenstance, but instead are the product of a rigorous **policy framework** adopted by governments and organizations at the highest levels. This policy framework:

- **Recognizes** that CI risk management efforts cannot succeed in the absence of **a strong public-private partnership;**
- **Clearly defines CI goals and roles;** and
- Makes a strategic **policy commitment to risk management.**

Strong, collaborative stakeholder partnerships are essential to both formulating an effective policy framework and implementing the trustworthy policies and plans that these frameworks generate. In order to maintain such collaboration, all stakeholders must continuously derive benefits that create value. Put another way, there must exist a strong "**value proposition**" that both recognizes and leverages stakeholders' respective expertise, providing a foundation for their continued participation. This value proposition takes into account the goals, expertise, and risk management concerns of all key parties: infrastructure owners and operators, technology vendors, and governments.

Table 1 illustrates some of the various, important roles that each of these major stakeholders have in a collaborative critical infrastructure protection policy framework.

Entity	Key Roles
Government	• Define CI policy and identify roles • Provide private sector value proposition • Identify government essential functions
Owners, operators, vendors	• Operate infrastructures • Implement controls • Respond to threats and incidents
Public-private partnership	• Define security goals and assurances • Determine acceptable risk levels • Assess risks • Prioritize risks • Identify controls and mitigations • Measure risk management effectiveness

Table 1 – Critical Infrastructure Protection Roles as Part of a Policy Framework

Resilient Operations

In addition to trustworthy policies and plans, effective critical infrastructure risk management requires **a focus on resiliency.** "Resiliency" refers to the capability to prevent or protect against significant risks, and to minimize the duration and consequence of incidents that do occur. Resiliency requires comprehensive preparedness for **all-hazards** events, which can include cyber attack, physical attack, natural disaster, mechanical breakdown, human error, or any combination therein. The focus on critical infrastructure *resiliency* represents a shift from traditional critical infrastructure "protection." Critical infrastructure *protection* implies the ability to prevent and protect against, rather than withstand, any potential disruption—an undertaking that is not realistic given the complexity of today's critical infrastructures and limited resources. Critical infrastructure *resiliency*, on the other hand, recognizes the importance of successfully managing, rather than simply avoiding, risks and incidents. Resiliency includes protection, as well as effective operational response.

Effective CI risk management focuses on enhancing resiliency by assessing the criticality or importance of a given infrastructure and the nature and level of risks it faces. Public and private stakeholders jointly identify those assets of greatest importance to them, and then help assess, prioritize, and manage related risks.

Of course, various nations organize their CI resiliency efforts differently. For example, as illustrated in Figure 2, some nations consider information and communications technologies (ICTs) a single, key sector; others categorize ICT and other assets cross-sectorally. Regardless of how a nation organizes its CI efforts, there is broad global recognition of the distinct and vital role of critical information infrastructures (CIIs) in the context of critical infrastructure protection.

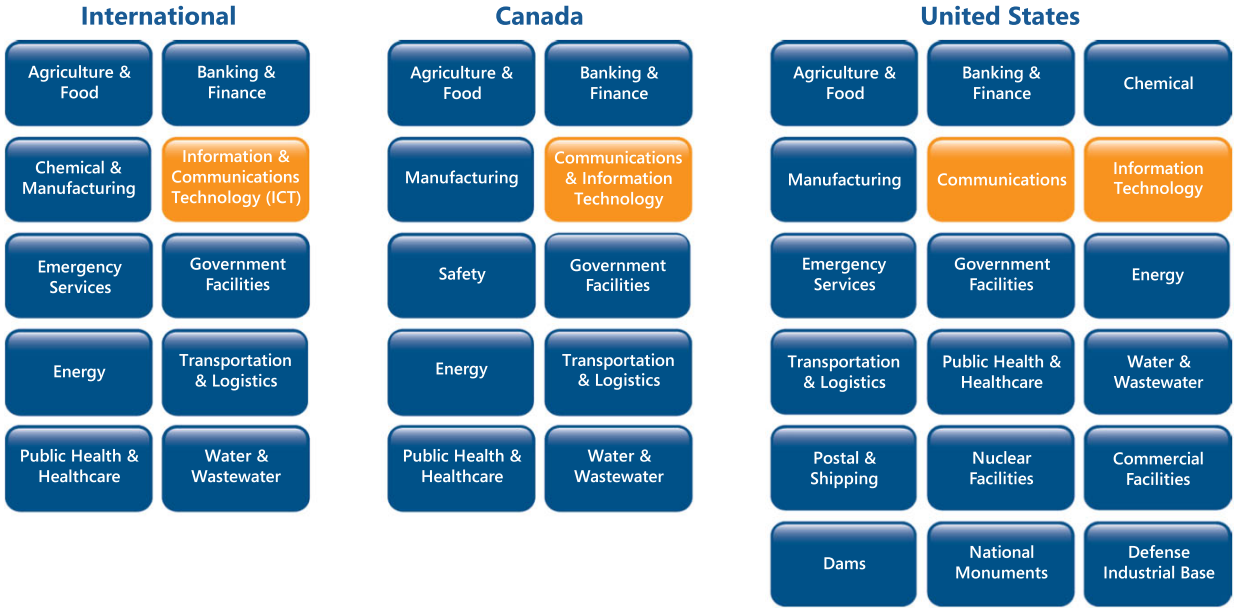

Figure 2 – Comparison of Critical Infrastructure Sector Classifications

Innovative Investments

Critical infrastructure must constantly evolve and enhance its security posture to counter ever more sophisticated threats. **People, processes, and technology** must all be considered when outlining CIP practices, programs, education and training, and research. Continuous, innovative investments in each of these areas comprise a third essential principle of CI risk management.

All stakeholders drive innovations that can improve critical infrastructure resiliency. In the case of critical information infrastructures, for example, operators can update risk management practices for managing risk, collaborate with vendors on emerging and evolving threats, and improve line-of-business applications, security operations, and incident response. CII vendors, on the other hand, can invest in research and development of technologies to mitigate emerging cyber threats, and strengthen resiliency by improving their development processes, security features, and products or services. Governments, for their part, can make much-needed investments in fundamental security research, and develop mechanisms to support trusted collaboration among disparate organizations. They can also strengthen education and training programs for information technology professionals. Finally, universities can help innovate by integrating security into curricula for computer scientists and engineers.

Trusted Collaboration and Information Sharing

All three principles of effective CI risk management—trustworthy policies and plans, resilient operations, and investments in innovation—are enabled and advanced through **continuous collaboration and information sharing.** Specifically, underpinning all successful CI risk management efforts is the existence of a safe environment where all stakeholders can freely and frankly share information on threats, vulnerabilities, and consequences. Such collaboration enables stakeholders to better identify trends, understand risk, and evaluate mitigations. Indeed, in the absence of trusted collaboration and information sharing, both strategic and operational infrastructure protection activities are simply inadequate to provide optimal security and resiliency.

Fundamentals of Risk Management for Critical Infrastructures

With the fundamental principles of effective CI risk management well understood, we turn to a core activity in CI risk resilient operations: proactive, strategic risk management. Specifically, in this section we examine:

- **Why** risk management should be used to improve the resiliency of infrastructures;
- **How** stakeholders can approach risk management for different types of infrastructures; and
- **What infrastructures** should be the focus of these efforts.

We will then apply these fundamentals to that increasingly important subset of critical infrastructures, *critical information infrastructures***.**

Why manage risk to critical infrastructures?

Stakeholders *manage* risk to critical infrastructures because it is simply infeasible to protect *all* infrastructures against *all threats*. In order to be used more effectively and efficiently, limited governmental and private sector resources must be applied in a manner that reflects risk. In other words, resources should be focused on what is critical, vulnerable, and facing the most consequential threats. Once risks are assessed, strategies and priorities for managing these risks—including mitigation, transfer, and, in some cases, acceptance—can be established.

And since risk management is a continuous process, rather than an end state, strategies for mitigating risk must be employed across *all* phases of the risk management process. Specifically, **prevention, preparedness, response,** and **recovery**. Figure 3, below, illustrates the application of risk management strategies across all four phases of continuous risk management.

Figure 3 – Risk Management Activities Across the Continuous Risk Management Cycle

How should critical infrastructure risk be managed?

