Report Prepared For
Paula J. Olsiewski, Ph.D., Program Director
Alfred P. Sloan Foundation

Framework for Voluntary Preparedness

January 18, 2008

Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 And Public Law 110-53
"Implementing Recommendations of the 9/11 Commission Act of 2007"

By representatives of
ASIS International (ASIS)
Disaster Recovery Institute International (DRII)
National Fire Protection Association (NFPA)
Risk and Insurance Management Society, Inc. (RIMS)

Framework for Voluntary Preparedness

INTERDISCIPLINARY TEAM REPRESENTATIVES

About **ASIS International (ASIS)**

ASIS International (ASIS) is the largest organization for security professionals, with more than 35,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine - *Security Management* - ASIS leads the way for advanced and improved security performance.

About **Disaster Recovery Institute International (DRII)**

DRI International was founded in 1988 as the Disaster Recovery Institute in order to develop a base of knowledge in contingency planning and the management of risk, a rapidly growing profession. Today DRI International administers the industry's premier educational and certification programs for those engaged in the practice of business continuity planning and management. More than 5,000 individuals throughout the world maintain professional certification through DRI International.

About the **National Fire Protection Association (NFPA)**

Established in 1896, NFPA is a private, not-for-profit, standards development organization that is the world's leading advocate for fire protection and prevention, and an authoritative source for public safety information. NFPA's over 300 codes and standards are part of the design requirements and the basis for regulations for buildings, processes, services, designs, and equipment installations in the United States as well as those in other countries. NFPA standards focus on the built environment, hazardous industrial processes and chemicals, and first responder operations and equipment. NFPA's codes and standards development process is accredited by the American National Standards Institute (ANSI) and is a model of openness, balance and consensus. NFPA has a membership of over 80,000 persons from 122 nations.

About the **Risk and Insurance Management Society, Inc. (RIMS)**

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the practice of risk management, a professional discipline that protects physical, financial and human resources. Founded in 1950, RIMS represents nearly 4,000 industrial, service, nonprofit, charitable, and governmental entities. The Society serves over 10,000 risk management professionals around the world.

BACKGROUND

On August 3, 2007, the U.S. federal law "Implementing Recommendations of the 9/11 Commission Act of 2007" (also referred to as H.R. 1 and Public Law 110-53) was signed. Title IX of the Act calls for the creation of a voluntary private sector preparedness standards program. While the U.S. Department of Homeland Security (DHS) is to take key actions in establishing this program, the legislation calls for wide private sector input into the program's development and ongoing operation. In order to provide the private sector input, the Alfred P. Sloan Foundation convened groups of key stakeholders to discuss the impact of the voluntary preparedness standards program on the private sector. The objective of these forums is to help provide DHS with the guidance in program development and implementation that would reflect the consensus of the private sector.

At one such forum on October 23, 2007, a group of stakeholders representing various professional organizations and businesses discussed the issue of standards, guidelines and best practices that address private sector preparedness. The participants (see Appendix A) recommended that, in order for the private sector to adequately and voluntarily establish preparedness programs, it should be given the flexibility to choose from various standards, guidelines and best practices that best meet their needs for preparedness. Assuring organizational resilience in the private sector requires the appropriate management of the risks related to intentional, unintentional and naturally caused disruptions that organizations of all sizes and types face. However, it was agreed among the participants that one size does not fit all and therefore, it is important that the private sector have appropriate choices that fit their respective business needs.

Recognizing that there are similarities in the core elements[1] of the existing standards, guidelines best practices, and regulations, four professional organizations, ASIS International (ASIS), Disaster Recovery Institute International (DRII), National Fire Protection Association (NFPA), and Risk and Insurance Management Society, Inc. (RIMS) (referred to as "The Interdisciplinary Team") combined their expertise and perspectives in a collaborative effort to develop a mechanism to address verifiable private sector preparedness. The Alfred P. Sloan Foundation has generously supported this effort to identify issues critical to program success and business viability.

Interdisciplinary Team Work Focus

The law states that "the term 'voluntary preparedness standards' means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs...." The Interdisciplinary Team brings together professional associations that view preparedness from security management, business continuity management, emergency management, and enterprise risk management perspectives. This work highlights the commonality of the different perspectives and approaches of these disciplines and their established standards, guidelines and best practices. Depending on the structure of businesses and organizations in the private sector, many are already pursuing elements or complete programs in preparedness based on the viewpoint of one or more of these disciplines. These businesses and organizations need the freedom to develop mature preparedness programs and systems building on their existing models.

[1] Core elements are those basic components that, when implemented within an organization's unique governance and culture, provide the underlying framework to enable the organization to sustain itself in spite of a disruptive event (i.e., the "common set of criteria for preparedness, disaster management, emergency management, and business continuity programs...." called for under the law.)

Preparedness involves issues and actions before, during and after a disruptive incident. Therefore, preparedness encompasses prevention, deterrence, readiness, mitigation, response, continuity, and recovery. Various disciplines, practitioners and organizations focus different weight on these components of preparedness. However, throughout this paper, the term "preparedness" is used in an inclusive sense of all phases before, during and after a disruptive event. The Interdisciplinary Team approached the work commissioned by the Sloan Foundation by first considering what core elements must be in place to increase the probability of a private sector company's continued sustainability and resiliency in light of a disruptive event, regardless of cause.

Core Elements in Relation to Regulations

Regulations are mandatory authoritative rules dealing with details or procedures having the force of law, which are issued by an authority of government. The Interdisciplinary Team reviewed the following relevant U.S. regulations to discover core elements already required of certain regulated industries: SEC, NASD, NERC, HIPAA, and FFIEC. The Interdisciplinary Team recognizes that organizations are subject to multiple regulations. It is not our intent to complete a study of all potential regulations that enterprises might face. The purpose of the review for this work is to determine whether certain regulations contain the identified core elements. Furthermore, regulatory audits of the regulatory requirements provide evidence of preparedness, conformity with standards, and best practices. The Interdisciplinary Team confirmed commonalities with respect to certain core elements contained within these identified various regulations.

Core Elements in Relation to Standards

Standards are a set of voluntary criteria, voluntary guidelines and best practices used to enhance the quality, performance, reliability and consistency of products, services and/or processes. International, national and regional standards bodies have initiated aggressive standards development programs addressing preparedness management. Generic management standards assure that an organization's management approach has a number of essential features in support of how it manages its processes or activities. Standards are applicable to any organization, large or small, whatever its function, products, or services. These standards typically include provisions for either first, second, or third party auditing and validation of meeting the requirements of the standard.[2] Standards are an alternative to regulations. In contrast to regulations, standards are market-driven by the sectors that will put them to use. Standards may become recognized as industry best practice and a market requirement. However, this is an acceptance and developing process over time within the private sector, not a legislated process. The Interdisciplinary Team reviewed the following standards and proposed standards as being pertinent to U.S. business preparedness: NFPA 1600-2007 Standard on Disaster/Emergency Management and Business Continuity Programs, ISO/PAS 22399-2007, ASIS International Organizational Resilience: Preparedness and Continuity Management – Best Practices Standard, BS 25999-2:2007 Business Continuity Management – Part 2 – Specification, and CSA Z1600 Standard on Emergency Management and Business Continuity Programs. The Interdisciplinary Team confirmed the commonality of the core elements contained within these standards and proposed standards.

