Software Engineering Institute

A Taxonomy of Operational Cyber Security Risks

James J. Cebula
Lisa R. Young

December 2010

TECHNICAL NOTE
CMU/SEI-2010-TN-028

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (http://www.sei.cmu.edu/library).

Table of Contents

List of Figures

List of Tables

Acknowledgements

We wish to acknowledge David Mundie, James Stevens, and Richard Caralli of the Software Engineering Institute's CERT® Program for their thorough review and input to this document.

Abstract

This report presents a taxonomy of operational cyber security risks that attempts to identify and organize the sources of operational cyber security risk into four *classes*: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events. Each class is broken down into *subclasses*, which are described by their *elements*. This report discusses the harmonization of the taxonomy with other risk and security activities, particularly those described by the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) Special Publications, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) method.

Introduction

Organizations of all sizes in both the public and private sectors are increasingly reliant on information and technology assets, supported by people and facility assets, to successfully execute business processes that, in turn, support the delivery of services. Failure of these assets has a direct, negative impact on the business processes they support. This, in turn, can cascade into an inability to deliver services, which ultimately impacts the organizational mission. Given these relationships, the management of risks to these assets is a key factor in positioning the organization for success.

Operational cyber security risks are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems. This report presents a taxonomy of operational cyber security risks that attempts to identify and organize the sources of operational cyber security risk into four *classes*: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events. Each class is broken down into *subclasses*, which are described by their *elements*. *Operational risks* are defined as those arising due to the actions of people, systems and technology failures, failed internal processes, and external events. The CERT® Program, part of Carnegie Mellon University's Software Engineering Institute (SEI), developed these four classes of operational risk in the CERT® Resilience Management Model [Caralli 2010b], which draws upon the definition of operational risk adopted by the banking sector in the Basel II framework [BIS 2006]. Within the cyber security space, the risk management focus is primarily on operational risks to information and technology assets. People and facility assets are also considered to the extent that they support information and technology assets.

This taxonomy can be used as a tool to assist in the identification of all applicable operational cyber security risks in an organization. Toward that end, this report also discusses the harmonization of the taxonomy with other risk identification and analysis activities such as those described by the Federal Information Security Management Act of 2002 [FISMA 2002], security guidance contained within the National Institute of Standards and Technology (NIST) Special Publications series, and the threat profile concept contained within the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) method.

® CERT and OCTAVE are registered marks owned by Carnegie Mellon University.

℠ Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

Taxonomy of Operational Cyber Security Risks

The taxonomy of operational cyber security risks, summarized in Table 1 and detailed in this section, is structured around a hierarchy of classes, subclasses, and elements. The taxonomy has four main *classes*:

- actions of people—action, or lack of action, taken by people either deliberately or accidentally that impact cyber security
- systems and technology failures—failure of hardware, software, and information systems
- failed internal processes—problems in the internal business processes that impact the ability to implement, manage, and sustain cyber security, such as process design, execution, and control
- external events—issues often outside the control of the organization, such as disasters, legal issues, business issues, and service provider dependencies

Each of these four classes is further decomposed into *subclasses*, and each subclass is described by its *elements*. The structure of this taxonomy is derived from risk taxonomies previously developed by the SEI in the engineered systems operations [Gallagher 2005] and high-performance computing software development [Kendall 2007] subject areas.

Additionally, this taxonomy complements the Department of Homeland Security (DHS) Risk Lexicon [DHS 2008] by describing instances of operational cyber security risks in greater detail. These risks are a small subset of the universe of risks of concern to DHS and covered by its lexicon.

It is important to note that risks can cascade: risks in one class can trigger risks in another class. In this case, the analysis of a particular risk may involve several elements from different classes. For example, a software failure due to improper security settings could be caused by any of the elements of inadvertent or deliberate actions of people.

Table 1: Taxonomy of Operational Risk

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent 1.1.1 Mistakes 1.1.2 Errors 1.1.3 Omissions **1.2 Deliberate** 1.2.1 Fraud 1.2.2 Sabotage 1.2.3 Theft 1.2.4 Vandalism **1.3 Inaction** 1.3.1 Skills 1.3.2 Knowledge 1.3.3 Guidance 1.3.4 Availability	**2.1 Hardware** 2.1.1 Capacity 2.1.2 Performance 2.1.3 Maintenance 2.1.4 Obsolescence **2.2 Software** 2.2.1 Compatibility 2.2.2 Configuration management 2.2.3 Change control 2.2.4 Security settings 2.2.5 Coding practices 2.2.6 Testing **2.3 Systems** 2.3.1 Design 2.3.2 Specifications 2.3.3 Integration 2.3.4 Complexity	**3.1 Process design or execution** 3.1.1 Process flow 3.1.2 Process documentation 3.1.3 Roles and responsibilities 3.1.4 Notifications and alerts 3.1.5 Information flow 3.1.6 Escalation of issues 3.1.7 Service level agreements 3.1.8 Task hand-off **3.2 Process controls** 3.2.1 Status monitoring 3.2.2 Metrics 3.2.3 Periodic review 3.2.4 Process ownership **3.3 Supporting processes** 3.3.1 Staffing 3.3.2 Funding 3.3.3 Training and development 3.3.4 Procurement	**4.1 Disasters** 4.1.1 Weather event 4.1.2 Fire 4.1.3 Flood 4.1.4 Earthquake 4.1.5 Unrest 4.1.6 Pandemic **4.2 Legal issues** 4.2.1 Regulatory compliance 4.2.2 Legislation 4.2.3 Litigation **4.3 Business issues** 4.3.1 Supplier failure 4.3.2 Market conditions 4.3.3 Economic conditions **4.4 Service dependencies** 4.4.1 Utilities 4.4.2 Emergency services 4.4.3 Fuel 4.4.4 Transportation

Class 1 Actions of People

Actions of people describes a class of operational risk characterized by problems caused by the action taken or not taken by individuals in a given situation. This class covers actions by both insiders and outsiders. Its supporting subclasses include *inadvertent* actions (generally by insiders), *deliberate* actions (by insiders or outsiders), and *inaction* (generally by insiders).

Subclass 1.1 Inadvertent

The *inadvertent* subclass refers to unintentional actions taken without malicious or harmful intent. Inadvertent actions are usually, though not exclusively, associated with an individual internal to the organization. This subclass is composed of the elements *mistakes*, *errors*, and *omissions*.

1.1.1 mistake—individual with knowledge of the correct procedure accidentally taking incorrect action

1.1.2 error—individual without knowledge of the correct procedure taking incorrect action

1.1.3 omission—individual not taking a known correct action often due to hasty performance of a procedure

Subclass 1.2 Deliberate

The *deliberate* subclass of actions of people describes actions taken intentionally and with intent to do harm. This subclass is described by the elements *fraud*, *sabotage*, *theft*, and *vandalism*. Deliberate actions could be carried out by either insiders or outsiders.

1.2.1 fraud—a deliberate action taken to benefit oneself or a collaborator at the expense of the organization

1.2.2 sabotage—a deliberate action taken to cause a failure in an organizational asset or process, generally carried out against targeted key assets by someone possessing or with access to inside knowledge

1.2.3 theft—the intentional, unauthorized taking of organizational assets, in particular information assets

1.2.4 vandalism—the deliberate damaging of organizational assets, often at random

Subclass 1.3 Inaction

The *inaction* subclass describes a lack of action or failure to act upon a given situation. Elements of *inaction* include a failure to act because of a lack of appropriate *skills*, a lack of *knowledge*, a lack of *guidance*, and a lack of *availability* of the correct person to take action.

1.3.1 skills—an individual's lack of ability to undertake the necessary action

1.3.2 knowledge—an individual's ignorance of the need to take action

1.3.3 guidance—a knowledgeable individual lacking the proper guidance or direction to act

1.3.4 availability—the unavailability or nonexistence of the appropriate resource needed to carry out the action

Class 2 Systems and Technology Failures

Systems and technology failures describes a class of operational risk characterized by problematic abnormal or unexpected functioning of technology assets. Its supporting subclasses include failures of *hardware*, *software*, and integrated *systems*.