Critical infrastructure risk should be managed by selecting a **methodology strategy** appropriate for the infrastructures in question. A methodology strategy is essentially the "camera angle," or viewpoint, taken on risk management. There are two principal strategies in this regard: **bottom-up** and **top-down**.

In essence, a bottom-up strategy for risk management focuses on first cataloguing all assets, and subsequently linking those assets to the entity or organization's overall goals. A top-down framework, on the other hand, establishes the entity or organization's overall goals at the outset, and then determines which infrastructures or assets support those goals. Each of these frameworks, along with its strengths and limitations, is discussed below.

Bottom-up

Using a bottom-up strategy for risk management, pieces of systems and/or business activities are classified with the intent of demonstrating their relevance to a grander system of organizational importance. This is done by exhaustively cataloging and characterizing assets, often based on specific risk management criteria. The goal is to gather a complete collection of assets, systems, or functions that, once combined, will provide a complete top-level view.

A bottom-up risk management strategy tends to work well in cases where the infrastructure in question is well-defined or easily identifiable, and where risks to that infrastructure are perceived to have a high consequence. For example, bottom-up strategies have been applied to risk management in the power and energy industry, where major assets—such as power stations—are easily quantified, and where risks to those assets have a clear and significant consequence. In cases like these, industry or governmental criteria already exists with respect to what assets are considered "critical," making the application of a bottom-up risk management strategy generally straightforward.

While comprehensive in scope, the bottom-up strategy often suffers from a **lack of integration**. Specifically, this framework can result in a complex tangle of elements, each of which is developed and assessed for risk in isolation. In addition, by starting at the bottom with components that make up a greater system, there are no overarching security goals or assurances established at the outset. These goals and assurances are, however, essential to underpinning risk assessment and management activities for critical information infrastructures. That is why a bottom-up strategy tends to instead work best for risk management activities that focus on physical or location-based assets. Physical assets, such as electric power substations or water reservoirs, are easily identifiable, and the number of high consequence risks can likely be easily identified and managed. That is not, however, the case with CII assets. Given the fact that CIIs are crosscutting, dynamic assets comprised of highly-complex interdependencies, assessing and managing their risks requires a **top-down**, **function-based** framework.

Top-down

Derived from systems theory, the top-down strategy for risk management begins with a high level view of the system, business or mission. It then works from the top down to decompose that system, business or mission into subsystems and functions. For a typical business or organization, the top-down strategy focuses on delineating business-critical processes, functions, or services.

In the case of governments, the top-down strategy examines essential national functions or services. That is the case in the United States, for example, where Homeland Security Presidential Directive 7, or HSPD-7, defines six consequence categories for prioritizing and categorizing essential services. Specifically, they are consequences that:

Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
Impair federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
Undermine state and local government capacities to maintain order and to deliver minimum essential public services;
Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
Undermine the public's morale and confidence in national economic and political institutions.

Table 2 – HSPD-7 Consequence Categories

At an organizational level, top-down risk management is commonly used. Senior leadership sets policy and direction regarding how much risk the organization is willing to take on, which then results in specific organizational policies, standards, and guidelines. A business impact analysis is another example of a top-down strategy. In that case, critical business functions, processes and assets are identified according to the potential impact of disruptions therein to the business, and risk management priorities are then set by organizational leadership.

In the realm of critical infrastructures, a top-down risk management strategy looks at **high level systems or functions** and examines the consequences of a potential threat or incident. It then supports these systems or functions by assessing, prioritizing, and managing risks to these systems or functions.

Regardless of whether a nation or sector initiates a top-down strategy for risk management by looking at nationally essential services or critical business processes, information and communications technologies will play a critical role in the assessment. That is because CII functions are characterized by important interdependencies and complex value or supply chains; they are essential to providing high-level functions across a number of assets, systems and functions not only in their own critical information infrastructure, but across other critical infrastructure sectors. National emergency response capabilities, for example, rely in large part on effective communications technologies. Not surprisingly, then, an effective top-down risk management framework for CII requires careful examination of these value chains.

What infrastructures should be assessed?

The appropriate object, or focus, of risk management varies depending on how stakeholders categorize a particular critical infrastructure and on the characteristics of that infrastructure. As Figure 2 illustrated, different nations or regions categorize various CIs differently. At the same time, different sectors have varying qualities, attributes and characteristics. In the Transportation Sector, for example, most infrastructure—roads, bridges, railways, and pipelines—are physical in nature. In the ICT sector, on the other hand, virtual "assets" far exceed physical ones. The Internet, for example, does not exist in one computer, network, or geographical location, but is instead a system of systems that spans computers, networks and locations. Indeed, most ICT infrastructures are not "assets" at all in the traditional, location-centric sense of risk management. Rather, they are **functional or service-oriented in nature**, requiring a unique framework and focus for risk management activities. Table 3, below, provides some common approaches to categorizing infrastructure: Asset-based, location-based, system-based, and function-based.

Risk Object Approach	Description
Asset-based (e.g., substation, monument, chemical plant)	Assesses traditional, physical assets based on their value and loss impact.
Location-based (e.g., nuclear power plant, stadium, dam, data center)	Assesses locations that are critical to activities based on geography, topography, and demographics.
System-based (e.g., rail system, highway system, pipeline, energy grid)	Assesses a functional system (or system of systems) based on its criticality to business success.
Function-based (e.g., Domain Name Services, Internet backbone, ICT)	Assesses function or service provided, rather than the physical nature or location of that function or service.

Table 3 – Risk Object Classification Approaches

Which risks should be managed?

All hazards to a critical infrastructure must be managed. An all-hazards approach prepares for threats originating from both natural and man-made sources, intentional and non-intentional. These range from human error to natural disaster to terrorism and cyber attacks.

An all-hazards approach is well suited to the challenge of infrastructure interdependencies, since disruptions to one asset or infrastructure can have huge, cascading effects on interconnected assets and infrastructures. These interdependencies make CII risk management all the more complex.

International Risk Management Standards

A wide range of risk management frameworks and standards exist globally. Most of these, however, focus on system or organizational risk, and thus generally lack applicability to the complex problem of risk management for critical infrastructures. In particular, current international standards for risk management fail to adequately address the interconnectedness and interdependencies common to critical information infrastructures. Appendix 1 includes a description of a number of international standards that, while appropriate in certain contexts, are not specifically designed for critical information infrastructures. These include:

- ISO/IEC 2700 Series
- Payment Card Industry Data Security Standard
- EU Data Protection Directive
- IS/IEC 16085
- Control Objectives for International and Related Technology (COBIT)
- U.S. NERC CIP Standards
- U.S. Sarbanes Oxley Act
- U.K. Data Protection Act

Additionally, in most cases where risk management standards are applied to critical infrastructure, they are generally applied to a *particular* critical infrastructure sector—for instance, banking or energy—rather than a crosscutting set of critical infrastructure *functions.* For example, ISO/IEC 27000 Series focuses on organizational information security management for information systems, while ISO/IEC 16085 focuses on risk management for systems and software engineering lifecycle processes.

The United States, Australia and New Zealand

While a strong body of standards exists for system and organizational risk, the same cannot be said for top-down, functional risk management standards for critical infrastructures. Of course, certain concepts of system and organizational risk do apply to critical infrastructure risk management, and some nations have employed these concepts in the context of critical infrastructure protection standards. The United States, as well as Australia and New Zealand, offer examples in this regard, although it should be stressed that neither set of standards fully meets the unique needs of CI risk management.

In the United States, the **National Infrastructure Protection Plan (NIPP)**[1] offers a risk management framework that is based on a process-oriented, generally top-down framework. The NIPP process:

- Begins with an assessment of goals and objectives;
- Moves on to an identification of assets, systems, and networks;
- Examines risks and prioritizes relevant responses; and
- Implements programs whose effectiveness is continually measured.

A somewhat different framework is reflected in the **Australian/New Zealand** standard known as **AS/NZS 4360:2004**[2]. This standard, which places a higher-level focus on overall organizational risk, provides a generic framework—usable in a broad range of contexts—that is top-down in nature. The AS/NZA process:

- Begins by establishing the context for risk management—whether from an organizational, national or sector perspective;
- Assesses the universe of potential risks;
- Treats identified risks; and
- Monitors and reviews risk treatments through a process of ongoing communication and consultation.