[2] First party self-reporting and self-declaration (e.g., checklist against core elements or internal audit review); Second party review against core elements (e.g., supply chain audit verification by clients); Third party auditing and validation against core elements or existing standards (e.g., outside auditors checklist and test against core elements or full standard certification)

Core Elements in Relation to Best Practices

There are a number of resources U.S. businesses can look to for guidance on best practices. Best practices often are the basis for the development of standards. The Interdisciplinary Team reviewed two authoritative sources: TR19-2005 Technical Reference for Business Continuity Management (BCM) and DRI/BCI Professional Practices for Business Continuity Planners. The Interdisciplinary Team confirmed the commonality of certain core elements contained within these authoritative source documents.

MAPPING THE CORE ELEMENTS FOR PREPAREDNESS

Preparedness involves a defined methodology, program, process and/or system to address critical core elements. The critical core elements, as determined by the Interdisciplinary Team, are listed below, are presented graphically as a process in Figure One, and are tied to elements found in various standards and best practices as detailed in Appendix C:

Critical Core Elements	Process (see Figure 1)	Elements of Standards and Best Practices used in Appendix C
■ Policy statement and management commitment ■ Scope, program roles, responsibilities, and resources	**Program Policies and Procedures**	■ Project scope, policy, principles and management commitment
■ Risk identification, assessments and criticality impact analyses, including legal and other requirements	**Analysis**	■ Legal, statutory, regulatory and other requirements ■ Risk assessment and impact analysis
■ Prevention and Mitigation Evaluation and Planning ☐ Strategic: prioritization, objectives, targets, dependencies, such as supply chain and third parties ☐ Tactical: plans for avoidance, prevention, deterrence, readiness, mitigation, response, continuity, and recovery	**Planning**	■ Setting objectives and priorities to develop risk and incident preparedness management strategies
■ Incident management (procedures and controls before, during and after a disruption, including emergency management of people, business operations and technology) ☐ Operational procedures and contingency plans ☐ Communications and warning ☐ Application and business	**Implementation and Operational Controls**	■ Developing and implementing operational and control plans, procedures and programs for preparedness, including prevention, avoidance, deterrence, readiness, preparedness, mitigation, response, continuity and recovery ■ Communication and warning

Critical Core Elements	Process (see Figure 1)	Elements of Standards and Best Practices used in Appendix C
function resiliency ☐ Document, information and data control and backup ☐ Execution resources, responsibilities and finances		■ Document, information and data control and backup ■ Allocation of human, physical and financial resources
■ Recovery ☐ May be considered by the reader to include rebuilding, repairing, and / or restoring	**Implementation and Operational Controls**	■ Included in both "Planning and Implementation" and "Operational Controls"
■ Awareness and training	**Implementation and Operational Controls**	■ Awareness, competence and training
■ Exercises and testing ☐ Post-mortem learning	**Checking and Evaluation**	■ Performance assessment and evaluation
■ Program revision and improvement ☐ Corrective actions	**Review, Maintenance, Improvement**	■ Review, maintenance, and improvement