Subclass 2.1 Hardware

The *hardware* subclass addresses risks traceable to failures in physical equipment due to *capacity*, *performance*, *maintenance*, and *obsolescence*.

2.1.1 capacity—inability to handle a given load or volume of information

2.1.2 performance—inability to complete instructions or process information within acceptable parameters (speed, power consumption, heat load, etc.)

2.1.3 maintenance—failure to perform required or recommended upkeep of the equipment

2.1.4 obsolescence—operation of the equipment beyond its supported service life

Subclass 2.2 Software

The *software* subclass addresses risks stemming from software assets of all types, including programs, applications, and operating systems. The elements of software failures are *compatibility*, *configuration management*, *change control*, *security settings*, *coding practices,* and *testing*.

2.2.1 compatibility—inability of two or more pieces of software to work together as expected

2.2.2 configuration management—improper application and management of the appropriate settings and parameters for the intended use

2.2.3 change control—changes made to the application or its configuration by a process lacking appropriate authorization, review, and rigor

2.2.4 security settings—improper application of security settings, either too relaxed or too restrictive, within the program or application

2.2.5 coding practices—failures due to programming errors, including syntax and logic problems and failure to follow secure coding practices

2.2.6 testing—inadequate or atypical testing of the software application or configuration

Subclass 2.3 Systems

The *systems* subclass deals with failures of integrated systems to perform as expected. Systems failures are described by the elements *design*, *specifications*, *integration*, and *complexity*.

2.3.1 design—improper fitness of the system for the intended application or use

2.3.2 specifications—improper or inadequate definition of requirements or failure to adhere to the requirements during system construction

2.3.3 integration—failure of various components of the system to function together or interface correctly; also includes inadequate testing of the system

2.3.4 complexity—system intricacy or a large number or interrelationships between components

Class 3 Failed Internal Processes

Failed internal processes describes a class of operational risk associated with problematic failures of internal processes to perform as needed or expected. Its supporting subclasses include *process design or execution*, *process controls*, and *supporting processes*.

Subclass 3.1 Process Design or Execution

The *process design or execution* subclass deals with failures of processes to achieve their desired outcomes due to process design that is improper for the task or due to poor execution of a properly designed process. The elements of process design or execution are *process flow*, *process documentation*, *roles and responsibilities*, *notifications and alerts*, *information flow*, *escalation of issues*, *service level agreements*, and *task hand-off*.

3.1.1 process flow—poor design of the movement of process outputs to their intended consumers

3.1.2 process documentation—inadequate documentation of the process inputs, outputs, flow, and stakeholders

3.1.3 roles and responsibilities—insufficient definition and understanding of process stakeholder roles and responsibilities

3.1.4 notifications and alerts—inadequate notification regarding a potential process problem or issue

3.1.5 information flow—poor design of the movement of process information to interested parties and stakeholders

3.1.6 escalation of issues—the inadequate or nonexistent ability to escalate abnormal or unexpected conditions for action by appropriate personnel

3.1.7 service level agreements—the lack of agreement among process stakeholders on service expectations that causes a failure to complete expected actions

3.1.8 task hand-off—"dropping the ball" due to the inefficient handing off of a task in progress from one responsible party to another

Subclass 3.2 Process Controls

The *process controls* subclass addresses process failures due to inadequate controls on the operation of the process. The elements of this subclass are *status monitoring*, *metrics*, *periodic review*, and *process ownership*.

3.2.1 status monitoring—failure to review and respond to routine information about the operation of a process

3.2.2 metrics—failure to review process measurements over time for the purpose of determining performance trends

3.2.3 periodic review—failure to review the end-to-end operation of the process on a periodic basis and make any needed changes

3.2.4 process ownership—failure of a process to deliver the expected outcome because of poor definition of its ownership or poor governance practices

Subclass 3.3 Supporting Processes

The *supporting processes* subclass deals with operational risks introduced due to failure of organizational supporting processes to deliver the appropriate resources. The supporting processes of concern are the elements *staffing*, *accounting, training and development*, and *procurement*.

3.3.1 staffing—failure to provide appropriate human resources to support its operations

3.3.2 funding—failure to provide appropriate financial resources to support its operations

3.3.3 training and development—Failure to maintain the appropriate skills within the workforce

3.3.4 procurement—failure to provide the proper purchased service and goods necessary to support operations

Class 4 External Events

External events describes a class of operational risk associated with events generally outside the organization's control. Often the timing or occurrence of such events cannot be planned or predicted. The supporting subclasses of this class include *disasters*, *legal issues*, *business issues*, and *service dependencies*.

Subclass 4.1 Hazards

The *hazards* subclass deals with risks owing to events, both natural and of human origin, over which the organization has no control and that can occur without notice. The elements supporting this subclass include *weather event*, *fire*, *flood*, *earthquake*, *unrest*, and *pandemic*.

4.1.1 weather event—adverse weather situations such as rain, snow, tornado, or hurricane

4.1.2 fire—fire within a facility or disruption caused by a fire external to a facility

4.1.3 flood—flooding within a facility or disruption caused by a flood external to a facility

4.1.4 earthquake—disruption of organizational operations due to an earthquake

4.1.5 unrest—disruption of operations due to civil disorder, riot, or terrorist acts

4.1.6 pandemic—widespread medical conditions that disrupt organizational operations

Subclass 4.2 Legal Issues

The *legal issues* subclass deals with risks potentially impacting the organization due to the elements *regulatory compliance*, *legislation*, and *litigation*.

4.2.1 regulatory compliance—new governmental regulation or failure to comply with existing regulation

4.2.2 legislation—new legislation that impacts the organization

4.2.3 litigation—legal action taken against the organization by any stakeholder, including employees and customers

Subclass 4.3 Business Issues

The *business issues* subclass, described by the elements of *supplier failure*, *market conditions*, and *economic conditions*, deals with operational risks arising from changes in the business environment of the organization.

4.3.1 supplier failure—the temporary or permanent inability of a supplier to deliver needed products or services to the organization

4.3.2 market conditions—the diminished ability of the organization to sell its products and services in the market

4.3.3 economic conditions—the inability of the organization to obtain needed funding for its operations

Subclass 4.4 Service Dependencies

The *service dependencies* subclass deals with risks arising from the organization's dependence on external parties to continue operations. The subclass is associated with the elements of *utilities*, *emergency services*, *fuel*, and *transportation*.

4.4.1 utilities—failure of the organization's electric power supply, water supply, or telecommunications services

4.4.2 emergency services—dependencies on public response services such as fire, police, and emergency medical services

4.4.3 fuel—failure of external fuel supplies, for example to power a backup generator

4.4.4 transportation—failures in external transportation systems, for example, inability of employees to report to work and inability to make and receive deliveries

Harmonization with Other Risk Practices

The taxonomy can be used as a tool to help identify all applicable operational cyber security risks in an organization. To provide context and prioritize and manage these risks in a structured manner, a basic understanding of the relationships among assets, business processes, and services needs to be established. Assets are the basic units of value in the organization. There are four primary types of assets: people, information, facilities, and technology. In the cyber security arena, the primary focus is on operational risks to information and technology assets, although people and facility assets are also considered. Assets are the building blocks of business processes. Business processes are the activities that support the organization's delivery of services. The relationships among assets, business processes, and services are shown in Figure 1.