Both the U.S. NIPP and AS/NZS frameworks are illustrated in Figure 4, below:

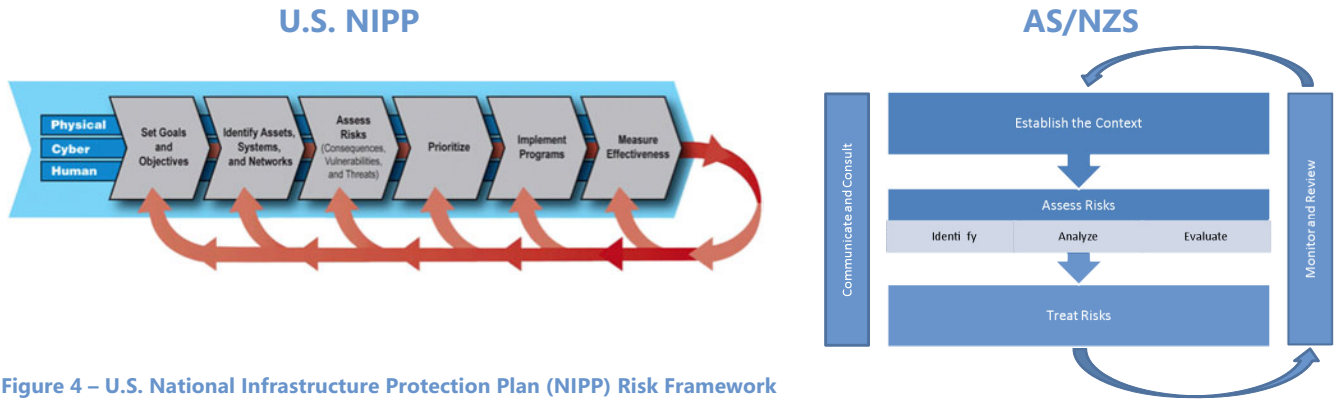

Figure 4 – U.S. National Infrastructure Protection Plan (NIPP) Risk Framework (left) and the Australia/New Zealand Risk Management Standard, 4360:2004 (right).

While each of these frameworks is useful in a general risk management context, neither the U.S. National Infrastructure Protection Plan (NIPP) nor the Australia/New Zealand Risk Management Standard adequately addresses the range of risk management challenges posed by critical information infrastructures. Indeed, the uniquely interconnected and interdependent nature of CIIs poses challenges not fully addressed by any single, traditional framework for risk management.

[1] For more information on the NIPP, see http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[2] For more information on the Australia/New Zealand Risk Management Standard, see: http://www.riskmanagement.com.au/

Microsoft's Framework for CII Risk Management

In response to shortcomings in the applicability of traditional risk assessment frameworks for critical information infrastructures, and based on years of engagement with governments and CI providers, Microsoft has developed a function-based framework specifically tailored to CII risk management. Microsoft offers this framework as input into the global conversation on enhancing the resiliency of critical infrastructures globally.

Microsoft's top-down framework for critical infrastructure risk management is built upon the key supporting principles highlighted in the first section of this guide:

- **Trustworthy policies and plans;**
- **Resilient operations;**
- **Investments in innovation; and**
- **Trusted collaboration and information sharing.**

Specifically, Microsoft's framework focuses on understanding the **functions** of the infrastructures in question, rather than cataloging any fixed, physical assets. It promotes a **qualitative assessment** of sector-wide risks that enables public and private partners to **prioritize and employ continuous risk management**. This is done by:

- Examining security and resiliency goals and assurances;
- Identifying critical functions; and
- Assessing existing risks and their level of acceptability, if any.

Microsoft's recommended framework for CII risk management is, importantly, a **continuous** process conducted within a **collaborative, public-private** partnership that includes governmental stakeholders as well as critical infrastructure owners, operators, and vendors. It is intended to augment and build a bridge to—rather than displace—risk management activities undertaken by individual organizations, including critical infrastructure owners and operators, vendors, and government agencies.

There are five steps to Microsoft's framework for CII risk management. They are:

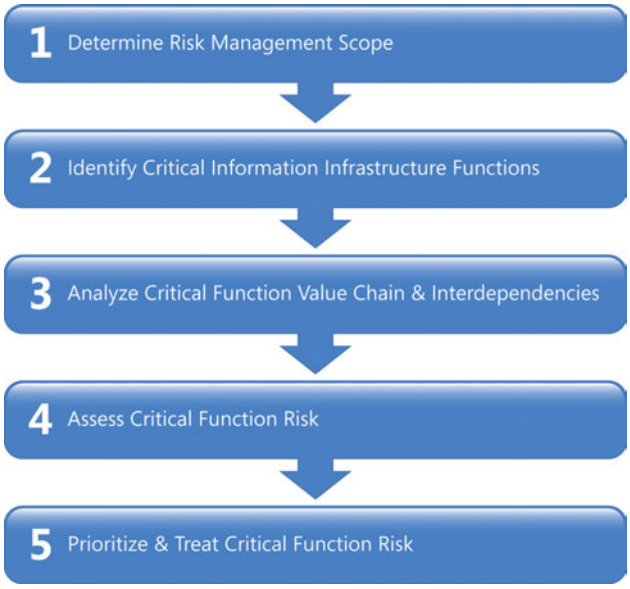

Figure 5 – A Top-Down Framework for Risk Management for Critical Infrastructures

As with traditional risk management endeavors, CII-focused risk management begins **by determining the appropriate scope of risk management objectives and activities.** This is done in three consecutive parts:

- Reaching stakeholder consensus on a **statement of mission and vision**;
- Setting forth specific **security and resiliency goals, objectives and assurances**; and
- **Identifying essential services**.

Reach Consensus on Mission and Vision

Stakeholders, both in individual organizations and critical infrastructure sectors, must first determine what they are trying to protect and why. Typically, this means describing a desired end state in a **statement of mission for—and vision of—security and resiliency.**

Figure 6 provides an example of the mission/vision statement for infrastructure resilience and security in the United States Information Technology Sector.

Vision Statement for the United States Information Technology Sector

Public and private IT Sector security partners will continue building infrastructure resilience to support:

- The Federal Government's performance of essential national security missions and preservation of general public health and safety;
- State and local governments' abilities to maintain order and to deliver minimum essential public services; and
- The orderly functioning of the economy.

The IT Sector will continue to coordinate with other CI/KR sectors and work to ensure that any disruptions or manipulations of critical IT Sector functions are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Source: U.S. IT Sector Specific Plan (SSP)
http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf

For more information on other U.S. sector specific plans, see
http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm

Figure 6 – A Vision for Security and Resiliency from the U.S. IT Sector

An information security and resilience mission/vision statement for an individual organization, on the other hand, may look similar to the following:

Organizational Vision Statement for Information Security and Resilience

IT environment comprised of services, applications, and infrastructure that implicitly provides availability, privacy, and security to any client while providing five key assurances:

- Identity is not compromised
- Resources are secure and available
- Data and communications are private and reliable
- Roles and accountability are clearly defined
- There is a timely response to risks and threats

Figure 7 – An Example Organizational Vision/Mission Statement for Information Security

Establish Goals, Objectives, and Assurances

Once stakeholders have established a statement of mission and vision, they should embark on a collaborative effort to identify **goals, supporting objectives, and assurances** for security and resiliency. In this context:

- Goals describe a high-level desired outcome or capability;
- Objectives refer to broad, supporting activities that help achieve those goals; and
- Assurances are end-state statements that build confidence about security and resiliency.

Goals for CII resiliency may cover a variety of areas. For example, they may include a specific risk management agenda, or they may include broad areas such as information sharing, situational awareness, or response and recovery. Reaching agreement on these goals, along with the objectives and assurances that support them, is essential for any successful risk management effort. Without such agreement, these efforts will fail to be unified and aligned across the given sector.

Reaching consensus in this area requires two things:

- A **collaborative partnership** among public and private sector stakeholders, since their expertise and participation will be required throughout the risk management process; and
- **Strong policy support** from the executive and legislative branches of government, since this indicates a serious commitment to cyber security and critical infrastructure protection.

Table 4, below, provides an example of agreed-upon, sector-level goals, objectives and assurances in the realm of information security (ISO/IEC 17799[3]).