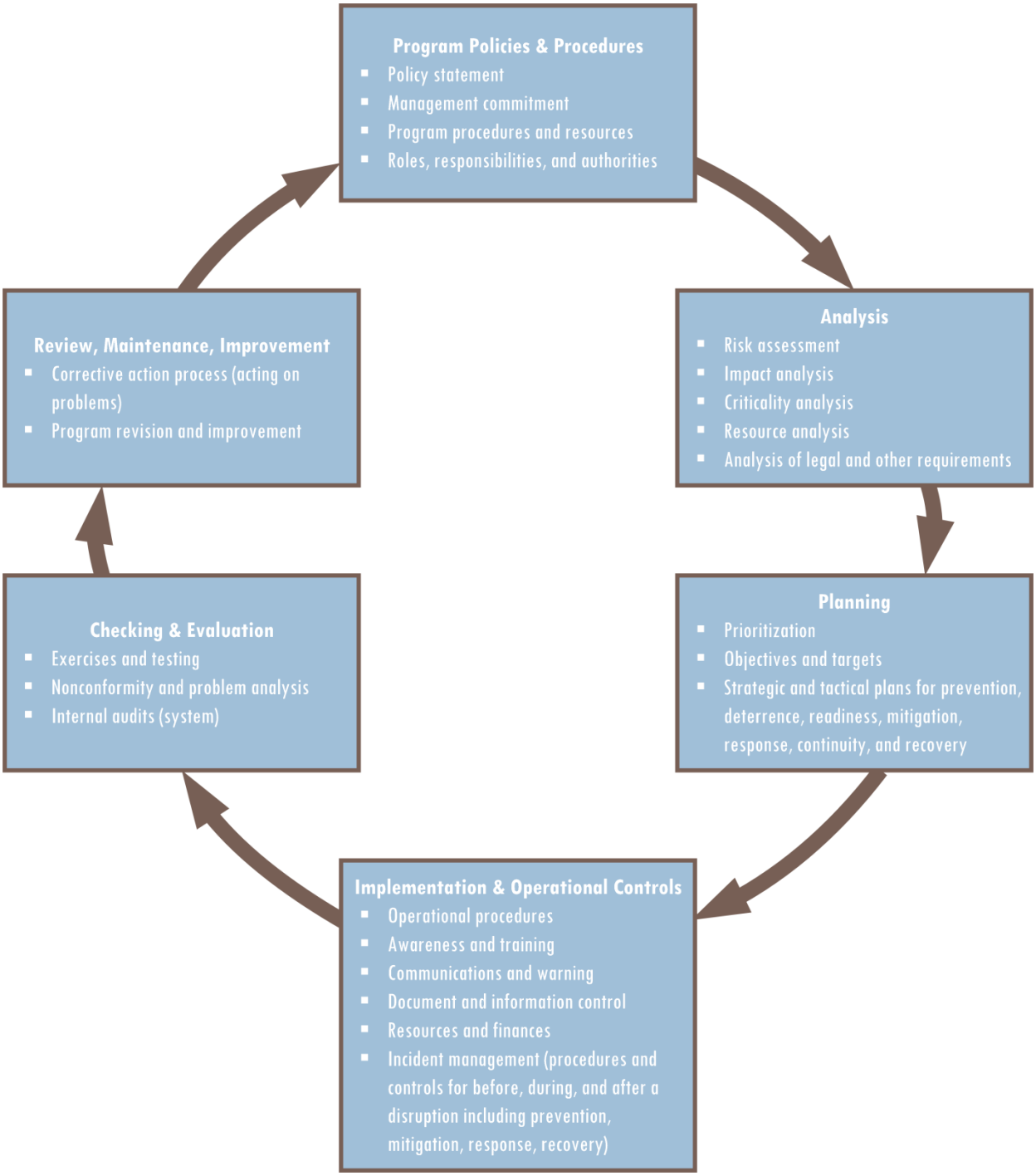


FIGURE 1 CORE PROGRAM ELEMENTS USING A PROCESS APPROACH

PROPOSED MECHANISM(S) TO ACHIEVE VERIFIABLE PRIVATE SECTOR PREPAREDNESS

Challenges Influencing Program Acceptance and Viability

In the Stakeholder Forums sponsored by the Sloan Foundation, it was clear to the participants that, for the legislation to make business sense, the DHS has to consider several major issues. As the implementation of Title IX of PL 110-53 is an unfunded effort, there are no tangible rewards; e.g., tax reductions in the form of deductions or tax credits to use as an incentive. While there are ongoing efforts to provide some insurance relief for business continuity planning, at this time no such incentives are available. Businesses face an array of risks with limited resources available to manage them.

Preparedness and Management Control Practices Already in Place

Enterprise Risk Management

A number of organizations have introduced enterprise risk management (ERM) systems that integrate preparedness into the overall risk management scheme (see Appendix B). Organizations practicing ERM already have mechanisms in place to address many or most preparedness issues. Therefore, it is important to recognize that they are addressing the core elements of preparedness, while not "siloing" these as unrelated operational risks. These frameworks should be recognized and given appropriate "credit" toward preparedness to the extent that the resulting management controls address the identified core elements.

PROPOSED VERIFICATION MECHANISMS: First party internal audit review; Second party (e.g., client) reviews; Rating agency ERM reviews; Self-declaration of compliance with chosen standard; Third party certification

EVIDENCE OF PREPAREDNESS: AUDIT REVIEWS, CLIENT REVIEWS, RATING AGENCY REVIEWS, CERTIFICATION TO CHOSEN STANDARD(S)

Supply Chain / Other Operational Standards

Businesses and organizations already have adopted elements of preparedness standards either by integrating them into their supply chain practices and/or by adopting other operational standards dealing with quality, environment, and information security. In a similar fashion to organizations practicing ERM, they could integrate the core elements of preparedness into their existing management systems without the financial burden of a "siloed" certification program solely for preparedness.

Furthermore, many larger businesses involved in supply chain activities already have existing internal policies and standard operating procedures addressing the core elements of preparedness. They have established contractually enforced internal preparedness policies and standard operating procedures that they require their supply chain partners to meet. Neither the larger businesses nor their supply chain partners would see a financial benefit in retooling simply to meet the new legislation.

Preparedness practices implemented under complementary standards and/or supply chain requirements should be recognized and "credited" in demonstrating preparedness to the extent that these management controls and systems address the identified core elements.

PROPOSED VERIFICATION MECHANISMS: First party internal audit review; Second party (e.g., client) reviews; Rating agency ERM reviews; Self-declaration of compliance with chosen standard; Third party certification

EVIDENCE OF PREPAREDNESS: AUDIT REPORT / CLIENT REVIEWS / RATING AGENCY REVIEWS / CERTIFICATION TO CHOSEN STANDARD(S)

Regulated Industries

Other private sector organizations are required to meet dozens of regulations or guidelines. Unlike Title IX of PL 110-53, the requirements may be punitive; i.e., be subject to fines, disciplinary actions or loss of the right to continue to operate. These include, but are not limited to, OSHA (Occupational Safety and Health Administration) regulations, fire and life safety codes, FFIEC (Federal Financial Institutions Examination Council) business continuity operating guidelines, NERC (North American Electric Reliability Corporation) security guidelines for utilities, other homeland security regulations for critical infrastructure, and state regulations for the sale of insurance. Private industry has invested billions of dollars to meet the requirements that, in many cases, address the core elements of preparedness standards. Demonstrating to regulators that these core elements are in place should be recognized as a "credit" toward preparedness to the extent that these regulatory controls address the identified core elements.

PROPOSED MECHANISMS: Regulatory review; First party self-declaration, Third party certification

EVIDENCE OF PREPAREDNESS: REGULATORY REPORT / CERTIFICATION TO CHOSEN STANDARD(S)

Small- and Medium-Sized Businesses

Small- (less than $10 million in annual revenue) and medium- (between $10 and $100 million in annual revenue) sized businesses face a significant cost-benefit challenge if required to spend scarce resources and needed capital for certification to a standard or compliance with government regulation. While many such organizations have created preparedness plans to meet the demands of their clients, they are unlikely to expand those efforts without seeing a tangible gain.

Furthermore, experience with quality, environmental and information security standards has shown that standards requiring certification set a high benchmark that is difficult for many small and medium enterprises to achieve and maintain in a cost-effective fashion. This is particularly true for companies not involved in supply chain activities with compliance with standards as a contractual requirement to do business.

Many small to medium businesses use standards as guidance for elements to consider in managing aspects of their operations. However, unless specifically required by contractual arrangements or regulations, they typically cannot financially justify formal implementation and the costs of third-party auditing and certification. It is important to recognize that certification is an ongoing process and the cost of maintaining implementation and certification is beyond the economic reach of many small businesses. Therefore, many small to medium businesses use the standards as a learning tool, adopting core elements that fit their business management model. This approach to standards has proven very effective in enhancing performance in quality and environmental management and has generated a system of recognition and reward for implementing core elements outside the formal certification process.

A similar approach for such businesses would significantly enhance preparedness performance of these businesses without imposing the financial burden of formal standard implementation and certification.

PROPOSED VERIFICATION MECHANISM: First Party Self-Declaration Against Core Element Checklist

EVIDENCE OF PREPAREDNESS: BUSINESS READINESS DECAL

MEETING THE CHALLENGES SUMMARY

The intent of Title IX of PL 110-53 is to enhance private sector preparedness. For this to be accomplished, private sector organizations need to be given the freedom and flexibility to address the core issues of preparedness that are appropriate to their existing management models, mission, and size of organization. From this discussion, it is clear that regulated industry sectors, unregulated industry sectors, small- to medium-sized businesses involved in the supply chain with other businesses and stand-alone small businesses face the challenge of enhanced preparedness performance from different economic realities. The approach to achieve this goal may be through compliance with regulations, implementations of standards, or adopting core elements of standards in simplified management models. Acceptance and viability of any approach will be dependent on business decisions consistent with the mission and economic realities of the organization. Obviously, building on existing management models and avoidance of duplication are at the heart of any successful preparedness program. Therefore, organizations that are in conformity with existing regulations, standards, guidelines or industry best practices that address the core elements of preparedness should be recognized as having achieved the intent of Title IX of PL 110-53, and should be credited for existing practices to the extent such practices address the identified core elements. Certification to a specific preparedness standard may be adopted voluntarily by an organization as a competitive differentiator.

CONCLUSIONS

Any of the three approaches (enterprise risk management, standards or regulatory approaches) can be used to meet the intent of Title IX of PL 110-53 for improved private sector preparedness performance. As has been seen in environmental management, these three approaches can be used together as complementary tools if this fits within the management scheme of the organization.

Also, as clearly demonstrated by environmental management, considerations must be made for the economic constraints of small business. Improved preparedness performance and all the core elements above can be addressed by less formal approaches to meet the intent of Title IX of PL 110-53.

It is important for the DHS to recognize that multiple approaches comply with the spirit of Title IX of PL 110-53. Therefore, greater resiliency success will be achieved if businesses are given the freedom and flexibility to determine how they will improve preparedness in a way that best fits their respective business models. Any process or approach that addresses the core elements addressed above is sufficient to improve preparedness performance without the need for duplication of efforts and unnecessary financial burden to the private sector.

It should be noted that mechanisms exist for certification to standards (see Appendix E). However, most standards provide for improved performance and demonstrate the conformity to the standard in balance with socio-economic needs of the organization. This allows for self-declaration, second-party auditing and contractually enforced conformity, in addition to third-party auditing and certification, as mechanisms for organizations to demonstrate successful implementation of the standard to assure interested parties that an appropriate system is in place. Therefore, for the private sector preparedness program to be successful it should adopt the same breadth of approaches to demonstration of conformity that has made environmental management a successful tool for improved environmental performance.

Based on the discussion above, it is evident that a number of excellent options are available for private sector organizations to implement approaches and demonstrate improved preparedness. Any of the existing standards, guidelines, best practices, or regulatory approaches can be used to meet the intent of Title IX of PL 110-53 (see Appendices C and D). Clearly, these mechanisms already exist in the private sector. What is lacking is the know-how, implementation tools and evaluation metrics to help the private sector, particularly small and medium businesses, successfully select and implement an approach appropriate to their situation.

RECOMMENDATIONS

For the private sector to adequately and voluntarily establish preparedness programs, it should be given the flexibility to choose from various standards, guidelines and best practices that best meet the respective organization's needs for preparedness. Organizations that have implemented preparedness management controls, best practices or complementary systems which address the core elements should be recognized and "credited" as demonstrating preparedness. Regulated industries should be given credit for their compliance with relevant regulations without the need for duplicative systems.

The biggest challenge facing the DHS and the private sector will be helping small and medium companies. Within the supply chain environment, it is likely that a standard that is implemented by large companies will be required of their supply chain vendors (typically, small and medium companies), as the price of doing business. However, these smaller companies will need assistance to meet these contractual requirements. What is lacking in preparedness management is the rich amount of training materials, case studies, tool sets, technical assistance and peer programs that have been developed over time to help small and medium companies meet these contractual requirements for environmental management.

The next effort should concentrate on creating tools to evaluate existing programs, and developing training materials, case studies, tool sets, technical assistance and peer programs to assist small and medium businesses develop and enhance their preparedness programs. The challenge is how to implement the above approaches in a cost-effective fashion. For the private sector to improve preparedness performance, it needs the tools and knowledge how to address the core elements in a business sensible fashion. Much can be learned from the decades of experience in quality and environmental management, particularly tailoring approaches that address the needs of small and medium businesses. The old adage – "you do not make a hog fatter by weighing it" applies in this context. Applying a voluntary certification standard, without the requisite underlying knowledge, tools and practices support, will not make the nation's private sector more prepared, as if by magic.

APPENDICES

Appendix A lists the participants in the October 23, 2007 Sloan Foundation Meeting

Appendix B presents a graphic representation of a generic ERM Framework, with attributes based on the RIMS Risk Maturity Model©. The core elements of preparedness management are completely consistent with integration into the holistic approach of enterprise risk management. ERM has achieved wide acceptance and provides organizations with a cost-effective approach to balance elements of risk management control options related to preparedness and other operational risk.

Appendix C presents a crosswalk of international and national standards, guidelines and best practices that address preparedness. While the list is not exhaustive, these were chosen by the Interdisciplinary Team as being the ones most pertinent to U.S. organizations, including those organizations with global operations. It is clear from this crosswalk that the identified core elements are common to all of the noted standards. The standards, guidelines and best practices represent a range of methods and approaches for achieving preparedness management while addressing the core elements needed to achieve improved preparedness performance. The choice of which standard to implement should be dependent on business considerations and existing management approaches used by the organization.

Appendix D presents a crosswalk of regulations that certain regulated industries must comply with related to preparedness. Here again, there are commonalities with the core elements of preparedness. Therefore, regulated industries can use conformity to regulations as a tool for enhanced preparedness performance without needing a redundant effort.

Appendix E defines accreditation bodies and certification (registration) bodies as well as the relevant standards that these bodies must follow. It also identifies other relevant standards and links to accreditation and certification bodies. Following the table, a brief description of relevant standards is presented.

Appendix A

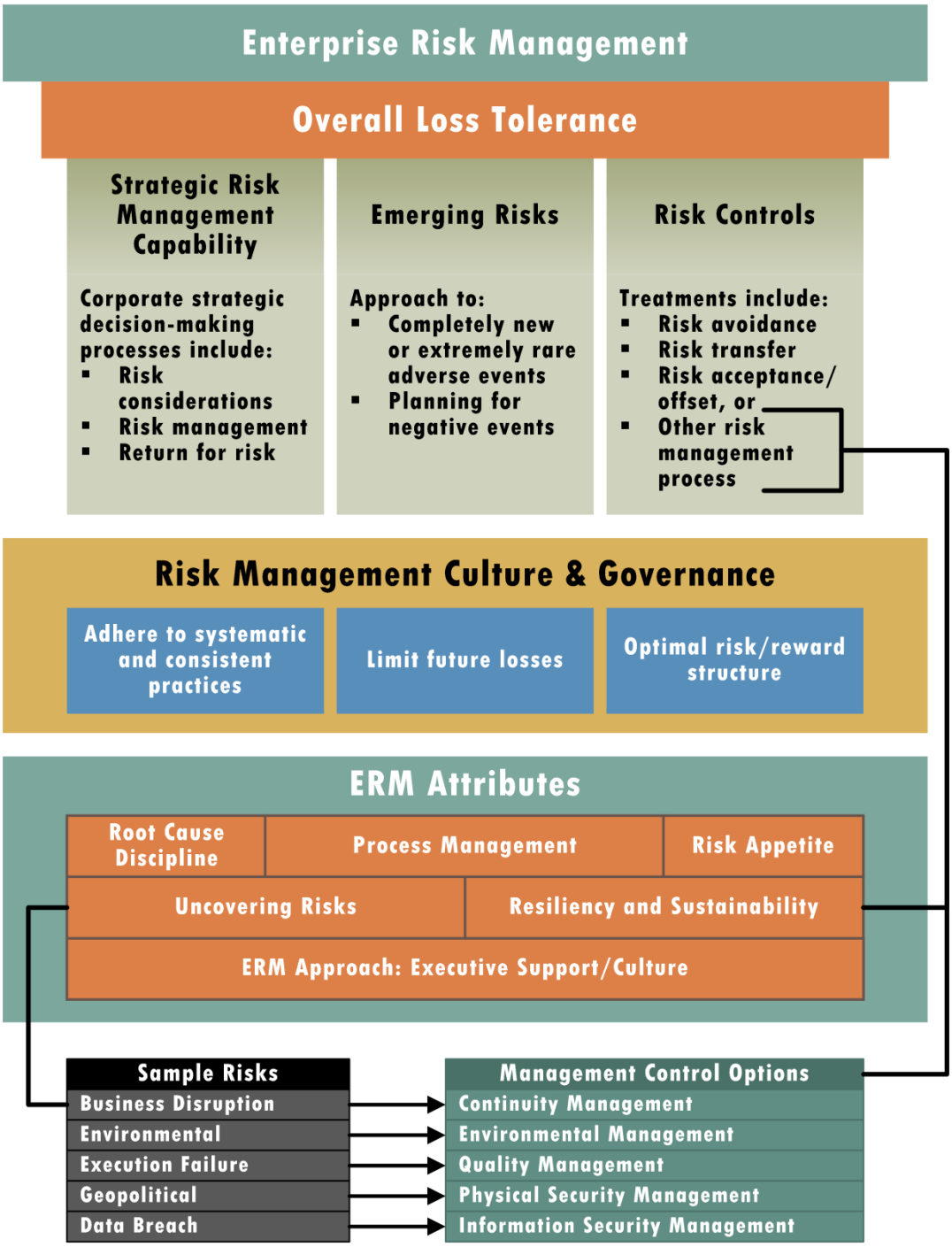
PARTICIPANTS IN THE OCTOBER 23, 2007 SLOAN FOUNDATION MEETING

- Nicholas Benvenuto, Jr., Managing Director, Protoviti, Inc.
- *Al Berman**, CBCP, MBCI Executive Director, Disaster Recovery Institute International (DRII)
- Bruce Blythe, CEO, Crisis Management International (CMI)
- Lynn Bruneau, Managing Director, Northeast Sarbanes-Oxley Services Leader, Protiviti, Inc.
- *Carol Fox**, former Board Member, Risk and Insurance Management Society (RIMS), Chair of RIMS ERM Development Committee and Senior Director, Risk Management and Business Continuity Planning, Convergys Corporation
- Jason Jackson, Director of Emergency Response, Wal-Mart Stores, Inc.
- Michael W. Janko, CBCP, Member NFPA 1600 Technical Committee Crisis Management Task Group, Manager, Global Business Continuity, The Goodyear Tire & Rubber Company
- Mike Rackley, Sr. Group Manager - Crisis Management & Security Services, Assets Protection, TARGET
- Bill Raisch, Director, International Center for Enterprise Preparedness (InterCEP), NYU
- *Donald L. Schmidt**, ARM, CEO, Preparedness, LLC and Chair, NFPA Technical Committee on Emergency Management and Business Continuity
- Frances Schrotter, Senior VP and COO, American National Standards Institute (ANSI)
- James Shortal, Director, Crisis Management/Business Continuity, The Home Depot
- *Marc H. Siegel**, Security Management System Consultant, ASIS International and Adjunct Professor, College of Business Administration and Master's Program in Homeland Security, San Diego State University
- Robert J. Vondrasek, Vice President, Technical Projects, National Fire Protection Association (NFPA)
- Paula J. Olsiewski, Ph.D., Program Director, Alfred P. Sloan Foundation

*** Interdisciplinary Team Member**

Appendix B

ENTERPRISE RISK MANAGEMENT FRAMEWORK / ATTRIBUTES BASED ON RIMS RISK MATURITY MODEL©



Appendix C

CROSSWALK OF STANDARDS, GUIDELINES AND BEST PRACTICES

COMMON ELEMENTS		STANDARDS, GUIDELINES AND BEST PRACTICES FOR MANAGEMENT OF INCIDENT PREVENTION, PREPAREDNESS, RESPONSE, CONTINUITY AND RECOVERY						
Common Elements	**Issues Addressed by Common Elements**	**NFPA 1600:2007**	**ISO/PAS 22399:2007**	**ASIS International**	**BS 25999-2: 2007**	**CSA Z1600**	**TR19:2005**	**DRI/BCI**
		Standard on Disaster/ Emergency Management and Business Continuity Programs	**Societal Security: Guidelines for Incident Preparedness and Operational Continuity Management**	**Organizational Resilience: Preparedness and Continuity Management Best Practices Standard**	**Business Continuity Management – Part 2: Specification**	**Standard on Emergency Management and Business Continuity Programs**	**Technical Reference for Business Continuity Management (BCM)**	**Professional Practices for Business Continuity Planners**
Project Initiation, Scope, Policy, Principles and Management Commitment	■ Establish the project to address preparedness management including provision of appropriate resources and authorities for conduct project. ■ Define to scope and/or boundaries for development and implementation of the preparedness management program. ■ Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. ■ Demonstrate top management and the organization's commitment to meeting the requirements of preparedness management.	4.1 Program administration 4.2 Program coordinator 4.3 Advisory committee 4.4 Program evaluation	5 Policy 5.1 Establishing the program 5.2 Defining program scope 5.3 Management leadership and commitment 5.4 Policy development 5.5 Policy review 5.6 Organizational structure for implementation	4.1.1 Scope of all hazards management system 4.2 All hazards risk management policy 4.2.1 Policy statement 4.2.2 Management commitment A.1 General requirements A.2 All hazards risk management policy	3 Planning the business continuity management system 3.1 General requirements 3.2 Establishing and managing the BCMS 3.2.1 Scope and objectives of BCMS 3.2.2 BCM policy 3.2.3 Provision of resources	4 Program management 4.1 Leadership and commitment 4.2 Program coordinator 4.3 Advisory committee 4.4 Program administration 4.4.1 Policy A.4.1 Leadership and commitment A.4.2 Program coordinator A.4.3 Advisory committee	8 Program management 5.1 Scope 5.2 Policies	1 Project initiation and management
Legal, Statutory, Regulatory and Other Requirements to which the Organizations Subscribes	■ Identify legal and other requirements to which the organization subscribes. ■ Establish a procedure or process for identifying, registering and evaluating legislative, regulatory and policy requirements pertinent to the organization's functions, activities and operations.	5.2 Laws and authorities A.5.2 Laws, authorities, and industry codes of practice and guidelines	6.2 Legal and other requirements	4.3.2 Legal and other requirements A.3.2 Legal and other requirements	1 Scope	4.5 Laws and authorities A.4.5 Laws and authorities	4.2.3 Regulatory requirements	10 Coordination with external agencies
Risk Assessment and Impact Analysis	■ Identify assets, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the organization and stakeholders. ■ Identify of hazards and threats.	5.3 Risk Assessment A.3.3.6 Impact Analysis A.5.3 Comprehensive risk assessment	6 Planning 6.1 General 6.3 Risk assessment and impact analysis 6.4 Hazard, risk, and threat	4.3 Planning 4.3.1 Risk assessment and impact analysis A.3 Planning A.3.1 Risk	4 Implementation and operation of the BCMS 4.1 Understanding the organization 4.1.1 Business	5. Planning 5.1 Hazard identification, risk assessment and business impact analysis	3 Risk assessment and review 4 Business impact analysis 5 Strategy 5.3 Processes	2 Risk evaluation and control 3 Business impact analysis

Common Elements		Standards, Guidelines and Best Practices for Management of Incident Prevention, Preparedness, Response, Continuity and Recovery						
Common Elements	**Issues Addressed by Common Elements**	**NFPA 1600:2007**	**ISO/PAS 22399:2007**	**ASIS International**	**BS 25999-2: 2007**	**CSA Z1600**	**TR19:2005**	**DRI/BCI**
	■ Establish a process for risk identification, analysis and evaluation. ■ Evaluate of the effect of uncertainty on the organization's objectives. ■ Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, environmental, information, and intangible). ■ Evaluate and establish recovery time objectives.	A.5.3.1 Methodologies and techniques for risk assessment A.5.3.2 Hazard identification A.5.3.3 Impact analysis	identification 6.5 Risk assessment 6.6 Impact analysis Annex A Impact analysis procedure	assessment and impact analysis	impact analysis 4.1.2 Risk assessment	A.5.1 Hazard identification, risk assessment and business impact analysis		
Setting Objectives and Developing Risk and Incident Prevention, Preparedness, Mitigation, Response, Continuity and Recovery Management Strategies	■ Prioritize the issues identified as a result of the risk assessment and impact analysis. ■ Set objectives and targets (including time frames) based on the prioritization of issues within the context of an organization's policy and mission. ■ Develop strategic plans for incident prevention, preparedness, mitigation, response, continuity and recovery. ■ Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. ■ Identify roles, responsibilities, authorities and their interrelationships within the organization as far as needed to ensure effective and efficient operations. ■ Plan the operational processes for actions effecting how the objectives and targets are achieved. ■ Make arrangements and contingency preparedness plans that need to be in place to manage foreseeable emergencies.	5.4 Incident prevention 5.5 Mitigation 5.6 Resource management and logistics 5.8.1 Planning process 5.8.2 Common plan elements 5.8.3 Plans A.3.3.12 Prevention A.3.3.12 Recovery A.3.3.15 Response A.4.1(3) Common criteria A.5.4 Prevention strategies A.5.5 Mitigation strategies A.5.6 Resource management	6.7 Incident preparedness and operational continuity management programs 6.7.1 General 6.7.2 Prevention and mitigation programs 6.7.3 Response management programs 6.7.4 Emergency response management program 6.7.5 Continuity management program 6.7.6 Recovery management program Annex B Emergency response management program Annex C Continuity management program	4.3.3 Objectives, targets and program(s) A.3.3 Objectives, targets and program(s)	4 Implementation and operation of the BCMS 4.1.3 Determining choices 4.2 Determining business continuity strategy	5.3 Common plan requirements 6.1 Prevention and mitigation 6.2 Resource management A.6.1 Prevention and mitigation A.6.2 Resource management	6 Business continuity plan	4 Developing business continuity strategies
Developing and Implementing Operational and Control Strategies, Plans, Procedures and Programs	■ Establish operational control measures needed to implement the strategic plan(s) and maintain control of activities and functions against defined targets. ■ Develop procedures for controlling key activities, functions and operations that are associated with	5.7 Mutual aid/assistance 5.9 Incident management 5.11 Operational procedures 5.12 Facilities A.4.2 Program	7 Implementation and operation 7.1 Resources, roles, responsibility and authority 7.5 Operational control Annex B Emergency	4.4 Implementation 4.4.1 Resources, roles, responsibility and authority 4.4.4 Documentation 4.4.5 Control of documents 4.4.6 Operational	3.4 BCMS documentation and records 3.4.1 General 3.4.2 Control of BCMS records 3.4.3 Control of BCMS	6 Implementation 6.2 Resource management 6.3 Mutual aid/ mutual assistance 6.4 Emergency response 6.4.1 Incident		5 Emergency response and operations 6 Developing and implementing business continuity

COMMON ELEMENTS		STANDARDS, GUIDELINES AND BEST PRACTICES FOR MANAGEMENT OF INCIDENT PREVENTION, PREPAREDNESS, RESPONSE, CONTINUITY AND RECOVERY						
Common Elements	**Issues Addressed by Common Elements**	**NFPA 1600:2007**	**ISO/PAS 22399:2007**	**ASIS International**	**BS 25999-2: 2007**	**CSA Z1600**	**TR19:2005**	**DRI/BCI**
	the organization. ■ Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. ■ Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. ■ Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, finance, etc. which have an impact on the organization's performance and its stakeholders. ■ Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the preparedness management program or system. ■ Formalize arrangements for those who supply and contract their services to the organization which have an impact on the organization's performance, including mutual aid agreements.	coordinator A.4.3 Advisory committee A.5.7 Mutual aid A.5.8 Planning and review A.5.11 Procedures for response A.5.12 Emergency operations centers	response management program Annex C Continuity management program	control 4.4.7 Incident preparedness and response A.4 Implementation and operation A.4.1 Resources, roles, responsibility and authority A.4.4 Documentation A.4.5 Control of documents A.4.6 Operational control A.4.7 Incident preparedness and response	documentation 4 Implementation and operation of the BCMS 4.3 Developing and implementing a BCM response 4.3.1 General 4.3.2 Incident response structure 4.3.3 Business continuity plans and incident management plans	management 6.6 Operational procedures 6.7 Facilities 6.9 Recovery A.4.4.5 Records management A.6.3 Mutual aid/ mutual assistance A.6.4.1 Incident management A.6.6 Operational procedures A.6.7 Facilities A.6.9 Recovery		
Awareness, Competence and Training Strategies, Plans and Programs	■ Assess, develop and implement training/education program(s) for the organization's personnel, contractors and other relevant stakeholders. ■ Identify and establish skills, competency requirements and qualifications to address both normal and abnormal conditions. ■ Develop organizational awareness and establish a culture to support preparedness management.	5.13 Training	7.2 Building and embedding IPOCM in the organization's culture 7.3 Competence, training and awareness Annex D Building an incident preparedness and operational continuity culture	4.4.2 Competence, training and awareness A.4.2 Competence, training and awareness	3.2.4 Competency of BCM personnel 3.3 Embedding BCM in the organization's culture	6.8 Training A. 6.8 Training A.6.5.3 Public awareness and public education programs		7 Awareness and training programs
Communication and Warning Strategies, Plans and Programs	■ Make arrangements for communications both within the organization and to/from external sources. ■ Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media)	5.10 Communications and warnings 5.15 Communications and public information A.5.15 Information	7.4 Communications and warning	4.4.3 Communication and warning A.4.3 Communication and warning	4.3.2 Incident response structure 4.3.3 Business continuity plans and incident management plans	6.5 Communications and warning A.6.5 Communications and warning A.6.5.4 Crisis communications		6.B.11 Developing communications systems 9. Crisis communications

Common Elements		Standards, Guidelines and Best Practices for Management of Incident Prevention, Preparedness, Response, Continuity and Recovery						
Common Elements	**Issues Addressed by Common Elements**	**NFPA 1600:2007**	**ISO/PAS 22399:2007**	**ASIS International**	**BS 25999-2: 2007**	**CSA Z1600**	**TR19:2005**	**DRI/BCI**
	for normal and abnormal conditions. ■ Develop and maintain reliable communications and warning capability in the event of a disruption.							
Allocation of Human, Physical and Financial Resources	■ Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. ■ Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. ■ Make arrangements for mutual aid and community assistance.	5.16 Finance and administration A.5.16 Finance and administration framework	7.1 Resources, roles, responsibility and authority 7.6 Finance and administration	4.4.1 Resources, roles, responsibility and authority A.4.1 Resources, roles, responsibility and authority A.4.7 Incident preparedness and response	4.2 Determining business continuity strategy 4.3.2 Incident response structure 4.3.3 Business continuity plans and incident management plans	4.6 Financial management 6.2 Resource management A.4.6 Financial management A.6.2 Resource management	6.4 People 6.5 Infrastructure	6.B.13 Implement the plans
Performance Assessment and Evaluation	■ Establish metrics and mechanisms by which the organization assesses its performance on an ongoing basis. ■ Determine nonconformities and the manner in which these are dealt with. ■ Conduct internal audits of system or programs. ■ Plan and coordinate tests exercises, and evaluate and document exercise results.	5.14 Exercises, evaluations and corrective actions A.5.14 Exercises	8 Performance assessment 8.1 System evaluation 8.2 Performance measurement and monitoring 8.3 Testing and exercises 8.4 Corrective and preventive action 8.5 Maintenance 8.6 Internal audits and self assessment	4.5 Checking 4.5.1 Monitoring and measurement 4.5.2 Evaluation of compliance and system performance 4.5.2.1 Evaluation of compliance 4.5.2.2 Exercises and testing 4.5.3 Nonconformity, corrective action and preventive action 4.5.4 Control of records 4.5.5 Internal audits A.5 Checking A.5.1 Monitoring and measurement A.5.2 Evaluation of compliance and system performance A.5.2.1 Evaluation of compliance A.5.2.2 Exercises and testing A.5.4 Nonconformity, corrective action and preventive action	4.4 Exercising, maintaining and reviewing BCM arrangements 4.4.1 General 4.4.2 BCM exercising 5.1 Internal audit	7 Exercises, evaluations and corrective actions A.7 Exercises, evaluations and corrective actions	7 Tests and exercises	8 Exercising and maintaining business continuity plans

Common Elements		Standards, Guidelines and Best Practices for Management of Incident Prevention, Preparedness, Response, Continuity and Recovery						
Common Elements	**Issues Addressed by Common Elements**	**NFPA 1600:2007**	**ISO/PAS 22399:2007**	**ASIS International**	**BS 25999-2: 2007**	**CSA Z1600**	**TR19:2005**	**DRI/BCI**
				A.5.6 Internal Audit				
Review, Maintenance, and Improvement	■ Create procedures for eliminating the causes of detected nonconformities in programs, system and/or the operational processes. ■ Establish mechanisms for instigating action to eliminate potential causes of nonconformities in programs, system and/or the operational processes. ■ Conduct management review of programs and/or system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. ■ Make provisions for continual improvement of programs, system and/or the operational processes.	4.4 Program evaluation 5.14 Exercises, evaluations and corrective actions A.5.8 Planning and review A.5.14 Corrective action program	8.4 Corrective and preventive action 8.5 Maintenance 9 Management review	4.5.3 Nonconformity, corrective action and preventive action 4.6.4 Maintenance 4.6 Management review 4.6.1 General 4.6.2 Review input 4.6.3 Review output 4.6.4 Maintenance 4.6.5 Continual improvement A.5.4 Nonconformity, corrective action and preventive action A.6 Management review	4.4.1 General 4.4.3 Maintaining and reviewing BCM arrangements 5 Monitoring and reviewing BCMS 5.2 Management review of the BCMS 5.2.1 General 5.2.2 Review input 5.2.3 Review output 6 Maintaining and improving the BCMS 6.1 Preventive and corrective action 6.1.1 General 6.1.2 Preventive action 6.1.3 Corrective action 6.2 Continual improvement	8 Management review A.8 Management review	8 Program management	
Approach		Program approach not requiring a management system	Systems approach not requiring a specific method, however similar to Plan-Do-Check-Act Model	Systems approach based on the Plan-Do-Check-Act Model	Systems approach based on the Plan-Do-Check-Act Model	Systems approach not requiring a specific method, however similar to Plan-Do-Check-Act Model	Systems approach not requiring a specific method, however similar to Plan-Do-Check-Act Model	Professional practices focusing on the application by the practitioner

Appendix D

CROSSWALK OF RELEVANT REGULATIONS

Core Elements	SEC	NASD	HIPAA	FFIEC	NERC
Policy statement and management commitment	▣			▣	
Scope, program roles, responsibilities, and resources	▣			▣	
Risk identification, assessments and criticality impact analyses, including legal and other requirements	▣	▣	▣	▣	▣
Prevention and Mitigation Evaluation and Planning					
■ Strategic: prioritization, objectives, targets and dependencies			▣		
■ Tactical: plans for avoidance, prevention, deterrence, readiness, mitigation, response, continuity, and recovery					
Incident management (procedures and controls before, during and after a disruption, including emergency management of people, business operations and technology)			▣		▣
■ Operational procedures and contingency plans					
■ Communications and warning		▣		▣	▣
■ Application and business function resiliency		▣		▣	▣
■ Document, information and data control and backup		▣	▣	▣	
■ Execution resources, responsibilities and finances					
Recovery					
■ Rebuild, repair, restore, renovate					
Awareness and training					
Exercises and testing			▣	▣	
■ Post-mortem learning			▣		
Program revision and improvement				▣	
■ Corrective actions					
Non-Core Elements Specific to Regulated Industries	**SEC**	**NASD**	**HIPAA**	**FFIEC**	**NERC**
■ Emergency Mode Operation Plan (security)			▣		
■ Enterprise wide				▣	
■ Independent Audit	▣			▣	
■ Insurance Planning				▣	

Appendix E

ACCREDITATION AND CERTIFICATION (REGISTRATION) BODIES

	Relevant Standards	Other Relevant Standards	Directory of Bodies
Accreditation Bodies An organization (usually a national standards body associated with ISO) that checks certification bodies and, provided their certification assessment processes pass muster, accredits them i.e. grants them the authority to issue recognized certificates.	■ **ISO/IEC 17011:2004,** Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies ■ **ISO/IEC 17040:2005,** Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies		■ There are over 50 accreditation bodies worldwide. For a complete list: http://www.compad.com.au/clients/iaf/indexPrev.php?updaterUrlPrev=articles&artId=145 ■ There is one accreditation body listed in the United States: ANAB: American National Standards Institute - American Society for Quality National Accreditation Board LLC
Certification (Registration) Bodies An independent external body that issues written assurance (the certificate) that it has audited a management system and verified that it conforms to the requirements specified in the standard.	■ **ISO/IEC 17021:2006,** Conformity assessment -- Requirements for bodies providing audit and certification of management systems	■ **ISO/IEC 27006:2007,** Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems ■ **ISO 28003:2007,** Security management systems for the supply chain -- Requirements for bodies providing audit and certification of supply chain security management systems	For a list of certification bodies, go to http://www.anab.org/Directory/Directory_Search.asp
Certification Guidelines	■ **ISO 19011:2002,** Guidelines for quality and/or environmental management systems auditing	■ **ISO/PAS 22399:2007** or ■ **ASIS Organizational Resilience: Preparedness and Continuity Management - Best Practices Standard** or ■ **NFPA 1600:2007** Standard on Disaster/Emergency Management and Business Continuity Programs or ■ **BS 25999-2**	**Note:** *Auditors from the certifying body must demonstrate competence both in ISO 19011:2002, as well as the standard against which they are auditing the organization.*
Organizations Implements standard – may seek formal recognition (certification) by a specialized third party body.	■ ISO/PAS 22399:2007 or ■ ASIS Organizational Resilience: Preparedness and Continuity Management - Best Practices Standard or ■ NFPA 1600:2007 Standard on Disaster/Emergency Management and Business Continuity Programs or ■ BS 25999-2 ■ etc.		

Brief Descriptions of Relevant Standards

(Source: http://www.iso.org)

ISO/IEC 17011:2004, Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies

- ISO/IEC 17011:2004 specifies general requirements for accreditation bodies assessing and accrediting conformity assessment bodies (CABs). It is also appropriate as a requirements document for the peer evaluation process for mutual recognition arrangements between accreditation bodies.
- Accreditation bodies operating in accordance with ISO/IEC 17011:2004 do not have to offer accreditation to all types of CABs.
- For the purposes of ISO/IEC 17011:2004, CABs are organizations providing the following conformity assessment services: testing, inspection, management system certification, personnel certification, product certification and, in the context of this document, calibration.

ISO/IEC 17040:2005, Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies

- ISO/IEC 17040:2005 specifies the general requirements for the peer assessment process to be carried out by agreement groups of accreditation bodies or conformity assessment bodies. It addresses the structure and operation of the agreement group only insofar as they relate to the peer assessment process.
- ISO/IEC 17040:2005 is not concerned with the wider issues of the arrangements for the formation, organization and management of the agreement group, and does not cover how the group will use peer assessment in deciding membership of the group. Such matters, which could for example include a procedure for applicants to appeal against decisions of the agreement group, are outside the scope of ISO/IEC 17040:2005.
- ISO/IEC 17040:2005 is applicable to peer assessment of conformity assessment bodies performing activities such as testing, product certification, inspection, management system certification (sometimes also called registration), and personnel certification.
- More than one type of activity can be included in a peer assessment process. This can be considered particularly appropriate when the body under assessment conducts combined assessments of multiple conformity assessment activities.
- ISO/IEC 17040:2005 is also applicable to peer assessment amongst accreditation bodies, which is also known as peer evaluation.

ISO/IEC 17021:2006, Conformity assessment -- Requirements for bodies providing audit and certification of management systems

- ISO/IEC 17021:2006 contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g. quality management systems or environmental management systems) and for bodies providing these activities. Certification bodies operating to this International Standard need not offer all types of management system certification.
- Certification of management systems is a third-party conformity assessment activity. Bodies performing this activity are therefore third-party conformity assessment bodies.

ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

- ISO 19011:2002 provides guidance on the principles of auditing, managing audit programmes, conducting quality management system audits and environmental management system audits, as well as guidance on the competence of quality and environmental management system auditors.
- It is applicable to all organizations needing to conduct internal or external audits of quality and/or environmental management systems or to manage an audit programme.
- The application of ISO 19011 to other types of audits is possible in principle provided that special consideration is paid to identifying the competence needed by the audit team members in such cases.

ISO/IEC 27006:2007, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

- ISO/IEC 27006:2007 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.
- The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for any body providing ISMS certification.

ISO 28003:2007, Security management systems for the supply chain -- Requirements for bodies providing audit and certification of supply chain security management systems

- ISO 28003:2007 contains principles and requirements for bodies providing the audit and certification of supply chain security management systems according to management system specifications and standards such as ISO 28000.
- It defines the minimum requirements of a certification body and its associated auditors, recognizing the unique need for confidentiality when auditing and certifying/registering a client organization.

- Requirements for supply chain security management systems can originate from a number of sources, and ISO 28003:2007 has been developed to assist in the certification of supply chain security management systems that fulfill the requirements of ISO 28000, Specification for security management systems for the supply chain, and other supply chain security management system International Standards. The contents of ISO 28003:2007 may also be used to support certification of supply chain security management systems that are based on other specified supply chain security management system requirements.

- ISO 28003:2007 also:

  - ☐ provides harmonized guidance for the accreditation of certification bodies applying for ISO 28000 (or other specified supply chain security management system requirements) certification/registration;
  - ☐ defines the rules applicable for the audit and certification of a supply chain security management system complying with the supply chain security management system standard's requirements (or other sets of specified supply chain security management system requirements);
  - ☐ provides the customers with the necessary information and confidence about the way certification of their suppliers has been granted.