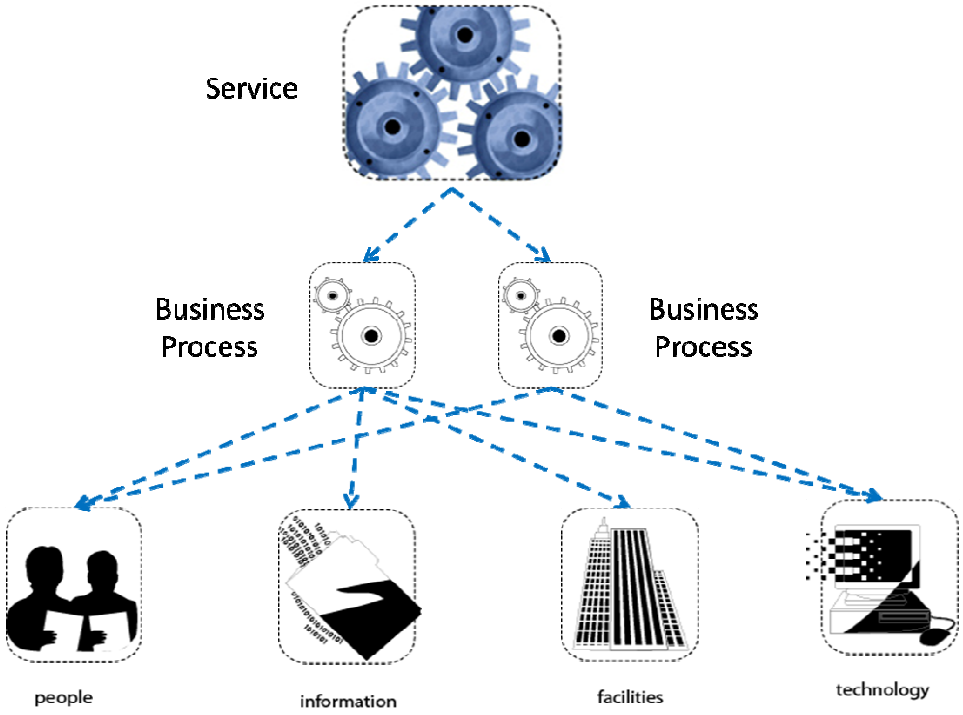

Figure 1: Relationships Among Assets, Business Processes, and Services [Caralli 2010a]

Failure of these assets can have a direct, negative impact on the business processes that they support. This, in turn, cascades into an inability to deliver services and ultimately impacts the mission of the organization. The taxonomy can assist in identifying operational risks in all four classes (*actions of people*, *systems and technology failures*, *failed internal processes*, and *external events*) to each of the four asset types.

Risk management involves a balance between risk conditions (such as threats and vulnerabilities) and risk consequences. As part of a risk management strategy, protective and sustaining controls are applied to assets, as shown in Figure 2.

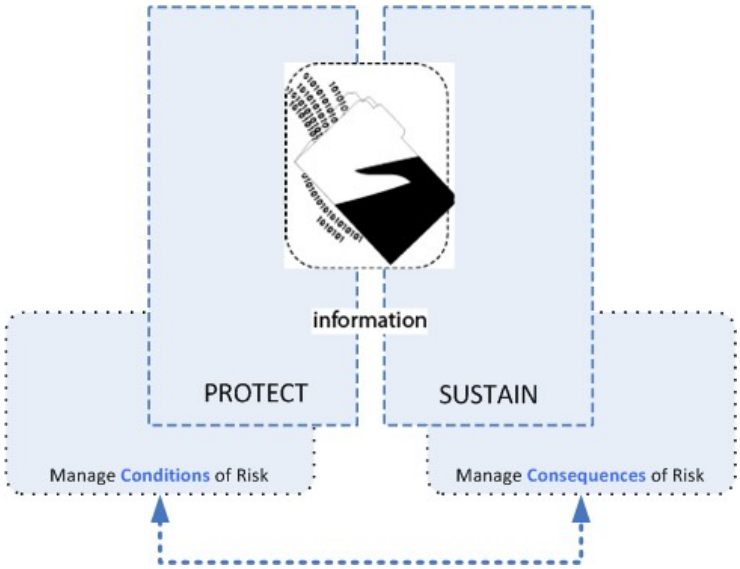

Figure 2: Protection, Sustainability, and Risk [Caralli 2010a]

Protective controls are intended to help manage risk conditions, while sustaining controls are intended to help manage risk consequences. In both cases, controls are applied at the asset level.

FISMA

The taxonomy provides a structured set of terms that covers all of the significant risk elements that could impact cyber security operations. The Federal Information Security Management Act of 2002 (FISMA), which applies to U.S. federal government agencies, provides a working definition of information security. This definition links the identified operational cyber security risks to specific examples of consequences impacting confidentiality, integrity, and availability. This is an important building block in the control selection and risk mitigation process. The FISMA definition of information security reads as follows:

> *The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—*
>
> *(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity;*
>
> *(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;*
>
> *and*
>
> *(C) availability, which means ensuring timely and reliable access to and use of information.*

NIST Special Publications

In addition to providing the definition of information security described above, the FISMA legislation also tasked the National Institute of Standards and Technology (NIST) with developing information security guidelines for use by federal agencies. These guidelines are known as the

NIST Special Publications (SP). Of particular interest is NIST SP 800-53 rev. 3 [NIST 2009], which provides a control catalog to be applied to federal information systems based on an analysis of the system's relative importance and consequence of loss. The controls specified in NIST SP 800-53 are primarily protective in nature and are applied tactically at the information-system level. In general, the controls specified in NIST SP 800-53 are at a lower level than the elements in the taxonomy. The taxonomy can be used as a tool to link the application of these controls into a broader risk management strategy. A mapping of the control catalog in NIST SP 800-53 rev. 3 to the risk subclasses identified in the taxonomy is provided in Appendix A. This appendix can be used to match NIST control families to types of operational cyber security risk. Appendix B provides the reverse: a mapping of taxonomy subclasses to the NIST SP 800-53 rev. 3 control catalog. Appendix B can be used to determine which NIST controls to consider in order to mitigate specific operational cyber security risks.

SEI OCTAVE Threat Profiles

The OCTAVE method, developed by the SEI [Alberts 2001a], provides a process for an organization to perform a comprehensive security risk evaluation. Phase 1 of the OCTAVE method uses the concept of asset-based threat profiles [Alberts 2001b]. While it is not the intent of this report to provide a detailed discussion of OCTAVE, the threat profiles are introduced here as a useful, graphical vehicle to link assets to risks and consequences, in-line with the definition of operational security risks. OCTAVE uses four standard threat categories: (1) human actors using network access, (2) human actors using physical access, (3) system problems, and (4) other problems. These generic categories can easily be extended or tailored to suit the particular need. In general, the threat categories from OCTAVE align with the classes in the risk taxonomy as follows:

- humans with network access – *actions of people* class
- humans with physical access – *actions of people* class
- system problems – *systems and technology failures* class
- other problems – *failed internal processes* and *external events* classes

The threat profiles are represented graphically in a tree structure. Figure 3 through Figure 6 below illustrate the OCTAVE generic threat profiles for the four threat categories. The taxonomy and the techniques described in OCTAVE can serve as cross-checks to each other to ensure coverage of all classes of operational cyber security risk.