Sector Goal	Objectives	Assurances
Goal 1: Prevention and Protection Through Risk Management Identify, assess, and manage risks to the sector's infrastructure and its international dependencies.	Identify and annually review critical sector functions that support the Nation's security, economy, public health, and safety. Assess and prioritize risks to critical sector functions, including evaluating emerging threats, vulnerabilities, and technology, and mapping them against the infrastructure to prioritize protective efforts. Tailor protective measures, which mitigate associated consequences, vulnerabilities, and threats, to accommodate the diversity of the sector and develop and share security and resiliency best practices and protective measures with security partners. Encourage sector entities to exchange information about risk management strategies and foster a better understanding of how they improve the overall posture of the sector.	*"The IT Sector will conduct continuous risk management activities that ensure risk treatment options are employed according to risk."* *"Risk treatment decisions will drive sector risk to acceptable levels with optimal resource usage."*

[3] ISO/IEC 17799, also known as ISO/IEC 27002, is part of the 'ISO/IEC 27000 series' and is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled *Information technology – Security techniques – Code of practice for information security management*.

Sector Goal	Objectives	Assurances
Goal 2: Situational Awareness Improve situational awareness during normal operations, potential or realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against sector infra-structure, technological emergencies and/or failures, or governmentally-declared disasters.	Collaborate, develop, and share appropriate threat and vulnerability information among public and private sector security partners, including development of indications and warnings. Expand strategic analytical capabilities that facilitate public and private sector security partner collaboration to identify potential incidents.	*"The sector provides a common operational picture of key sector functions and activities."* *"The IT sector provides world-class cyber analytical capabilities."*
Goal 3: Response, Recovery, and Reconstitution Enhance the capabilities of public and private sector security partners to respond to and recover from realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against sector infrastructure, technological emergencies and/or failures, or presidentially declared disasters, and develop mechanisms for reconstitution.	Develop and maintain communications, including establishing mechanisms and processes for communicating with other sectors during contingencies, and conduct annual tests of the resulting communication plans and programs. Develop and maintain incident response and coordination plans and procedures, and exercise them annually to ensure readiness and resilience. Develop plans, protocols, and procedures to ensure that critical sector functions can be reconstituted rapidly after an incident. Collaborate with law enforcement to identify and mitigate criminal activities that have the potential to harm the sector's infrastructure.	*"There is a timely response to risks and threats."* *"The IT Sector response is aligned and synchronized with sector partners."* *"Recovery of IT Sector critical functions is accomplished in minimal timeframes."*

Table 4 – Example of ICT Sector Security Goals, Objectives, and Assurances

Goals Yield Operating Principles

Collaboratively developed CII resiliency goals, objectives, and assurances yield an important tool: **Operating principles**. These are **fundamental concepts used to design, develop, and operate secure and resilient infrastructures, functions, networks, and systems**. Such principles:

- Enable CIP stakeholders and partners to understand and incorporate resiliency and security concepts in the design, development, and operation of infrastructure functions;
- Organize and communicate security policies, requirements, and guidelines throughout the CII "ecosystem"; and
- Improve the way security risks are communicated between the public and private sectors, among specific infrastructure sectors internally, and to others who are dependent on critical infrastructures.

Operating principles are important because they can be leveraged by stakeholders to build a given operational response framework. Specifically, they enable CIP stakeholders to develop consistent processes to generate deliverables, such as risk assessments, security and resiliency policies, and requirements to manage risk.

Identify Essential Services

Determining core organizational "assets" is another key component of establishing the appropriate scope of risk management activities. These "assets" are the **essential services, processes, or functions** that enable an organization to succeed, achieve revenue goals, or keep customers and shareholders satisfied. From the point of view of a government, essential services are things like revenue collection, monetary transfer and exchange, national defense and command authority, continuity of government, public safety and emergency response services, public health systems, and citizen services, among others. Figure 8, below, provides examples of essential government services, processes or functions.

Figure 8 – Example Essential Government Services, Processes, or Functions

2 Identify Critical Information Infrastructure Functions

Identifying critical information infrastructure functions is the next step in effective CII risk management. In this step, stakeholders conduct an open dialogue about criticality; that is, they **jointly determine which information infrastructure elements, critical functions, and key resources are needed** to deliver essential government services, ensure orderly functioning of the economy, and provide public safety.

Because of their virtual and non-location centric nature, however, CIIs cannot simply be "inventoried." Instead, they **must be identified according to how they support essential services**, including stakeholders' shared vision, security goals and objectives.

Not every information infrastructure, however, is "critical." Some ICT networks play a greater role in enabling essential functions than others. For example, a particular computer network may have no role in a critical infrastructure, while another will play a key role in enabling key services such as banking, transportation, or the provision of energy. By using a top-down, function-based risk management methodology, CIP partners can focus on the key aspects of critical information infrastructures—those on which essential services depend—applying limited resources to where they are most needed.

Figure 9, below, illustrates the relationship between critical and non-critical infrastructures, both physical and virtual.

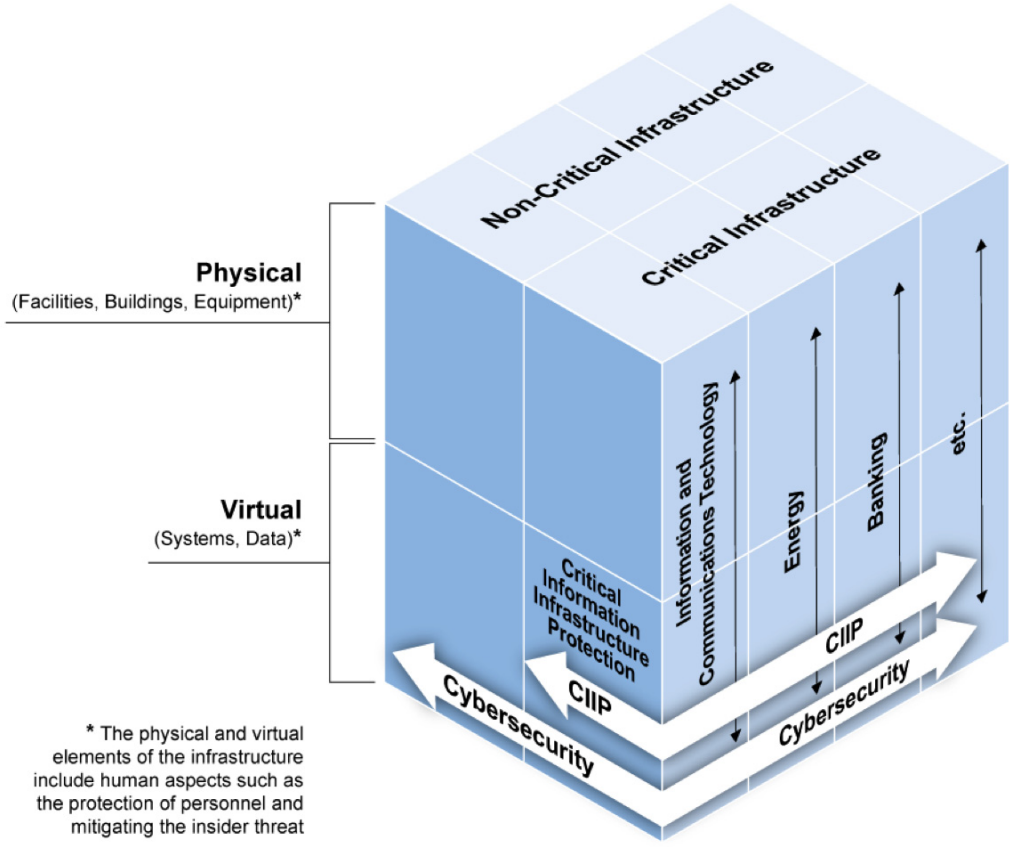

Figure 9 – Relationship Between Cybersecurity and Critical Information Infrastructure Protection (Source: ITU)

A critical component of stakeholder identification of CIIs is the enumeration of **critical functions**.
This is done by:

- Noting the full range of elements that must be enumerated;
- Grouping ICT elements into functional constructs that are logically organized; and
- Continually re-enumerating critical functions.

Note full range of elements to be enumerated

All elements of an information infrastructure must be enumerated. These include not only the infrastructure's physical *and* cyber elements, but also the processes and people that directly support its operations.

Group ICT elements into functional constructs

Once all elements of the infrastructure have been enumerated, they should be grouped according to either the services they provide or the critical information infrastructure activities that they support. For example, grouping according to services provided may yield categories such as routing, Internet content services, and broadcast delivery. On the other hand, grouping according to the critical information infrastructure activities supported may result in categories such as sector-wide incident management or operational response. Either way, these elements are organized according to functions that, if disrupted, could have an immediate and debilitating impact on the infrastructure's essential missions or services.

Continually re-enumerate critical functions

Since criticality is situation dependent, all critical functions must continually be re-enumerated. In other words, what is critical in one instance may not be critical in the next. As a result, identified and prioritized critical infrastructure and key functions will change as essential services change, and as technology, infrastructure, and processes evolve.

Enumeration Reveals Interdependence, Value Chains

This process of enumerating critical functions will yield two important findings:

- These essential functions, services or processes will have a key **dependence on critical information infrastructure**. That is, essential ICT systems will enable these functions to be carried out and to meet their security and resiliency goals; and
- These functions will be comprised of **complex value chains spanning multiple, interdependent infrastructures**, of which CII is only one.

Sample Critical Function: DNS

One widely-recognized critical function of the Internet is the **Domain Name Service (DNS) infrastructure.** DNS is comprised of a set of technologies and services provided by infrastructure owners/operators and vendors which, taken as a whole, deliver a critical unit of functionality to higher level services, such as resolving a name to an IP address. Like other critical functions, a complex and interdependent value chain characterizes DNS. It is subject to vulnerabilities and risks that, if exploited, could have serious consequences to business and economic activities, as well as critical government services involving national security, public health, and safety.

No "One Size Fits All"

There is no "one size fits all" answer to defining a set of CII functions, however. These may vary by country and region and are dependent on how that particular country or region organizes (or "breaks out") their particular sectors. (Figure 2 of this guide illustrated the diversity with which countries and regions compose their critical infrastructure sectors, and the fact that there is not one agreed-upon classification of the information technology and communications sectors.) The key is to select a set of CII functions that best describes the dependencies that other infrastructures have on the critical information infrastructure in question.

Table 5, below, provides a hypothetical set of CII Functions. Using a top-down framework, the example begins by determining a top-level set of essential services and processes. It then enumerates the CII functions on which these essential services and processes depend.

Critical Information Infrastructure Function	Description and Components
Develop and Provide Information and Communications Technology Products and Services	Design, develop, support and sustain information and communications hardware and software. Design, develop, deploy, operate, and sustain online information and collaboration services. Provide incident management and response for information and communications technologies.
Provide Domain Name Registration and Resolution Services	Provide, operate, support, and sustain DNS Registration Services[4]. Provide, operate, and sustain DNS root, TLD and other domain infrastructure. Provide governance and oversight of the global DNS system and infrastructure.
Provide Digital Identity Management and Trust Infrastructure Services	Manage and operate root certification authorities and associated certification issuance and revocation services and infrastructure. Provide organizational digital identity provisioning and verification services and infrastructure. Provide individual digital identity provisioning and verification services.
Provide Internet Access, Routing and Core Services	Provide, operate, and sustain critical Internet exchange and interconnection facilities and infrastructure. Provide, operate, and sustain Internet backbone/core services and infrastructure. Provide, operate, and sustain local access infrastructure. Provide governance, operations, management, and support for Internet routing, peering and core services.

Table 5 – Hypothetical Set of Critical Information Infrastructure Functions Representing ICT

[4] DNS registration services allow domain names to be registered with a top-level domain for the purposes of resolving them to host addresses on the Internet. See http://www.icann.org/en/general/glossary.htm

3 Analyze Critical Function Value Chain & Interdependencies

Understanding and analyzing value chains is the third step in managing risk for CII functions. After all, essential services, processes, and functions are not monolithic entities, but rather a composition of integrated sub-components, services, processes, and functions that jointly enable an end objective. Each of these subcomponents, in turn, is comprised of a value or supply chain—physical or logical—that is essential to the delivery and function of that service.

Figure 10, below, illustrates the complex value chain that typically exists for critical functions, as well as the "web" of interdependencies often encountered. Understanding these complex and interdependent value chains not only assists in the analysis of threat, vulnerability and consequence, but also helps identify stakeholders and key providers in the value chain that may otherwise be overlooked.

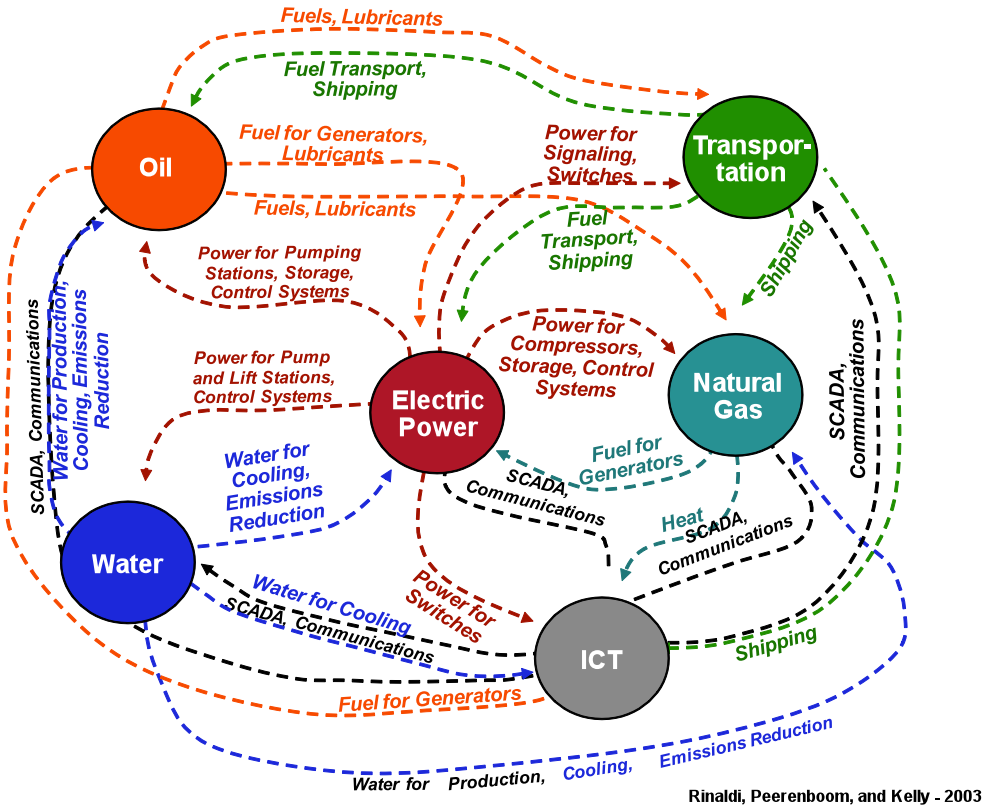

Figure 10 – An illustration of Value Chain and Interdependency Analysis

The sample Domain Name Service (DNS) CII function discussed earlier provides a useful example of a hypothetical value chain. Like most essential functions, the DNS service upon which the Internet depends is not monolithic in nature. Instead, it is comprised of numerous sub-functions that jointly enable Internet host and domain names to be resolved to IP addresses. For example, there exists a sub-function that provides registration and registry services such that domain names can be recognized Internet-wide. There also exists a group of DNS "root servers"[5] distributed globally, which maintain information about the domain naming infrastructure, as well as a DNS governance function provided by ICANN[6] and other entities. In short, the worldwide DNS infrastructure consists of thousands of DNS servers and clients deployed across enterprises, governments, Internet service providers, and private homes, each of which runs a variety of software programs, from Microsoft Windows to UNIX, BIND[7] and NSD[8].

Like all critical functions, DNS functions create a wide variety of interdependencies that must be examined within a specific context of criticality. For example, if the United States Government were to examine critical services utilizing the ".gov" or ".mil" domains, it would need to understand how those domains are provisioned and operated, and who provides those services. It would also need to understand the dependencies that those services bear on other CII functions, such as Internet Routing and Access, and other CI sectors, such as energy or transportation.

4 Assess Critical Function Risk

In step 4 of the CII risk management process, stakeholders focus specifically on **threats to, and vulnerabilities of, critical functions**.