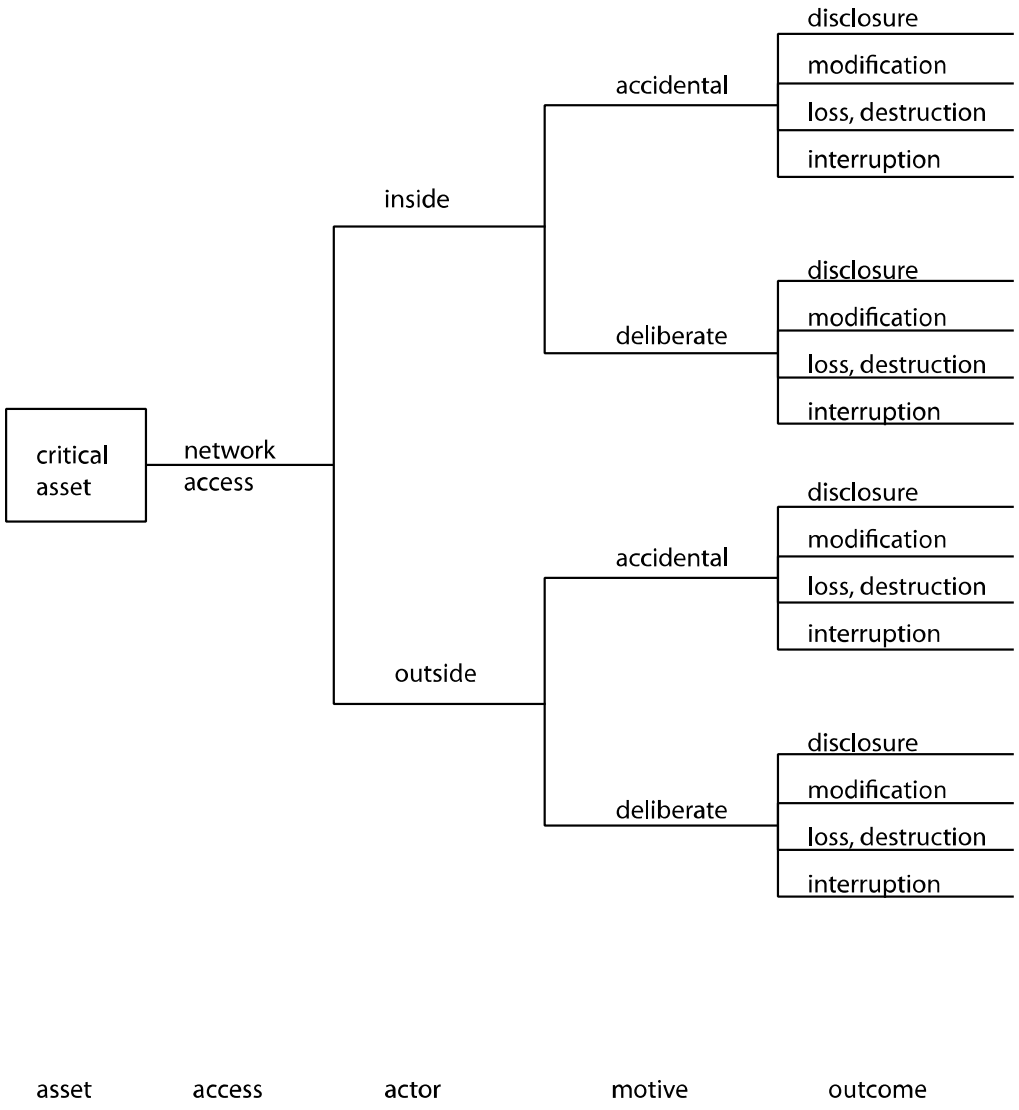

Figure 3: OCTAVE Generic Threat Profile for Human Actors Using Network Access [Alberts 2001b]

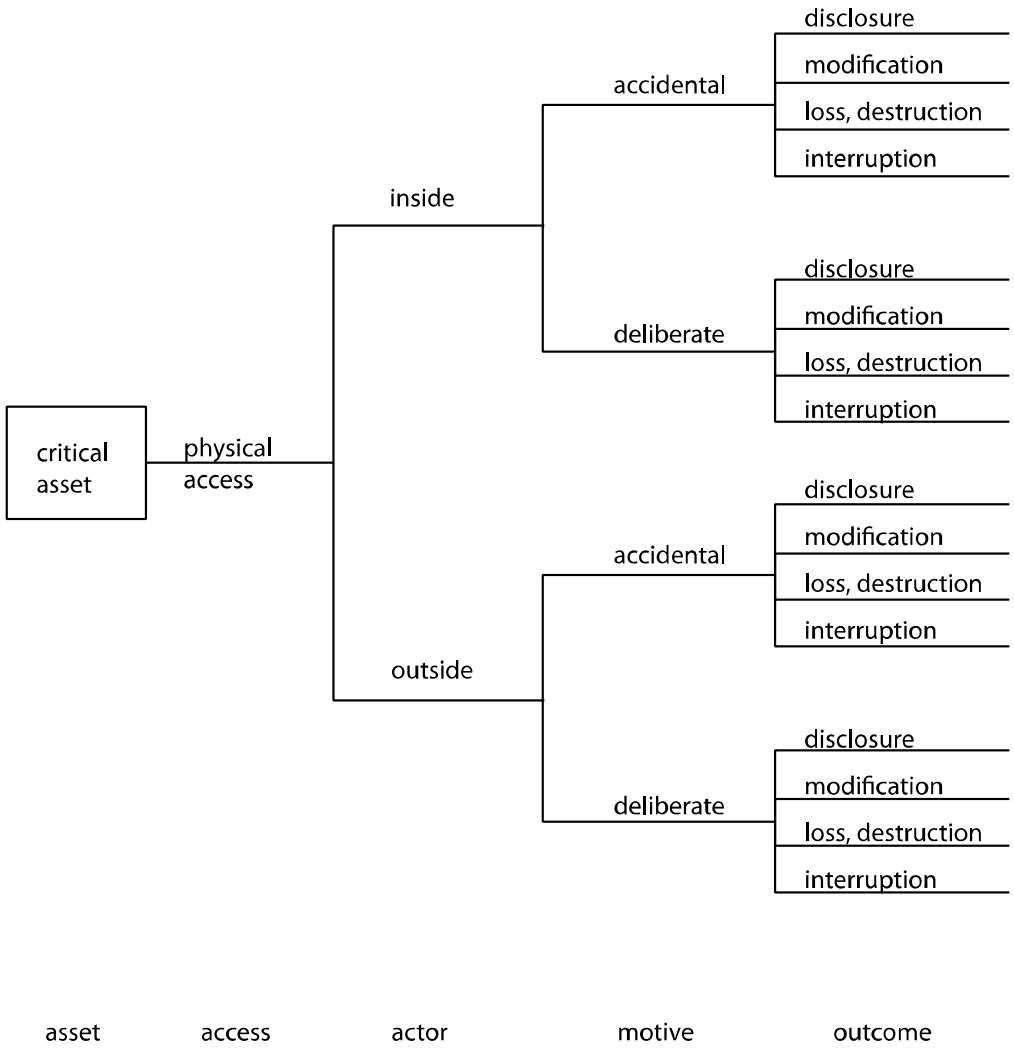

Figure 4: OCTAVE Generic Threat Profile for Human Actors Using Physical Access [Alberts 2001b]