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

Risk to CIIs is **a function of threat, vulnerability, and consequence**, where:

- ***Threat*** refers to natural and manmade agents—and their motivations, intentions and capabilities—as well as the likelihood that the threat exists or will occur[9].
- ***Vulnerability*** refers to a weakness or limitation that can be exploited by a threat.
- ***Consequence*** (also called *impact*) is the cost, loss or resulting outcome of a threat that successfully exploits vulnerability. Put simply, consequence is what assigns the value or loss factor to any risk assessment.

[5] For more information on the DNS root server infrastructure see http://www.root-servers.org/ and http://en.wikipedia.org/wiki/Root_nameserver

[6] ICANN – Internet Corporation for Assigned Names and Numbers – http://www.icann.org

[7] BIND Berkeley Internet Name Domain or "named" – http://en.wikipedia.org/wiki/BIND

[8] Name Server Daemon – http://en.wikipedia.org/wiki/NSD

[9] Note that threat can also refer to the aggregate of threat agent and the vulnerability exploited. However, in the context of this risk management framework, threat is treated in its purest form, as described above.

In short, **risk is the likelihood that an event—a threat exploiting vulnerability leading to an undesirable consequence—will occur.** Undesirable consequences vary depending on the organization in question. At the national level, they are typically consequences that impact national and economic security and public health, safety and confidence.

Figure 11, below, illustrates the relationship between risk, threats, vulnerability, and consequence.

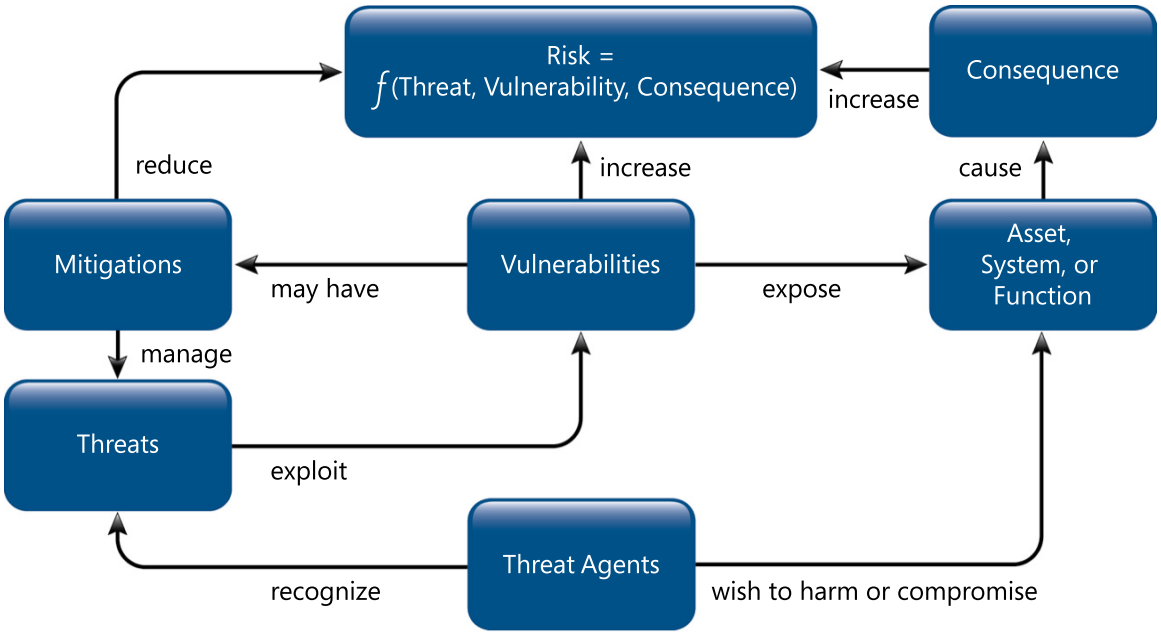

Figure 11 – An Illustration of Risk

Modeling Risk: Two Sample Methods

Critical functions risk is typically assessed with the help of different assessment "models." In fact, stakeholders often use *multiple* risk assessment modeling techniques in order to ensure thoroughness and diversity of perspective. Two highly complementary frameworks for risk modeling—**scenario and "threat tree"**—are discussed in detail below.

Scenario-based Method

A scenario-based method for modeling risk for critical functions focuses on evaluating risks resulting from **specific predetermined threat actors and vulnerabilities**. These threat actors may be natural or manmade, intentional or unintentional nature (in other words, all-hazards). For example, an organization that has critical assets located in a region where hurricanes are commonplace may evaluate risk given a specific hurricane threat.

Scenario-based risk modeling looks at specific, predetermined threat actors and vulnerabilities.

Similarly, a **scenario-based assessment for a critical information infrastructure** may **focus on specific concerns about or threats against critical functions**. For example, in the case of the DNS critical function, CIP stakeholders are likely to evaluate risk for a specific set of scenarios that are top-of-mind for DNS. These may include DNS cache poisoning, amplification attacks, or root server compromises[10].

Figure 12 illustrates how a scenario-based framework first focuses on *threat x vulnerability,* and then evaluates potential consequences that may result from that scenario. Inherent or existing risk treatments may also be considered.

Scenario-based risk assessment, however, is not foolproof. While this framework provides strong coverage for threats and vulnerabilities that are top-of-mind, it does not include scenarios that have not been conceived in the minds of those conducting the risk assessment. This weakness is often referred to as "a failure of imagination,"[11] in which threats, vulnerabilities, or consequences are either over-looked or simply not contemplated. As a result, while scenario-based risk assessment maintains an important place in CII risk assessment, it must be complemented with other frameworks.

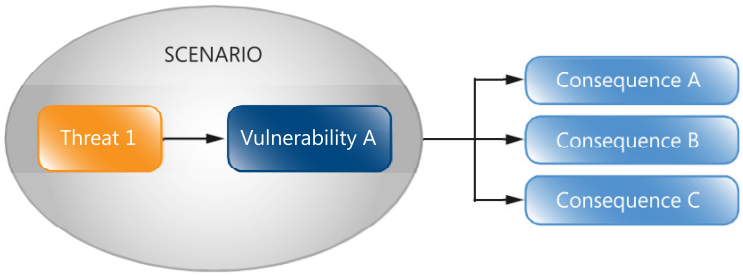

Figure 12 – A Scenario-based Risk Modeling Framework

[10] For a more examples of common DNS threat scenarios see: http://en.wikipedia.org/wiki/DNS_cache_poisoning, http://www.dnssec.net/dns-threats, http://tools.ietf.org/html/draft-ietf-dnsext-dns-threats, http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf, and http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

[11] In the United States, the 9/11 Attacks in 2001 demonstrated that a motivated actor could use a commercial airliner as a flying fuel bomb—a risk assessment oversight that the 9-11 Commission Report referred to as a "failure of imagination"—see: http://www.9-11commission.gov/

Threat Tree Method

Threat tree-based risk modeling uses conceptual diagrams to map out the full range of potential threats and lines of attack to a given system.

The **"threat tree"** method for modeling CII risk uses **conceptual diagrams to map out potential threats and vectors of attack** to a given system. These multi-leveled diagrams, or "trees," consist of one **"root" representing the attacker's goal** (or, from the perspective of the CII risk manager, the undesired consequence of an attack). **"Branches"** of this tree denote the conditions—also known as the exploitation path—that must be satisfied in order for the attacker's goal to be reached. By examining the full tree, stakeholders can evaluate the universe of potential threats and vulnerabilities to a critical function and make appropriate risk management decisions therein. These decisions include whether to **accept, reduce**, or **transfer risk** until an acceptable level is reached.

Threat tree analysis is an important complement to scenario-based risk management because, rather than focusing narrowly on a finite set of scenarios, the threat tree framework examines:

- All of a critical function's **vulnerabilities**;
- All of that critical function's potential **threat actors** (natural, manmade, intentional and unintentional); and
- All attack goals and **undesired consequences**.

Figure 13 illustrates the threat tree-based framework:

THREAT TREE APPROACH

Attributes: Landscape of risks
Begins with consequences, branches to vulnerabilities & threats
More comprehensive and more complex

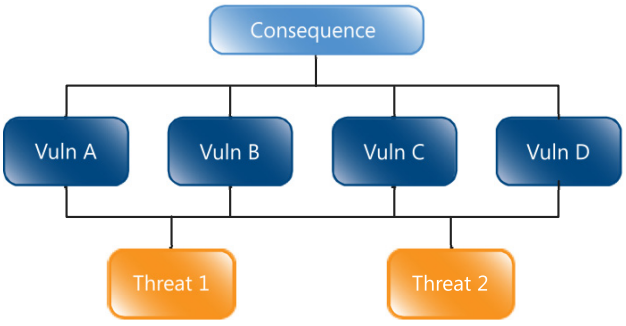

Figure 13 – A Threat Tree-based Risk Modeling Framework

In fact, Microsoft uses a threat-modeling framework very similar to this one in the company's **Software Development Lifecycle, or SDL**. Specifically, software components are diagramed in terms of the interactions between key entities, such as server, client, data stores, data flows, and trust boundaries, among others. Threats to each of these software components are then enumerated, rated, and prioritized. Developers then make decisions about mitigations to the threats modeled in the exercise. In Microsoft's experience, this form of risk assessment and management has significantly reduced security vulnerabilities in the company's software and services.

Example: Threat Tree Method for DNS Critical Function

The Domain Name System (DNS) critical function provides a useful example of the threat tree method of risk management. Specifically, in the January/February 2006 issue of IEEE Security and Privacy12, Steven Cheung posits a hypothetical denial of service attack that causes DNS resolution to fail. The Internet-wide consequences of such an attack are illustrated in Cheung's DNS threat three (Figure 14), below.

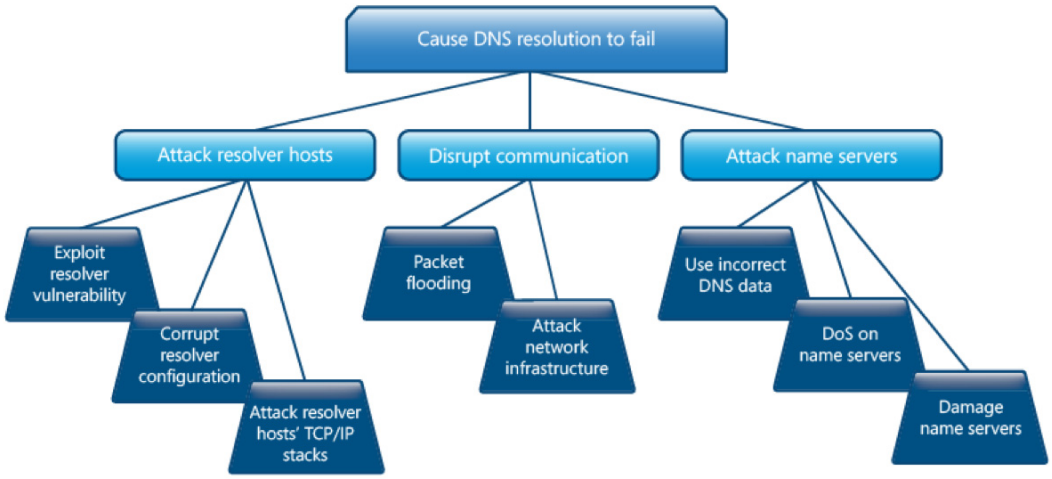

Figure 14 – Example DNS Threat Tree

In this example, stakeholders identify the undesired consequence, or "actor goal"—in this case, failure of DNS resolution—and examine the potential threat agent paths that could result in that consequence. Similarly, stakeholders look at all undesired consequences that could deny, degrade or compromise critical information infrastructure functions. This can be done at the level of the whole function or decomposed into sub-functions, depending on the desired level of granularity.

The goal of this effort is to build threat trees that represent the full "landscape" of threats to the CII function. Each top-level undesired consequence represents the root node of a particular threat branch, with each branch representing the various pathways to be evaluated. In most cases, stakeholders need to reach consensus on which are the key branches and limit the risk evaluation to those. That is because examining every path or branch for a specific function may be, from a practical standpoint, infeasible.

The result is a risk assessment for each CII function that yields:

- A complete threat tree that represents the **landscape of threats**;
- **Three to five key threat branches** for detailed evaluation (the exact number will depend on stakeholder consensus); and
- A **detailed analysis** of each key threat branch. This analysis includes a framework **for measuring and rating threat, vulnerability** and **consequence**.

[12] http://ieeexplore.ieee.org/iel5/8013/33481/01588824.pdf

Profiling Critical Function Risk

Whether stakeholders opt for a threat-tree, scenario-based, or combined framework for risk management, they must incorporate a **scoring or rating system** in their efforts.

One common risk profiling technique is the **Risk Matrix** (also called a risk "heat map"), which uses a table to illustrate the likelihood of a given risk and its potential impact. This technique is illustrated in Table 6, below.

	Negligible Impact	Marginal Impact	Critical Impact	Catastrophic Impact
Certain	HIGH	HIGH	EXTREME	EXTREME
Likely	MODERATE	HIGH	HIGH	EXTREME
Possible	LOW	MODERATE	HIGH	EXTREME
Unlikely	LOW	LOW	MODERATE	EXTREME
Rare	LOW	LOW	MODERATE	HIGH

Table 6 – Example Heat Map Matrix

Another profiling technique is the risk scatter chart. As with the risk matrix, this method looks at risk in terms of likelihood and impact (or consequence), but does so within a four-quadrant graph. Figure 15, below, illustrates a risk scatter chart, where impact (or consequence) is mapped on the vertical (X) axis, and likelihood (or probability) is mapped on the horizontal (Y) axis.

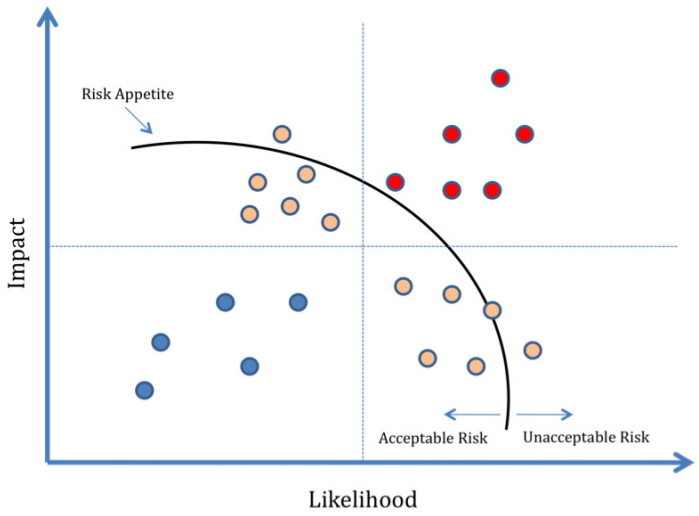

Figure 15 – Example of a Risk Scatter Plot Incorporating Heat Map Characteristics

No matter how stakeholders choose to illustrate risk, they must ultimately determine their **"risk appetite."** That is, after evaluating the likelihood and impact of any given risks, stakeholders must determine which risks are acceptable and which are not. Unacceptable risks are those that require risk treatment, the final step in Microsoft's Risk Management Framework for CIIs.

5 Prioritize & Treat Critical Function Risk

The process of profiling and ranking risks inevitably yields a set of hazards that are outside the stakeholders' **"risk appetite,"** yielding the final step in the CII risk management process: prioritizing and continuously treating unacceptable critical function risk. And of course, these risks must continuously be treated at each phase of the CIP continuum, from prevention to preparedness, response and recovery.

Continuous risk treatment options in critical infrastructure protection typically fall into one of four categories: **Risk mitigation; avoidance; transfer;** or **acceptance**. Each of these is described in Table 7, below.

Risk Treatment Option	Description/Definition
Risk Mitigation	A selective application of appropriate techniques and management principles to reduce or mitigate the likelihood of an occurrence, its consequences, or both[13]. These include plans and processes that allow an organization to avoid, preclude, or limit the impact of a crisis occurring, including through compliance with corporate policy, mitigation strategies, behavior and programs[14].
Risk Avoidance	An informed decision to either not become involved in[15], or to withdraw from[16], a risk situation.
Risk Transfer	A shifting of the burden of loss to another party for a risk through legislation, contract, insurance or other means[17]. These may include various means of addressing risk through insurance and similar products[18].
Risk Acceptance	An informed decision to accept the probability and impact of a particular risk[19]. Similarly, "risk retention" refers to the decision to retain or accept a given risk to the organization or entity.