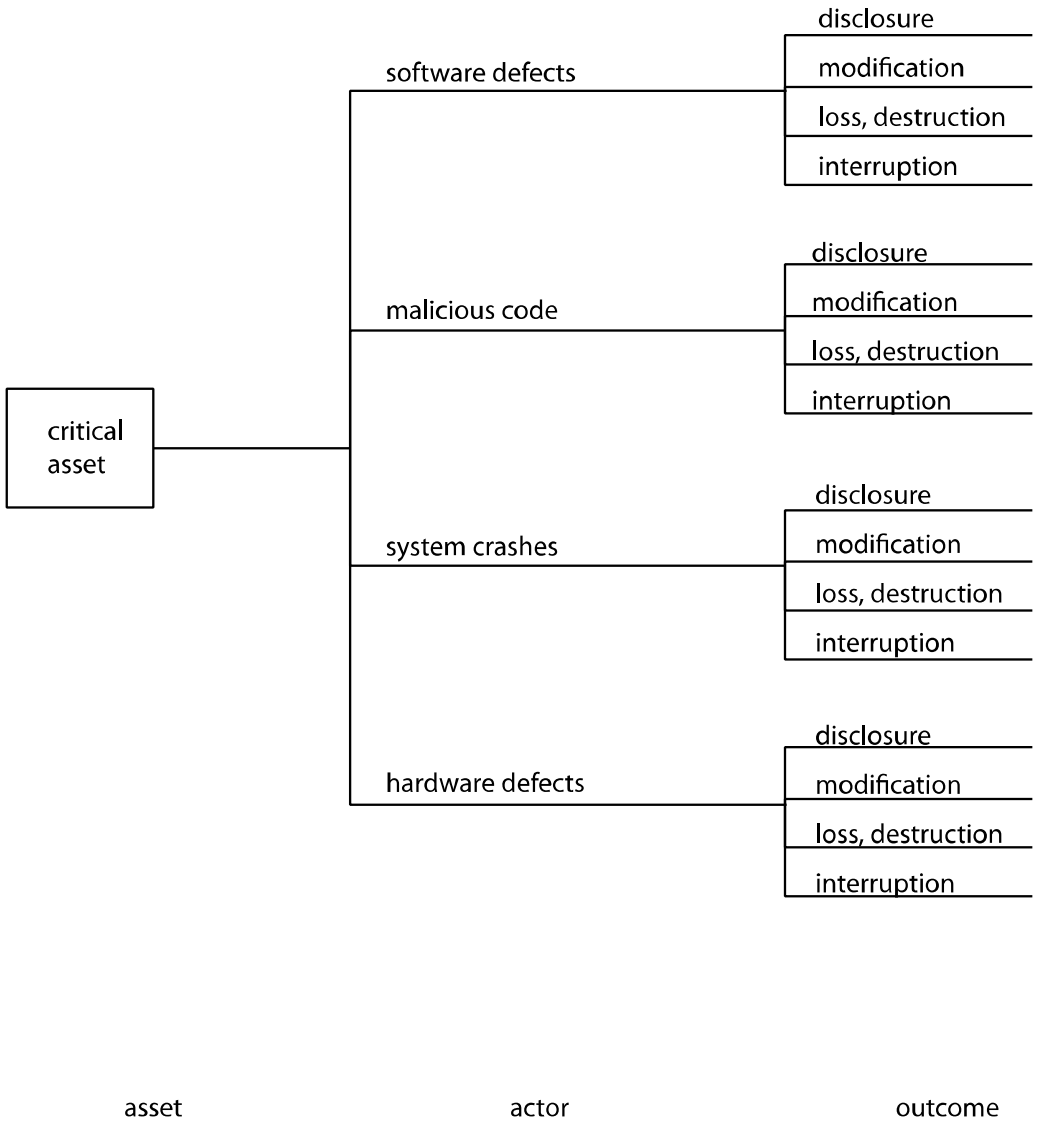

Figure 5: OCTAVE Generic Threat Profile for System Problems [Alberts 2001b]

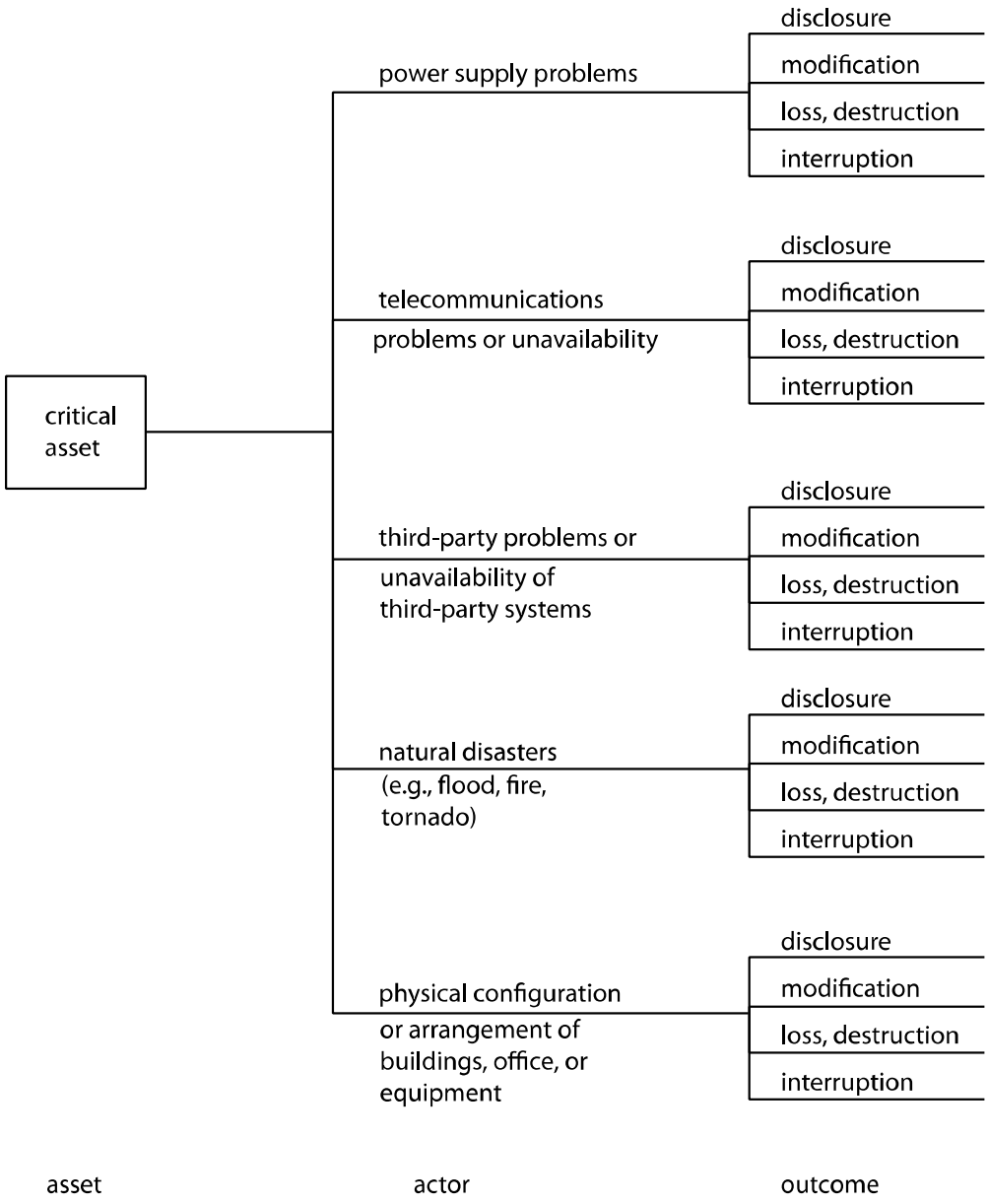

Figure 6: OCTAVE Generic Threat Profile for Other Problems [Alberts 2001b]

Conclusion

This report presents a taxonomy of operational cyber security risks and also discusses the relationship of the taxonomy to other risk and security activities. The taxonomy organizes the definition of operational risk into the following four classes: (1) *actions of people*, (2) *systems and technology failures*, (3) *failed internal processes*, and (4) *external events*. Each of these four classes is further decomposed into subclasses and elements. Operational cyber security risks are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and integrity of information and information systems. The relationship of operational risks to consequences is discussed in the context of FISMA, the NIST Special Publications, and the OCTAVE method.

We anticipate that revisions to the taxonomy will be necessary to account for changes in the cyber risk landscape. The present taxonomy is being validated through fieldwork with organizations under varying levels of regulatory compliance obligation and risk tolerance. The results of this fieldwork will inform taxonomy revisions.

Appendix A: Mapping of NIST SP 800-53 Rev. 3 Controls to Selected Taxonomy Subclasses and Elements

Table 2 can be used to match NIST control families to types of operational cyber security risk.

References to taxonomy subclasses and elements refer to the numbering scheme shown in Table 1 and the body of this report. For example, item 1.1 refers to the subclass *inadvertent actions of people* (all elements apply), and item 2.2.2 refers to the *configuration management* element of *systems and technology failures – software*.

Table 2: Mapping of NIST Control Families to Selected Taxonomy Subclasses and Elements

NIST SP 800-53 Rev. 3		***Taxonomy Subclasses and Elements***
Control Number	***Control Description***	
AC-1	Access Control Policy and Procedures	3.1
AC-2	Account Management	1.1, 1.2, 2.2.2, 2.2.3
AC-3	Access Enforcement	1.1, 2.2, 2.3
AC-4	Information Flow Enforcement	1.1, 2.2, 2.3
AC-5	Separation of Duties	1.1, 1.2, 2.2.2, 2.2.3, 2.2.4, 2.3.2, 3.1, 3.2
AC-6	Least Privilege	1.1, 1.2, 2.2.2, 2.2.3, 2.2.4, 2.3.2, 3.1, 3.2
AC-7	Unsuccessful Login Attempts	2.2, 2.3
AC-8	System Use Notification	2.2, 2.3
AC-9	Previous Logon (Access) Notification	2.2, 2.3
AC-10	Concurrent Session Control	2.2, 2.3
AC-11	Session Lock	2.2, 2.3
AC-12	*Withdrawn*	*N/A*
AC-13	*Withdrawn*	*N/A*
AC-14	Permitted Actions Without Identification or Authentication	2.2, 3.1
AC-15	*Withdrawn*	*N/A*
AC-16	Security Elements	1.1, 1.2, 2.3, 3.1
AC-17	Remote Access	1.2, 2.1, 2.2, 3.1, 3.2