Table 7 – Definitions of Risk Treatment Options

In the context of typical information security or business continuance policies, the risk treatment options outlined in Table 7 are well known and generally simple to apply. Applying risk treatment options in the context of critical information infrastructures, however, is not as straightforward or obvious.

[13] Business Continuity Institute – BCI
[14] ASIS International
[15] Business Continuity Institute – BCI
[16] Singapore Standard 540 – SS 540:2008
[17] Ibid
[18] Business Continuity Institute – BCI
[19] Singapore Standard 540 – SS 540:2008

For example, within a typical information security department, risk management may involve simply deploying certain IT controls (such as passwords or firewalls) to reduce the likelihood or consequence of a risk. In the CII arena, however, risk treatment is more nuanced and complex. Not only are diverse public and private stakeholders involved, but the overall focus of risk assessment efforts is different. Specifically, CII stakeholders are looking at risk from the perspective of *critical functions*, which means that risk treatment options at this level are more akin to strategies and priorities than actual controls. For example, government and industry may decide upon a set of standards and reasonable practices that are shown to demonstrably improve security and resilience, and these would be implemented across critical information infrastructure functions.

R&D Advances Risk Treatment

Research and development (R&D) also plays an important role in risk treatment, since many of the challenges faced in CII resiliency are not resolvable using existing technologies. Establishing R&D priorities, funding, and market incentives is thus an important component of improving security and resiliency in the long term.

Naturally, vendors who perceive a market opportunity invest in creating improved technologies and solutions. Microsoft, for example, recently became the first online services vendor[20] to achieve the prestigious ISO 27001 certification[21] for its online services infrastructure. Microsoft recognized that enhanced security and resiliency in its critical online services data centers not only served its customers, but also enhanced overall critical information infrastructure resiliency. In this way, a competitive advantage translated into important benefits for the broader cyber ecosystem.

As with any private entity, CII owners/operators and vendors face the challenge of balancing corporate responsibility and citizenship with shareholder value and business goals. That is why a value proposition—such as establishing a competitive advantage, for example—must exist in order for the private sector to invest sufficiently in infrastructure security and resiliency.

On the other hand, in cases where such a value proposition is insufficient or nonexistent, governments can help create other incentives for such investments. For example, they can make direct public investments in research and development programs that might otherwise have limited commercial appeal. Such investments should not seek to displace private sector activities, of course, but rather boost these efforts with thorough early support. Governments can also create incentives for the development of resiliency tools by working to remove discriminatory market barriers that might otherwise preclude a viable environment for these products. In the presence of fair and transparent market conditions, vendors will have the incentive and the means to competitively offer cutting-edge resiliency tools.

[20] http://www.bsiamerica.com/en-us/About-BSI/News-Room/News/Microsoft-Earns-ISO-27001-Certification/

[21] http://www.27000.org/iso-27001.htm

Conclusion: CII Risk Management—A Continuous Process

This guide has detailed the ways in which **critical information infrastructures require** a unique, **top-down, function-based framework for risk management**. Consisting of five steps, this framework calls for:

- Determining Risk Management Scope
- Identifying Critical Information Infrastructure Functions
- Analyzing Critical Function Value Chain and Interdependencies
- Assessing Critical Function Risk
- Prioritizing and Treating Critical Function Risk

This process, however, can succeed only in the context and culture of ***ongoing risk management activity*** throughout each phase of the CIP continuum; that is, prevention, preparedness, response, and recovery. After all, the dynamic nature of CII risk—an **evolving threat landscape**, **developments in innovation**, and a maturing **policy framework**—all require ongoing, rather than static, strategies.

A **strong public-private partnership** among stakeholders is absolutely vital to each of these stages in the risk management process. Through this guide, Microsoft seeks to enable a framework in which government and industry stakeholders can come together and take the steps necessary to enhance information resiliency and security. Microsoft welcomes comments, thoughts and suggestions on this guide in the hopes of furthering this vital mission.

For more information about Microsoft's approach to critical infrastructure protection and its Global Security Strategy and Diplomacy team, visit http://www.microsoft.com/twc or contact cipteam@microsoft.com

Appendix 1: Survey of International Standards and Regulations Related to Risk Management

Standard/Regulation/Guideline	Scope or Applicability
ISO/IEC 27000 Series	Contains best practice recommendations on information security management for use by IT management for initiating, implementing, or maintaining Information Security Management Systems (ISMS) and a growing family of related ISO/IEC ISMS standards. ISO/IEC 27005, for example, provides techniques for information security risk management that includes information and communications technology security risk management.
ISO/IEC 16085	Defines a process for the management of risk in the lifecycle. It can be added to the existing set of software lifecycle processes defined by the ISO/IEC 12207 or ISO/IEC 15288 series of standards, or it can be used independently.
United States Sarbanes-Oxley Act	Establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. It does not apply to privately held companies.
Payment Card Industry Data Security Standard	Requires that a company processing, storing, or transmitting payment card data be PCI DSS compliant or risk losing its ability to process credit card payments, and face fines and/or audits.
Control Objectives for Information and Related Technology (COBIT)	Provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist in maximizing the benefits derived from the use of information technology and developing appropriate IT governance and controls in a company.
United Kingdom Data Protection Act	Defines a legal basis for the handling in the United Kingdom of information relating to living individuals. Serves as the nation's primary law governing the protection of personal data.
European Union Data Protection Directive	Regulates the processing of personal data within the European Union.
United States NERC CIP Standards	Used to secure bulk electronic system. The newest version of NERC 1300 is CIP-002-1 through CIP-009-2.
ISF Standard of Good Practice (SoGP)	A detailed documentation of identified recommended practices in information security. First released in 1996, the Standard is published and revised every two or three years by the Information Security Forum (ISF), an international association of organizations in financial services, manufacturing, consumer products, telecommunications, government, and other areas.

Appendix 2: References and Resources

Note: The information below is provided as a reference only. Microsoft does not endorse any particular standard or methodology.

Risk Assessment Terminology and Fundamentals

ISO/IEC Guide 73:2002 – Risk management – Vocabulary – Guidelines for use in standards
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34998

National Institute of Standards (NIST) Risk Management Guide for Information Technology Systems Special Publication 800-30
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

The Mitre Corporation Risk Management Toolkit
http://www.mitre.org/work/sepo/toolkits/risk/index.html

The Information Risk Manager (IRM) Standard
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

International IT Risk Management and Security Management Standards

ISO/IEC 17799:2005 – Information technology – Security techniques – Code of practice for information security management
http://www.iso.org/iso/catalogue_detail?csnumber=39612

ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

ISO/IEC 27005:2008 – Information technology – Security techniques – Information security risk management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

ISO/IEC 16085:2006 – Systems and software engineering – Lifecycle processes – Risk management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40723

Control Objectives for Information and related Technology – COBIT
http://www.isaca.org/cobit

Australia/New Zealand Risk Management Standard – AS/NZ 4360:2004
http://www.riskmanagement.com.au/
http://www.saiglobal.com/shop/script/details.asp?docn=AS0733759041AT

Institute of Risk Management (IRM) Risk Management Standard
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Carnegie Mellon Software Engineering Institute
Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC)
http://www.sei.cmu.edu/publications/documents/07.reports/07tn008.html

Governmental CIP Programs and Risk Assessment Initiatives

United States Department of Homeland Security
National Infrastructure Protection Plan – IT Sector Specific Plan
http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf

United States Department of Homeland Security
National Infrastructure Protection Plan – Communications Sector Specific Plan
http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf

United Kingdom Centre for the Protection of National Infrastructure (CPNI)
http://www.cpni.gov.uk/default.aspx

Australian Government Critical Infrastructure Protection Program
http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection

Australian Government Trusted Information Sharing Network (TISN)
http://www.tisn.gov.au/

United Kingdom National Risk Assessment
http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx

United Kingdom Centre for the Protection of National Infrastructure (CPNI) Good Practice Framework for SCADA
http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

European Network and Information Security Agency (ENISA) Risk Management
http://www.enisa.europa.eu/rmra/rm_home.html

Microsoft
Trustworthy Computing

Global Security Strategy and Diplomacy

cipteam@microsoft.com
http://www.microsoft.com/twc