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
AC-18	Wireless Access	1.2, 2.1, 2.2, 3.1, 3.2
AC-19	Access Control for Mobile Devices	1.1, 1.2, 2.1, 2.2, 3.1, 4.2
AC-20	Use of External Information Systems	1.1, 1.2, 3.1, 3.3.4, 4.3
AC-21	User-Based Collaboration and Information Sharing	1.1, 1.2, 3.1, 3.2, 3.3.3
AC-22	Publicly Accessible Content	1.1, 1;2, 3.1, 3.3.3
AT-1	Security Awareness and Training Policy and Procedures	3.1, 3.3.3
AT-2	Security Awareness	1.3.2, 1.3.3, 3.1, 3.3.3
AT-3	Security Training	1.3.1, 1.3.3, 3.1, 3.3.3, 4.1
AT-4	Security Training Records	1.2, 3.1, 3.3.3
AT-5	Contacts with Security Groups and Associations	1.3.1, 1.3.2
AU-1	Audit and Accountability Policy and Procedures	1.1, 1.2, 3.2, 4.2.1, 4.2.2
AU-2	Auditable Events	1.1, 1.2, 3.1, 3.2, 4.2.1, 4.2.2
AU-3	Content of Audit Records	1.1, 1.2, 3.1, 3.2
AU-4	Audit Storage Capacity	2.1.1
AU-5	Response to Audit Processing Failures	1.1, 1.2, 3.2
AU-6	Audit Review, Analysis, and Reporting	3.2
AU-7	Audit Reduction and Report Generation	2.2, 2.3, 3.1
AU-8	Time Stamps	2.2, 2.3
AU-9	Protection of Audit Information	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
AU-10	Non-Repudiation	1.1, 1.2, 2.2, 2.3, 3.2
AU-11	Audit Record Retention	3.1, 3.2
AU-12	Audit Generation	2.2, 2.3, 3.1

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
AU-13	Monitoring for Information Disclosure	3.1, 3.2, 4.2
AU-14	Session Audit	2.2, 2.3
CA-1	Security Assessment and Authorization Policies and Procedures	1.1, 1.2, 3.1, 3.2
CA-2	Security Assessments	1.1, 1.2, 3.1, 3.2
CA-3	Information System Connections	1.1, 1.2, 3.1
CA-4	*Withdrawn*	*N/A*
CA-5	Plan of Action and Milestones	1.3, 2.2, 3.1, 3.2, 3.3
CA-6	Security Authorization	3.1, 3.2
CA-7	Continuous Monitoring	2.2, 2.3, 3.2
CM-1	Configuration Management Policy and Procedures	2.2.2, 2.2.3, 2.2.4, 3.1, 3.2
CM-2	Baseline Configuration	2.2.2, 2.2.3, 2.2.4, 3.1, 3.2
CM-3	Configuration Change Control	2.2.2, 2.2.3, 2.2.4, 3.1, 3.2
CM-4	Security Impact Analysis	2.2.2, 2.2.3, 2.2.4, 2.2.5, 3.1
CM-5	Access Restrictions for Change	1.1, 1.2, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 3.1
CM-6	Configuration Settings	2.2.2, 2.2.3, 2.2.4, 3.1, 3.2
CM-7	Least Functionality	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
CM-8	Information System Component Inventory	2.1, 2.2, 2.3, 3.1
CM-9	Configuration Management Plan	2.2.2, 2.3
CP-1	Contingency Planning Policy and Procedures	3.1, 3.2, 4.1, 4.3, 4.4
CP-2	Contingency Plan	1.2, 1.3, 3.3, 4.1, 4.2, 4.3, 4.4
CP-3	Contingency Training	1.3, 3.3.3, 4.1, 4.4
CP-4	Contingency Plan Testing and Exercises	1.3, 3.1, 3.3.3, 4.1, 4.2, 4.3, 4.4
CP-5	*Withdrawn*	*N/A*

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
CP-6	Alternate Storage Site	2.1, 2.2, 4.1, 4.3
CP-7	Alternate Processing Site	2.1, 2.2, 2.3, 4.1, 4.4
CP-8	Telecommunications Services	2.2, 2.3, 3.3, 4.1, 4.2, 4.3
CP-9	Information System Backup	2.2, 2.3, 3.1
CP-10	Information System Recovery and Reconstitution	3.1, 4.1, 4.2, 4.3
IA-1	Identification and Authentication Policy and Procedures	1.1, 1.2, 2.2, 2.3, 3.1
IA-2	Identification and Authentication (Organizational Users)	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
IA-3	Device Identification and Authentication	1.1, 1.2, 2.1, 2.3, 3.1, 3.2
IA-4	Identifier Management	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
IA-5	Authenticator Management	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
IA-6	Authenticator Feedback	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
IA-7	Cryptographic Module Authentication	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
IA-8	Identification and Authentication (Non-Organizational Users)	1.1, 1.2, 2.2, 2.3, 3.1, 3.2, 4.2, 4.3
IR-1	Incident Response Policy and Procedures	1.1, 1.2, 1.3, 3.1, 3.2
IR-2	Incident Response Training	1.3, 3.3.3
IR-3	Incident Response Testing and Exercises	1.1, 1.2, 1.3, 3.1, 3.2
IR-4	Incident Handling	1.1, 1.2, 1.3, 3.1, 3.2
IR-5	Incident Monitoring	1.1, 1.2, 1.3, 3.1, 3.2
IR-6	Incident Reporting	1.1, 1.2, 1.3, 3.1, 3.2. 4.2
IR-7	Incident Response Assistance	1.1, 1.2, 1.3, 3.1, 3.2, 3.3.4
IR-8	Incident Response Plan	1.1, 1.2, 1.3, 3.1, 3.2
MA-1	System Maintenance Policy and Procedures	2.1.3, 2.3, 3.1, 3.2

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
MA-2	Controlled Maintenance	1.1, 1.3, 2.1.3, 2.3, 3.1, 3.2, 3.3
MA-3	Maintenance Tools	1.1, 1.3, 2.1.3, 2.3, 3.1, 3.2, 3.3
MA-4	Non-Local Maintenance	1.1, 1.3, 2.1.3, 2.3, 3.1, 3.2, 3.3
MA-5	Maintenance Personnel	1.1, 1.3, 2.1.3, 2.3, 3.1, 3.2, 3.3, 4.3
MA-6	Timely Maintenance	1.1, 1.3, 2.1.3, 2.3, 3.1, 3.2, 3.3
MP-1	Media Protection Policy and Procedures	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
MP-2	Media Access	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
MP-3	Media Marking	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
MP-4	Media Storage	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
MP-5	Media Transport	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
MP-6	Media Sanitization	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.2
PE-1	Physical and Environmental Protection Policy and Procedures	1.1, 1.2, 2.1, 3.1, 3.2
PE-2	Physical Access Authorizations	1.1, 1.2, 2.1, 3.1, 3.2
PE-3	Physical Access Control	1.1, 1.2, 2.1, 3.1, 3.2
PE-4	Access Control for Transmission Medium	1.1, 1.2, 2.1, 3.1, 3.2
PE-5	Access Control for Output Devices	1.1, 1.2, 2.1, 3.1, 3.2
PE-6	Monitoring Physical Access	1.1, 1.2, 2.1, 3.1, 3.2
PE-7	Visitor Control	1.1, 1.2, 2.1, 3.1, 3.2
PE-8	Access Records	1.1, 1.2, 2.1, 3.1, 3.2
PE-9	Power Equipment and Power Cabling	1.1, 1.2, 2.1, 3.1, 3.2
PE-10	Emergency Shutoff	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-11	Emergency Power	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-12	Emergency Lighting	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-13	Fire Protection	1.1, 1.2, 2.1, 3.1, 3.2, 4.1.2, 4.4

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
PE-14	Temperature and Humidity Controls	1.1, 1.2, 2.1, 3.1, 3.2
PE-15	Water Damage Protection	1.1, 1.2, 2.1, 3.1, 3.2, 4.1.3, 4.4
PE-16	Delivery and Removal	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-17	Alternate Work Site	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-18	Location of Information System Components	1.1, 1.2, 2.1, 3.1, 3.2, 4.1, 4.4
PE-19	Information Leakage	1.1, 1.2, 2.1, 3.1, 3.2, 4.2
PL-1	Security Planning Policy and Procedures	3.1, 3.2, 3.3
PL-2	System Security Plan	3.1, 3.2, 3.3
PL-3	*Withdrawn*	*N/A*
PL-4	Rules of Behavior	1.1, 1.2, 1.3, 3.3.3
PL-5	Privacy Impact Assessment	4.2, 4.3
PL-6	Security-Related Activity Planning	3.1, 3.2, 3.3
PS-1	Personnel Security Policy and Procedures	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-2	Position Categorization	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-3	Personnel Screening	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-4	Personnel Termination	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-5	Personnel Transfer	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-6	Access Agreements	1.1, 1.2, 1.3, 3.3.3, 4.2
PS-7	Third-Party Personnel Security	1.1, 1.2, 1.3, 3.3.3, 4.3
PS-8	Personnel Sanctions	1.1, 1.2, 1.3, 3.3.3, 4.2
RA-1	Risk Assessment Policy and Procedures	3.1, 3.2
RA-2	Security Categorization	3.1, 3.2, 4.2, 4.3
RA-3	Risk Assessment	3.1, 3.2, 4.2, 4.3
RA-4	*Withdrawn*	*N/A*
RA-5	Vulnerability Scanning	1.1, 1.2, 1.3, 2.2.4, 3.1, 3.2

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
SA-1	System and Services Acquisition Policy and Procedures	2.3, 3.3.4, 4.4
SA-2	Allocation of Resources	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-3	Life Cycle Support	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-4	Acquisitions	2.3, 3.3.4, 4.4
SA-5	Information System Documentation	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-6	Software Usage Restrictions	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-7	User-Installed Software	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-8	Security Engineering Principles	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-9	External Information System Services	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-10	Developer Configuration Management	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-11	Developer Security Testing	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-12	Supply Chain Protections	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-13	Trustworthiness	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SA-14	Critical Information System Components	2.1, 2.2, 2.3, 3.3, 4.2, 4.3
SC-1	System and Communications Protection Policy and Procedures	1.1, 1.2, 2.1, 2.2, 2.3
SC-2	Application Partitioning	1.1, 1.2, 2.1, 2.2, 2.3
SC-3	Security Function Isolation	1.1, 1.2, 2.1, 2.2, 2.3
SC-4	Information in Shared Resources	1.1, 1.2, 2.1, 2.2, 2.3
SC-5	Denial of Service Protection	1.1, 1.2, 2.1, 2.2, 2.3
SC-6	Resource Priority	1.1, 1.2, 2.1, 2.2, 2.3
SC-7	Boundary Protection	1.1, 1.2, 2.1, 2.2, 2.3
SC-8	Transmission Integrity	1.1, 1.2, 2.1, 2.2, 2.3
SC-9	Transmission Confidentiality	1.1, 1.2, 2.1, 2.2, 2.3
SC-10	Network Disconnect	1.1, 1.2, 2.1, 2.2, 2.3

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
SC-11	Trusted Path	1.1, 1.2, 2.1, 2.2, 2.3
SC-12	Cryptographic Key Establishment and Management	1.1, 1.2, 2.1, 2.2, 2.3
SC-13	Use of Cryptography	1.1, 1.2, 2.1, 2.2, 2.3
SC-14	Public Access Protections	1.1, 1.2, 2.1, 2.2, 2.3
SC-15	Collaborative Computing Devices	1.1, 1.2, 2.1, 2.2, 2.3
SC-16	Transmission of Security Elements	1.1, 1.2, 2.1, 2.2, 2.3
SC-17	Public Key Infrastructure Certificates	1.1, 1.2, 2.1, 2.2, 2.3
SC-18	Mobile Code	1.1, 1.2, 2.1, 2.2, 2.3
SC-19	Voice Over Internet Protocol	1.1, 1.2, 2.1, 2.2, 2.3
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	1.1, 1.2, 2.1, 2.2, 2.3
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	1.1, 1.2, 2.1, 2.2, 2.3
SC-22	Architecture and Provisioning for Name/Address Resolution Service	1.1, 1.2, 2.1, 2.2, 2.3
SC-23	Session Authenticity	1.1, 1.2, 2.1, 2.2, 2.3
SC-24	Fail in Known State	1.1, 1.2, 2.1, 2.2, 2.3
SC-25	Thin Nodes	1.1, 1.2, 2.1, 2.2, 2.3
SC-26	Honeypots	1.1, 1.2, 2.1, 2.2, 2.3
SC-27	Operating System-Independent Applications	1.1, 1.2, 2.1, 2.2, 2.3
SC-28	Protection of Information at Rest	1.1, 1.2, 2.1, 2.2, 2.3
SC-29	Heterogeneity	1.1, 1.2, 2.1, 2.2, 2.3
SC-30	Virtualization Techniques	1.1, 1.2, 2.1, 2.2, 2.3
SC-31	Covert Channel Analysis	1.1, 1.2, 2.1, 2.2, 2.3
SC-32	Information System Partitioning	1.1, 1.2, 2.1, 2.2, 2.3

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
SC-33	Transmission Preparation Integrity	1.1, 1.2, 2.1, 2.2, 2.3
SC-34	Non-Modifiable Executable Programs	1.1, 1.2, 2.1, 2.2, 2.3
SI-1	System and Information Integrity Policy and Procedures	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-2	Flaw Remediation	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-3	Malicious Code Protection	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-4	Information System Monitoring	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-5	Security Alerts, Advisories, and Directives	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-6	Security Functionality Verification	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-7	Software and Information Integrity	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-8	Spam Protection	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-9	Information Input Restrictions	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-10	Information Input Validation	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-11	Error Handling	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
SI-12	Information Output Handling and Retention	1.1, 1.2, 2.2, 2.3, 3.1, 3.2, 4.2
SI-13	Predictable Failure Prevention	1.1, 1.2, 2.2, 2.3, 3.1, 3.2
PM-1	Information Security Program Plan	3.1, 3.2, 3.3
PM-2	Senior Information Security Officer	3.1, 3.2, 3.3
PM-3	Information Security Resources	3.1, 3.2, 3.3
PM-4	Plan of Action and Milestones Process	3.1, 3.2, 3.3
PM-5	Information System Inventory	3.1, 3.2, 3.3
PM-6	Information Security Measures of Performance	3.1, 3.2, 3.3
PM-7	Enterprise Architecture	3.1, 3.2, 3.3
PM-8	Critical Infrastructure Plan	3.1, 3.2, 3.3
PM-9	Risk Management Strategy	3.1, 3.2, 3.3

NIST SP 800-53 Rev. 3		*Taxonomy Subclasses and Elements*
Control Number	***Control Description***	
PM-10	Security Authorization Process	3.1, 3.2, 3.3
PM-11	Mission/Business Process Definition	3.1, 3.2, 3.3

Appendix B: Mapping of Selected Taxonomy Subclasses and Elements to NIST SP 800-53 Rev. 3 Controls

The following table can be used to determine which NIST controls to consider in order to mitigate a specific operational cyber security risks.

Table 3: Mapping of Taxonomy Subclasses and Elements to NIST Controls

Taxonomy Class, Subclass, Element	**NIST SP 800-53 Rev. 3 Controls**
1 Actions of People	
1.1 Inadvertent	AC – 2-6, 16, 19-22 AU – 1-3, 5, 9-10 CA – 1-3 CM – 5, 7 IA – 1-8 IR – 1, 3-8 MA – 2-6 MP – 1-6 PE – 1-19 PL – 4 PS – 1-8 RA – 5 SC – 1-34 SI – 1-13
1.1.1 Mistakes	
1.1.2 Errors	
1.1.3 Omissions	
1.2 Deliberate	AC – 2, 5-6, 16-18, 19-22 AT – 4 AU – 1-3, 5, 9-10 CA – 1-3 CM – 5, 7 CP – 2 IA – 1-8 IR –1, 3-8 MP – 1-6 PE – 1-19 PL – 4 PS – 1-8 RA – 5 SC – 1-34 SI – 1-13
1.2.1 Fraud	
1.2.2 Sabotage	
1.2.3 Theft	
1.2.4 Vandalism	

Taxonomy Class, Subclass, Element	NIST SP 800-53 Rev. 3 Controls	
1.3 Inaction	CA – 5 CP – 2-4 IR – 1-8 MA – 2-6 PL – 4 PS – 1-8 RA – 5	
1.3.1 Skills		AT – 3, 5
1.3.2 Knowledge		AT – 2, 5
1.3.3 Guidance		AT – 2, 3
1.3.4 Availability		
2 Systems and Technology Failures		
2.1 Hardware	AC – 17, 18, 19 CM – 8 CP – 6, 7 IA – 3 MP – 1-6 PE – 1-19 SA – 2, 3, 5-14 SC – 1-34	
2.1.1 Capacity		AU – 4
2.1.2 Performance		
2.1.3 Maintenance		MA – 1-6
2.1.4 Obsolescence		
2.2 Software	AC – 3, 4, 7-11, 17, 18, 19 AU – 7-10, 12, 14 CA – 5, 7 CM – 7, 8 CP – 6-9 IA – 1, 2, 4-8 MP – 1-6 SA – 2, 3, 5-14 SC – 1-34 SI – 1-13	
2.2.1 Compatibility		
2.2.2 Configuration Management		AC – 2, 5, 6 CM – 1-6, 9
2.2.3 Change Control		AC – 2, 5, 6 CM – 1-6
2.2.4 Security Settings		AC – 5, 6 CM – 1-6 RA – 5
2.2.5 Coding Practices		
2.2.6 Testing		CM – 4, 5

Taxonomy Class, Subclass, Element	NIST SP 800-53 Rev. 3 Controls	
2.3 Systems	AC – 3, 4, 7-11, 16 AU – 7-10, 12, 14 CA – 7 CM – 7-9 CP – 7-9 IA – 1-8 MA – 1-6 SA – 1-14 SC – 1-34 SI – 1-13	
2.3.1 Design		
2.3.2 Specifications		AC – 5, 6
2.3.3 Integration		
2.3.4 Complexity		
3 Failed Internal Processes		
3.1 Process Design and/or Execution	AC – 1, 5, 6, 14, 16-22 AT – 1-4 AU – 2, 3, 7, 9-13 CA – 1-3, 5, 6 CM – 1-8 CP – 1, 4, 9, 10 IA – 1-8 IR – 1, 3-8 MA – 1-6 MP – 1-6 PE – 1-19 PL – 1, 2, 6 RA – 1-3, 5 SI – 1-13 PM – 1-11	
3.1.1 Process Flow		
3.1.2 Process Documentation		
3.1.3 Roles and Responsibilities		
3.1.4 Notifications and Alerts		
3.1.5 Information Flow		
3.1.6 Escalation of Issues		
3.1.7 Service Level Agreements		
3.1.8 Task Hand-Off		

Taxonomy Class, Subclass, Element	NIST SP 800-53 Rev. 3 Controls	
3.2 Process Controls	AC – 5, 6, 14, 17, 18, 21 AU – 1-3, 6, 9-11, 13 CA – 1, 2, 5-7 CM – 1-3, 6, 7 CP – 1 IA – 2-8 IR – 1, 3-8 MA – 1-6 MP – 1-6 PE – 1-19 PL – 1, 2, 6 RA – 1-3, 5 SI – 1-13 PM – 1-11	
3.2.1 Status Monitoring		
3.2.2 Metrics		
3.2.3 Periodic Review		
3.2.4 Process Ownership		
3.3 Supporting Processes	CA – 5 CP – 2, 8 MA – 2-6 PL – 1, 2, 6 SA – 2, 3, 5-14 PM – 1-11	
3.3.1 Staffing		
3.3.2 Funding		
3.3.3 Training and Development		AC – 21, 22 AT – 1-4 CP – 3, 4 IR – 2 PL – 4 PS – 1-8
3.3.4 Procurement		AC – 20 IR – 7 SA – 1, 4
4 External Events		
4.1 Hazards	AT – 3 CP – 1-4, 6-8, 10 PE – 10-12, 16-18	
4.1.1 Weather Event		
4.1.2 Fire		PE – 13
4.1.3 Flood		PE – 15
4.1.4 Earthquake		
4.1.5 Unrest		
4.1.6 Pandemic		

Taxonomy Class, Subclass, Element	NIST SP 800-53 Rev. 3 Controls	
4.2 Legal Issues	AC – 19 AU – 13 CP – 2, 4, 8, 10 IA – 8 IR – 6 MP – 1-6 PE – 19 PL – 5 PS – 1-6, 8 RA – 2, 3 SA – 2, 3, 5-14 SI – 12	
4.2.1 Regulatory compliance		AU – 1, 2
4.2.2 Legislation		AU – 1, 2
4.2.3 Litigation		
4.3 Business Issues	AC – 20 CP – 1, 2, 4, 6, 8, 10 IA – 8 MA – 5 PL – 5 PS – 7 RA – 2, 3 SA – 2, 3, 5-14	
4.3.1 Supplier Failure		
4.3.2 Market Conditions		
4.3.3 Economic Conditions		
4.4 Service Dependencies	CP – 1-4, 7 PE – 10-13, 15-18 SA – 1, 4	
4.4. Utilities		
4.4.2 Emergency services		
4.4.3 Fuel		
4.4.4 Transportation		

References

URLs are valid as of the publication date of this document.

[Alberts 2001a]
Alberts, Christopher & Dorofee, Audrey. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method Implementation Guide, v2.0*. Software Engineering Institute, Carnegie Mellon University, 2001. http://www.cert.org/octave/

[Alberts 2001b]
Alberts, Christopher & Dorofee, Audrey. *OCTAVE Threat Profiles*. Software Engineering Institute, Carnegie Mellon University, 2001.
http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

[BIS 2006]
Bank for International Settlements (BIS). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version*.
http://www.bis.org/publ/bcbs128.pdf (2006).

[Caralli 2010a]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. *CERT® Resilience Management Model, v1.0* (CMU/SEI-2010-TR-012). Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

[Caralli 2010b]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. *CERT® Resilience Management Model, v1.0 - Risk Management (RISK)*. Software Engineering Institute, Carnegie Mellon University, 2010. http://www.cert.org/resilience/rmm.html

[DHS 2008]
Department of Homeland Security (DHS) Risk Steering Committee. *DHS Risk Lexicon.* Department of Homeland Security, September 2008.
http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

[FISMA 2002]
Federal Information Systems Management Act of 2002, 44 U.S.C. § 3542(b)(1). Office of the Law Revision Counsel, 2002. http://uscode.house.gov/download/pls/44C35.txt

[Gallagher 2005]
Gallagher, Brian P.; Case, Pamela J.; Creel, Rita C.; Kushner, Susan; & Williams, Ray C. *A Taxonomy of Operational Risks* (CMU/SEI-2005-TN-036). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/library/abstracts/reports/05tn036.cfm

[Kendall 2007]
Kendall, Richard P.; Post, Douglass E.; Carver, Jeffrey C.; Henderson, Dale B.; & Fisher, David A. *A Proposed Taxonomy for Software Development Risks for High-Performance Computing (HPC) Scientific/Engineering Applications* (CMU/SEI-2006-TN-039). Software Engineering Institute, Carnegie Mellon University, 2007.
http://www.sei.cmu.edu/library/abstracts/reports/06tn039.cfm

[NIST 2009]
National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Revision 3). U.S. Department of Commerce, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	December 2010	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
A Taxonomy of Operational Cyber Security Risks	FA8721-05-C-0003

6. AUTHOR(S)

James J. Cebula, Lisa R. Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2010-TN-028

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report presents a taxonomy of operational cyber security risks that attempts to identify and organize the sources of operational cyber security risk into four *classes*: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events. Each class is broken down into *subclasses*, which are described by their *elements*. This report discusses the harmonization of the taxonomy with other risk and security activities, particularly those described by the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) Special Publications, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) method.

14. SUBJECT TERMS	15. NUMBER OF PAGES
taxonomy, operational risk, FISMA, NIST, cyber security, OCTAVE, resilience	47

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL