ATL PREVENTION RESEARCH L.L.C.

SPECIAL REPORT SERIES: NATIONAL SAFETY STANDARDS

RESEARCH PROJECT: ISO9001 2015 NEW QMS FRAMEWORK, REQUIREMENTS AND IMPLICATIONS

Produced By: ATL PREVENTION RESEARCH L.L.C.
Experimental Draft: Version1.4E
Origination: 2015-01-05T06:00 UTC
Last Updated: 2016-09-01T11:00 UTC

SPONSOR AND DISTRIBUTION:
This document is a FREE product of ATL Prevention Research L.L.C. for all to use as they wish.

SPECIAL THANKS:
Much gratitude and thanks to MJC for contributing facts, inferences, and helping to examine, clarify, and refocus elements of this topic.

PRELIMINARY THEORY:

At this time, the relationship of Government Agencies with ISO9001:2015 certified Businesses as (Public-Private Partnerships, Agreements, or Memorandums of Understanding) should be re-evaluated to improve opportunities, compatibility, security, and resilience for the benefit of everyone.

PREMISE:

The brief discussion conducted herein argues that it is a "good" and productive idea for DHS/FEMA to provide (early transitional support) for ISO9001:2015 certified business, (and should be justified and considered to be a "Win-Win") in the circumstance that said businesses products and/or services (directly support FEMA [e.g. as in logistics], or under the circumstance that the ISO9001 certified private business supports National Essential Functions, or Emergency Management Mission criteria, or local capabilities, or community resilience, is occupied daily by large numbers of people (e.g. schools), or broadly provides other resources, essential functions, products and services to the Public or Private sector unrelated to the NIPP-CI/PR-Infragard program).

WORKING HYPOTHESIS:

As an (undeniable antecedent), many DHS/FEMA educational and training courses, guides, products or recommendations have been evaluated and recognized (through consensus) as being very successful in framing, structuring, unifying and preparing many aspects of our Government Agencies and I expect that (as a consequent) this same education and training can provide transitional support for the New Risk Management component of ISO9001:2015, and enable said businesses to benefit internally, achieve further NIMS compatibility, and potentially enable new partnerships and enhance local and National resilience.

SUMMARY STATEMENT:

Exploring the above stated theory holds justifiable intrinsic value, and is recommended as a plausible and potentially fruitful project to examine "win-win" and "reciprocating" relationships between Government and ISO9001 certified businesses, it aligns with the trajectory of current DHS/FEMA services, and has the agenda of improving these relationships through advancement of education, training, and compatibility requirements. As a Nation we work together to build, sustain and improve our capabilities to prepare for, protect against, respond to, recover from and mitigate all threats and hazards. ISO9001:2015 is introduced here as a component of this calculus in that it is very compatible with many National standards and the (NEW RISK MANAGEMENT COMPONENTS) of this Quality Management Systems (QMS) may provide a path to enhance business resilience, coordination, and inclusion into local community capabilities, societal security, and enhance our National resilience. The available DHS/FEMA support to said businesses may be provided in many forms such as (e.g. grants, or special services offered to critical infrastructure or protected resource holdings, and others). For the purposes of this discussion, the recommended support for ISO9001:2015 transitioning businesses is in the form of ensuring awareness of DHS/FEMA products, providing additional training and education opportunities related to PS-Prep, COOP, risk management, and resource typing workshops, (such that opportunities are maximized and said businesses will be more in-tune with National Standards, improve their compatibility with NIMS requirements or with other Agency requirements), and further opportunities and partnerships may be examined. Upon examination of the national implications of these ISO9001:2015 changes, we find that some ISO9001 certified Organizations through Public-Private Partnerships (PPP) and/or their principles (via consensus) are figured into NIMS through the NIC and therefore their successful transition, stability, and continued conformity to the new requirements may impact our Nation in various ways. NIMS provides event specific principles, coordination of structures and roles, interoperability, portability, redundancy, and scalability for the management of incidents. Whereas the NRF provides core doctrine & partner guidelines, national planning, Federal & Private-sector support function annexes, role descriptions, responsibility descriptions,

incident annexes, and procedures relative to national-level response policy, (including integrated capabilities and resources as a seamless national framework). Therefore, changing the ISO9001 standard may impact the dynamic resilience environment and components listed above in NIMS, (both locally and nationally) for the benefit of all, (IF) the new risk management evaluations and improvements are appropriately acknowledged by relevant stakeholders as (imperatives).

TIMING OF THIS ARTICLE:

ISO9001:2008 standards will change this year to the new ISO9001:2015 standard. The FDIS was recently released, and contains NEW clauses and emphasizes on the importance of integrating RISK MANAGEMENT principles throughout the implementation process and systematic "Risk-Based Thinking" woven into the overall Quality Management System. Additionally, all Management System Standards are migrating to a new uniform framework, with identical core text and definitions, (see Annex SL containing the common operating framework 10 clauses and a minimum 84 requirements for details). Any additional training for discipline-specific requirements are undertaken as separate or supplementary modules pertaining to the select Management System needs of the organization. Said additional training would pertain to the industry, but could also take the form of PS-Prep or other FEMA courses that would cover the Risk Management requirement, and simultaneously may enable businesses to be compatible with local emergency managers, and nationally through NIMS.

PURPOSE, OPPORTUNITIES, AND PERTINENT ASSOCIATIONS:

- ✓ General: This topic aims to develop or enhance conditions that may lead to improvements in ISO9001 certified businesses, and yield benefits to local and national stakeholders.
- ✓ Magnitude: This is an important topic because 1.5 million Organizations (world-wide) are ISO9001 certified, and many of them conduct business with the U.S. Government, and impact our lives in various ways.
- ✓ Integration and Impact: ISO9001 co-exists and influences NIC Standards related to products and Capability Targets, (which are the performance thresholds for Core Capabilities), and impacts the Quality, Efficiency, Supply Chains, Logistics, Continuity of Operations, Mutual Aid Agreements, and other areas of National importance. NIMS, through the NIC, enables working relationships among Standards Development Organizations (SDOs), and with businesses that require Standard credentials to service incident management agencies, or develop performance standards, products, systems, and technologies for incident management. ISO9001 business products contribute to resource quality, quantity, FLUIDITY and ADAPTIVITY for the requirements of an incident. The (risk management component) of the Public-Private-sector partners (is enforced by ISO9001) and is therefore critical to the products and services these organizations provide to Local, State, and National Agencies and stakeholders.
- ✓ Support of National Essential Functions (NEF): Processes and conditions necessary for some NEFs are supported or enforced by ISO9001, (see NEF discussion within this topic).
- ✓ Safety and Security: The International Standards Organization chose Annex SL for development of the new ISO9001 standard, and is particularly pertinent to Societal Security, Information Technology & Security, Environmental Safety Management Systems, and Food Safety Management Systems. It is implied here that the new changes will impact societal security since individuals will likely be in these businesses when disaster strikes, and the Societal Security ISO22301 standard also contains the same Annex SL framework as the new ISO9001:2015 standard. Likewise, ISO9001:2015 requires all Occupants and Stakeholders to be considered in the businesses emergency plan. Food safety and continued quality of other products are also important public concerns that are enforced by ISO9001 safety requirements.
- ✓ Urgency and Imperatives: One important feature of this topic is related to (the new integration of Risk Management components into the NEW ISO9001 Standard), which implies that, (the sooner all stakeholders convert over to the NEW ISO9001:2015 Standard, the sooner the enhanced risk

management component will improve overall National Resilience). The assumption here is that we are a bit more resilient if we are more capable of identifying and managing or controlling risk, (now multiply this times all businesses that have the ISO9001 certification spread out across our Nation and we should see a good deal of national improvement). As a challenge to implementation, the NEW Risk Management (Risk-Based Thinking) components of ISO9001:2015 may require further analysis for impact, context, feasibility, continuity and/or deconfliction with Public-Private partners, operations, and dependencies. We should also evaluate the opportunities available to (save training costs, decrease duplicity, and gain uniformity) by utilize recommendations within the DHS PS-Prep program, CGC-1, CPG101 & 201, NIMS training, COOP education, and other National educational and training resources. The new ISO9001:2015 standard bears a striking resemblance to Continuity Guidance Circular-1, and could easily integrate concepts from it, therefore, I've included CGC-1 principles within the planning section, (for the observer to evaluate for themselves).

TOPIC SCOPE, FRAMEWORK, AND BOUNDARIES:

The application of said hypothesis (to test the enhancement of ISO9001:2015 certified businesses using said DHS/FEMA products) is framed as a preliminary experimental draft (illumination, discussion and suggestions) rather than scientific methodology because the experimental testing, evaluations and documentation of results would be quite lengthy and complicated to design and delineate at this preliminary stage of theory development. This topic will provide the reader with a brief overview of how National and International Standards impact U.S. businesses, capabilities, resources, and National Resilience, then focuses on the new ISO9001:2015 Standard, and will help businesses interpret and meet the new requirements for ISO9001:2015 certification.

NOTE-1: The flow of this document has a slightly redundant quality (that I've tried to limit). The redundancy results from the fact that all important "aspects" of a business (relate to "objectives"), that are then "defined," given "context," and a "policy" is formed, which is then "planned for," and provisioned for, then put into practice in "operations," "evaluated," and "improved" through time (this implies the same "aspect" of the business appears in most sections or clauses). Therefore, since a critical part of this discussion revolves around the new "risk management aspect" of the business and its relationship to National standards, as well as the implications of DHS/FEMA education, and the impact on national resilience, it is a logical choice to select risk management to be the "aspect" that will be exemplified throughout most major sections of this topic.

TOPIC BACKGROUND:

Nationally, and throughout the World, standards and standardization processes are managed by a large number of SDO's. SDO's examine facts, data, technical information, outputs, outcomes, lessons learned, and other reports to develop a consensus regarding best practices for a wide variety of industries, systems, processes, goods, services, competencies, and functions (See a list of SDO's in the Reference section). SDO activities ensure our country and the world will continue to be compatible and satisfy all mandates and requirements for businesses to remain safe, effective, functional, stable, dependable, efficient, and adaptive to change throughout the processes of providing goods and services. As advancements occur SDO's reflect improvements via a 3 to 5 year cycle of continuous revisions made to their preexisting Standards, and subsequently transition periods whereby businesses update their policies, recommendations, and procedures, conducting audits, and the renew their business certifications. Historically, in 1918 the U.S. American National Standards Institute (ANSI) was created (NOT to develop standards), but rather, to Oversee and Accredit SDO's, and coordinate U.S. Standards with International Standards via its members (now comprised of government agencies, organizations, corporations, academic and international bodies, and individuals, currently representing the interests of ~125,000 companies and 3.5 million professionals). In 1974 globalization activities lead to the U.S. Co-founding the International Organization for Standardization (ISO), and in 1987 ISO9001 was first published. The ISO9001 standard impacts many businesses and trade practices through providing equipment, products,

services, and is estimated to directly or indirectly impact nearly all protected resources in some way including: Agriculture and Food, Defense Industrial Base, Energy, Public Health and Healthcare, Financial Services, Drinking Water and Water Treatment Systems, Chemical Industry, Commercial Facilities, Dams, Emergency Services, Nuclear Reactors, Materials, and Waste, Information Technology, Communications, Postal and Shipping, Transportation Systems, Government Facilities. ISO9001 certified businesses are also involved in initiatives for sustainable development, accessibility, climate change, and a wide range of goods and services (See the Reference "ISO Standards in Action"). I concede here that there are other ISO's that relate more directly to Societal Security and Preparedness, but explain below how ISO9001:2015 will bridge gaps, and impact National resilience.

ISO9001 RELEVANCE AND IMPORTANCE TO LOCAL AND NATIONAL RESILIENCE:

In recent decades, the relative state of Resiliency has been examined by subject-matter experts and a consensus has resulted in the modification of certain Standards to enhance National Resilience. Among the many effectors impacting National Resilience is (the relative state of National Preparedness). Preparedness can be enhanced in many ways (e.g. through Risk Assessments, improvement of Core Capabilities, and improvement of Security Standards etc.). Implementation of Standards enforces various requirements that enhance actions taken to plan, organize, equip, train, and exercise in order to build and sustain continuity options and the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from events that pose the greatest risk to the security of our Nation. As stated in the topic background, ISO9001 is one of the most widely used standards in the world, and is important to businesses that provide products and services to both the Public and Private sectors. ISO 9001 & ISO 9004 are standards that create a climate of quality, consistency, stability, trust, and dependability. Quality and stability are important everywhere, but particularly to our energy systems, Emergency Equipment, transportation, supply chain relationships and dependencies, and our National Security apparatus. More than four decades of committee analysis and documentation has been compiled related to ISO9001 topics with aspects incorporated into our important Frameworks for Disaster Preparedness (especially in hospital settings). During the recent ISO update, the new Annex SL Framework was applied to ISO9001:2015 to address these important concepts and to help the new ISO changes integrate with other National Frameworks and other Standards that business concomitantly use. The U.S. NIMS Integration Center stresses the importance of standardization, credentialing, interoperability, and Continuity of Operations capabilities to ensure the adoption of common National standards, methods, resources and systems that are modern, dependable, compatible, and capable of improving our resilience through our National Incident Management System (NIMS). NIMS and CGC-1 align well with the new ISO9001:2015 standard, because ISO9001 strives to improve these factors as well. Businesses (in general) play a key role in building resilient communities, and as businesses consider what they need to do to survive a disaster or emergency they consider collateral implications of injuries to their employees and other occupants present on their premises. A Businesses ongoing effort to achieve stability and involvement in internal preparedness activities paves the way to both economic and societal resiliency within their communities. A percentage of these businesses are large enough to impact the resilience of their community and in some cases national resilience. Unfortunately, at this time there is not perfect integration of all business resilience stakeholders into the community or national resilience calculus. As Government Agencies plan for (individuals, businesses, CI/KR, NGOs, volunteers and others), and focus on ever increasing National resilience and capabilities, it opens pathways to a bidirectional functionality toward achieving our high-level missions as (Prevention, Protection, Mitigation, Response, and Recovery) and performance targets. However, VETTING CONCERNS are barriers to achieving some of said functional pathways, and are related to unknown multinational industry activities, foreign national influence or involvement in organizations, and vaguely attributable patterns of criminal activity. Those businesses that are left out (due to vetting concerns) or other incompatibilities, create cracks in what ideally should be a continuous interwoven community of trust and inclusiveness. Nonetheless, since programs like PS-Prep, and others contain the crisis management or continuity certification components and NIMS contains the agreement, credentialing, uniformity, Resource Typing and the collaboration components, the prospect of aligning many businesses

resources, capabilities, continuity and preparedness standards is very good and might be made possible for through DHS/FEMA education and training, especially for businesses transitioning to the new ISO9001:2015 standard. Once a Business is acknowledged as a resource, it could be typed, inventoried, evaluated as a "use case," incorporate its elements into capability targets, and be integrated into local and National capability options through NIMS Resource Typing, or other minimum NEMA/EMAC criteria. This makes good sense strategically in that integration patches cracks in community resilience (as discussed above) and through mutual aid agreements may enhance resources or capabilities. Statistically, re-evaluation of relationships between Agencies and ISO9001 certified businesses could help Government Officials and Emergency Management personnel gauge the quantitative and qualitative value associated with utilizing said businesses and their resources. In-depth NIMS compatibility requirements (generally are evaluated on a case-by-case basis) and are beyond the scope of this topic.

NOTE-2: (ISO9004:2009) "Managing for the Sustained Success of an Organization" (relates well to FEMA Continuity of Operations policies and other procedures), but is not pending imminent revision or new publication, and therefore will NOT be discussed further in this topic.

ISO9001 SUPPORT OF NATIONAL ESSENTIAL FUNCTIONS:

ISO9001 cultivates an environment to support National Essential Functions (NEF), (the reader is directed here to notice the CAPITALIZED WORDS in the next 3 NEF sub-points, then keep them in mind, and they will see that the capitalized words are also reflected throughout this topic and demonstrate that many processes and conditions necessary for NEFs are ENFORCED BY ISO9001). The private-sector support of NEF's occurs under a condition that I like to call "Public-Private Sector Continuous Essential Function Reciprocation." In other words, every day private sector businesses and organizations contribute local capability and to the health and stability of our Federal Government NEFs, and support is returned back to the Private Sector as discussed below. This reciprocation is observed in at least (Three) ways as follows:

a. Financial health, the NEF "protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems." ISO9001 certified businesses accomplish this through ensuring accurate and timely FINANTIAL RECORDS MANAGEMENT/MAINTANENCE, (e.g. book keeping, accounting, quarterly reports, payroll, banking practices, and record capabilities for forensic attribution especially foreign malfeasance). Both Local and Federal Government reciprocates by monitoring and ensuring crimes and serious disruptions or destabilizing conditions are addressed legally or otherwise (among other safeguards).

b. Physical health and security, the NEF "providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States." ISO9001 certified businesses accomplish this through ensuring their own SECURITY & CONTINUITY OF OPERATIONS, ensuring OCCUPANT SAFETY, generating RESOURCES that can be shared during emergencies, creating QUALITY PRODUCTS AND ADVANCEMENTS that our Government and everyone else can depend upon, providing QUALITY SERVICES that can be relied upon to keep us safe, healthy, and help us when in need, as well as other functions that enhance Local and National capabilities. Both Local and Federal Government reciprocates by Leading us, protecting /serving / responding to incidents, directing and implementing law / order / prevention mechanisms, ensuring stable energy, communications, transportation, distribution, sponsoring programs and giving back when resources are depleted (among vast other functions).

c. The NEF "Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident." This National Essential Function is contiguous with statements listed above in (b.), but I would like to add here that our wonderful volunteer organizations represent an expansion cadre that enhances response and recovery. Our Government in many instances provides the Policy, Framework, Education and TT&E programs behind these volunteering programs and functions, and ISO9001 businesses may supply both responders and volunteers with EQUIPMENT, LOGISTICS, or other resources.

d. (The provisional fourth NEF relationship) I would like to briefly state here that everyone in our country can help with one additional National Essential Function "Protecting against threats to the

homeland and bringing to justice perpetrators of crimes or attacks." This objective is partially accomplished by businesses (and everyone) through the program called "IF YOU SEE SOMETHING SAY SOMETHING," to which we are all implied members, and with which all good people are ethically beholden to participate. In many instances, Private-sector Surveillance videos, audio, data, and transaction trails (required in Banks and some other ISO9001 businesses) are critical to securing indictments, and ensuring fair judicial proceedings.

ESTIMATED VALUE OF ISO9001:2015 CERTIFICATION:

(INTERNAL) EFFECT OF STANDARDIZATION:

- ✓ Enhanced efficiency and utilization of resources (Improved likelihood of achieving objective, saves funds)
- ✓ Encourages and improves business governance and control, proactive risk management, safety, security, loss prevention as theft, environmental protection (protective)
- ✓ Improved stability and continuity, establishes a reliable base for decision making and planning (stabilizing)
- ✓ Improved Leadership, credentials and accountability (direction, and corrective action)
- ✓ Improves framework, evaluation and process assessments, integration with other standards, fulfillment of requirements, work-flow, and uniformity (less confusion, less conflicts, less duplication, less misunderstandings, less waste, and less error)
- ✓ Improved awareness, learning, and culture (cultivates an environment that will identify and report risks and abnormalities).
- ✓ Systematized compliance with requirements and legal obligations.
- ✓ Improved response to incidence, continuity, and overall resilience.

(EXTERNAL) EFFECT OF STANDARDIZATION & CERTIFICATION STATUS:

- ✓ Enables businesses to maintain access to (or gain new access to) select markets, whereby, customers require the certification as a prerequisite to (e.g. bid on contracts, or maintain a license).
- ✓ The certification provides a competitive advantage as a (quality assurance) differentiating factor.
- ✓ The certification provides customers with documentation that demonstrates the business continues to provide quality and improve throughout iterations of audits as it is re-evaluated over time.
- ✓ This certification may be a mandatory requirement prior to a business becoming eligible to produce critical goods or services and/or distribute them.
- ✓ Improved product and service quality (increases customer confidence in the business) and meeting product or service requirements or expectations (increases customer satisfaction).

ISO9001:2015 CORE DISCUSSION OF THE NEW HIGH LEVEL STRUCTURE (1-10):

Many organizations have a basic outline of processes, operations and Quality Assurance structures that correlates with their Business objectives, licensing agreements, or expectations related to inspection, and is realized through planning and policies. The NEW ISO9001:2015 standard emphasizes the use of Annex SL as the business Quality Management System framework, and discusses the structure and function of the QMS via 10 (clauses) A.K.A. sections (8 clauses previously) that are included in the FDIS, and will be part of the new standard this year (see sections 1-10 below):

ISO9001 (CURRENT) Transition Timeline to Know:

- ✓ Between Nov. 2014 and Feb. 2015 (Stage-5): FDIS was published for ballot.
- ✓ Between Aug. & Sept. 2015 (Stage-6): ISO9001-2015 is expected to become a standard.
- ✓ September 2015-September 2018: This is the ISO9001:2015 business transition period for (Certification and/or Auditing) accepted by the International Accreditation Forum.

- ✓ Sometime after September 2018- New audits may begin, upon which time nonconformity Reports will relate to the businesses ability to adhere to the ISO9001:2015 standard.

NOTE-3: Average time required to implement the new ISO9001:2015 standard is estimated to be 6-12 months. Therefore, ISO is urging businesses to get started with their ISO9001-2015 implementation project as soon as feasible.

0. INTRODUCTION TO THE NEW ISO9001: (descriptive section only)
    a. Process Approach: The requirements for applying the process approach are strongly emphasized in ISO9001:2015. A whole sub-section within the Introduction section is dedicated to explaining the Process Approach. It requires businesses to systematically define and manage not just their processes, but also the interaction between them. Companies, who currently have simple procedures written for each clause of the Standard, will be required to create some additional documentation.
    b. Risk Management: Unique to this version of ISO9001 is the ENHANCED EMPHASIS ON RISK MANAGEMENT, and integration of ANNEX SL. The basis for this is the assumption that (for business plans to remain effective in adverse scenarios), it is necessary for them to participate in risk based strategic planning, compile a list of potential risks, emergencies, threats, hazards, and dangers with contexts and impacts, and consider their capabilities, contingencies, backups, and the secondary and tertiary affects that events will have on all stakeholders. FEMA has addressed this issue for every business through the creation of CPG101 & 201, and CGC-1 and other guidance. Many industries have much more stringent requirements, via FAR agreements, compliance via contracts, and Legal obligations or mandates to follow various national and international standards and will be held to them separately from the Annex SL framework.
        1. EXAMPLE ANNEX: SL Framework components supporting Risk Management may include (e.g. Reference Documentation, Objectives addressing risk, Essential Functions assessment, Orders of Succession, Delegations of Authority, Resources, Support, Plans and procedures /SOP/EOP/OEP, Continuity Plans/Facilities/Communications, Vital Records Management, Human Capital safety and management, TT&E Programs, Audit & Review processes, mandatory Improvements, Devolution of Control & Direction, and Reconstitution Operations).
        2. EXAMPLE SPECIAL REGULATIONS (addressed outside of Annex SL requirements): Special circumstances, requirements and regulations that may pertain to (e.g. food, drug, chemical, biological, radioactive isotopes, medical, aviation, automotive, marine, energy, environment, defense, offense, technologies, imports, exports, legal, banking, schools, prisons, hospital-care centers, and other critical or sensitive products/services/facilities, especially CI/KR).

1. SCOPE OF THE QUALITY MANAGEMENT SYSTEM: (same as before, sets out the intended outcome of the Management System)
    a. Business Area Analysis: This is the examination and understanding of the business functions, sub-functions and processes, and the interdependencies, which requires consideration of (e.g. the major business functions, the business sub-functions and processes, which functions and processes are essential or critical to the continuity of the business, what are the businesses PRIORITIES). This information feeds into a continuous loop with the business Evaluations function including risk and vulnerabilities, and is conducted to ensure change is accounted for and included within a prevention strategy, analyzed for opportunities, and optimized.
    b. Delineates the intended outputs and outcomes (specific to the business) as per usual with consideration of the risk assessment and CONTEXT (expanded upon Clause-4).
    c. Certain aspects related to the boundaries of the quality management system will be documented here.
    d. CGC-1 (subsection 9a & Annex D), the intended outcome of Elements of quality and Elements of a viable continuity capability could be identified here. CGC-2 will help with identifying intended outcomes of essential functions.

e. The organization may have internal documentation and procedures as supplemental to the ISO certificate they hold. The specifications of the ISO certificate they hold (in this case ISO9001:2015) applies to completing the full 10 steps of the ISO documentation process, but also may include Technical Specifications (TS), Publicly Available Specifications (PAS), and Guidance for Implementation, Use, and Auditing as relevant.
f. ISO9001:2015 now contains seven Quality Management Principles: (see Annex B of the ISO9001 Standard), the last principle "Relationship Management" replaces the previously titled "Mutually beneficial supplier relationships" and broadens the business scope to encompass relationships with all stakeholders.

2. NORMATIVE REFERENCE: (same as before, provides details of the businesses and referenced standards or publications relevant to their particular requirements)
   a. Risk-Based thinking aims to prevent undesirable outcomes such as (nonconforming products and services) and additional information as reference values from similar organizations goods and services may be provided here and also given in the definitions section.
   b. The (establishment) of quality management systems (specific to the business objectives, risks, and context) aims to improve the organization, its products, services, processes, relationships, and resilience.
   c. The (implementation) of a formal quality management system is assumed to act as the first step in the creation of a corporate prevention program.
   d. The (Process Approach) concepts are distributed throughout the documentation. Many businesses have found that it is vital to their operations, and maintain its (Three) core concepts:
      1. Systematic Definition and management (maintenance) of processes and interaction of the processes. This is an important step to help the organization to achieve the intended results, consistent products, services, outputs, and outcomes in accordance with their Quality Policy.
      2. Defining a Methodology (e.g. Plan-Do-Check-Act) this applies to individual processes and to the system as a whole. This allows businesses to analyze how core processes fit together, evaluates success rates and bottle-necks, related to desired results the business sets out to achieve.
      3. Evaluating results of the Process Approach (which is incorporated within the Quality Management System) and requires the businesses to consider efficiency (but also opportunity and risks) at every step, and attempt to achieve alignment between the strategic objectives of the business and the quality policy. This should yield benefits, opportunities, and continuous improvements such as: improved Business Strategy, improved perspective for achieving key Business Objectives, enhance Performance, enhance Resource Management, enhance Quality, Safety, and Satisfaction through risk reduction.
   e. Documentation requirements: (the Auditors dream or nightmare depending on the circumstance) There is no specified requirement for a "Quality Manual," and there is no longer a set of specified mandatory procedures. ISO 9001:2015 clause 4.4 Quality management system and its processes currently states "organizations shall maintain documented information to the extent necessary to support the operation of processes and retain documented information to the extent necessary to have confidence that the processes are being carried out as planned." In reality, most businesses currently manage their documentation (policies, procedures, instructions, forms, records etc.) electronically, with the exception of hard copy documentation required by the IRS or other legal bodies. In other settings, the business might have to maintain lot numbers, biological “retention segments” or other components of their products, via some predetermined method and mandatory duration. The nature of those documents and items retained will be relative to the type of business, its approach to its QMS and the need to demonstrate compliance with the Standard, statutory, regulatory or contractual requirements.
   f. Purchasing: Referred to as the "external provider" suggests that (products and services) which are outsourced are included and controlled as appropriate by the QMS.

g. Compliance: As a general requirement, businesses must understand what statutory and regulatory requirements, (or any requirements from stakeholders e.g. customer contracts) are, and understand how the audit process relates to compliance issues.
h. Clause Exclusions: A statement has to be prepared stating and justifying the clauses or sub-clauses that do not apply to the QMS of a given Organization.

3. TERMS AND DEFINITIONS: (same as before, details, terms, and definitions applicable to the ISO9001 standard are given in addition to any formal business related terms and definitions)
   a. Emphasis on the creation of clear terms and definitions enables clear understanding between all stakeholders. Businesses should continue to focus upon the core text, common terms, and common definitions as per the previous ISO9001 standard.
   b. Businesses should also define areas where opportunities may exist to achieve more effective Process Management, or enhance desired outcomes.
   c. ISO 9001 defines a Management System as a set of procedures that an organization must follow to meet its requirements and objectives. A Management System Standard is a model used while operating the business or processes, (this is generally electronic and systematized in contemporary times).
   d. Definitions of elements of the Process Approach and requirements language used during transition to ISO9001:2015 should be as clear and simplified as possible (enables ease of auditing).
   e. The determination of risk includes identification and characterization of credible threats and hazards, their consequences, and our vulnerabilities. Risk factors that affect capability within the business and locally may include: local population and population density, the presence of critical infrastructure and key resources on the premises, location in high threat areas or high risk natural disaster areas, local capabilities available to prevent, protect against, or mitigate them. The relative importance of these risk factors in determining (where or how much of a capability is needed) varies by capability. The type and amount of resources needed are generally different in high population, high-density areas than in less densely populated areas. While each is important (for capabilities-based planning and national preparedness), determinations of vulnerability are critically important since they include not only exposure and sensitivity, but resilience.
   f. The “Preventive Action” requirements have been removed categorically, under the assumption that the new requirement to implement a risk based approach to quality management, effectively makes the QMS a preventive tool (in and of itself).
   g. Resilience is important to business stability and refers to our coping capacity to absorb events, adapt, and respond to and recover from their effects.
   h. Continuity is the ability of a business to continuously maintain its operations and functions during all circumstances and is described further throughout this document.

4. CONTEXT OF THE ORGANIZATION: (NEW, with 4 sub-clauses)
   Several new clauses (sections) require the organization to determine the issues and requirements that can impact the planning of their quality management system and how to account for them and/or control them by incorporating them as inputs into the feedback-loop for continuous improvement and development of the quality management system.
   a. CLAUSE 4.1 Context is the (prerequisite) information needed for understanding the business and its objectives, but is also critical information for Risk Management and “Risk-based thinking” (NEWLY emphasized in ISO9001:2015). Businesses will need to determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its management system. The THIRA tool is a FEMA product that can assist with categorizing threats, hazards and giving them context.
   b. CLAUSE 4.2 Understanding and document the needs, expectations, and requirements of Interested Parties. This may be in the form of specifications, quantity, quality, timing duration, delivery type, and many other aspects the customer may need or desire. This sub-clause relates to policy, scope

and Clause 4.3 in that the boundaries that businesses must consider are expanded to include required assessment of customers as components of the businesses Management System.

c. CLAUSE 4.3 A loop-back cross-check requirement that emphasizes the consideration of the Context broadly while determining the Scope of the Organization.
d. CLAUSE 4.4 Determine the organizations relevant issues, both inside and outside, that have an impact on what it is trying to achieve, its intended outcomes, including the boundaries and range values of the Quality Management System. The businesses boundaries are aligned with the business objectives.

5. ORGANIZATIONAL LEADERSHIP: (Newly emphasized, with 3 sub-clauses, similar to NIMS)
   a. CLAUSE 5.1 Leadership and Commitment: Whether realistic or not, the emphasis here is for top management personnel to play key roles in the management system such that they oversee the integration of all appropriate components of the organizations business processes, ensuring they achieve their intended outcomes, and have adequate resources for uninterrupted production. This includes features of organizational Structure, and Work-flow (as a function of personnel and objectives), relates to authority, efficiency, and effective communications across one or multiple facilities, this might also include overseeing resource typing and inventory management. The business will define leadership's commitments to the project, and obligations to perform auditing or consulting for process and safety evaluations and other business and process specific requirements.
   b. CLAUSE 5.2 Policy: The policy must reflect comments and dialogue demonstrating satisfaction of requirements for continual improvement, and also contains the typical rules, regulations, and procedures of the business. The new risk management integration throughout implies that policy will consider management of Essential Functions, critical process, applications, COOP capability, backup functions, on-hand resources, acceptable (attributes, timing and rates) of production.
   c. CLAUSE 5.3 Organizational Roles, Responsibilities and Authorities: This clause (as with the planning section), contains components from Orders of Succession (see CGC-1 Annex E) and Delegation of Authority (see CGC-1 Annex F), Devolution of Control and Direction (see CGC-1 Annex L), as a matter of ensuring a through documentation process. Also included are Top Management Responsibilities, division of labor, tasking for auditing, committees and review processes and the like. Organization, structure, function and capability all feed into one another such that if one is modified the others will change and require re-evaluation. Top managers must evaluate and ensure the management system requirements integrate into the Organizations core Business processes, are functioning in an efficient way, priorities are being communicated, and awareness issues are addressed as components or processes become dysfunctional. A given duty, authority, competency and resource or equipment is associated with a given set of personnel, (and therefore must be evaluated together), to ensure their duties are fulfilled and the given business capability remains available and functional.

6. PLANNING: This section contains a comparison of CGC-1 continuity planning principles, versus ISO9001:2015 requirements, and a brief discussion of common business planning problems. In contemporary times, an incident may have a mix of political, economic, social, environmental, public safety, public health, supply chain, and other financial (or sustainability) implications with potentially Local, National, or Global serious long-term effects. All corporations at baseline are assumed to have their by-laws and reports in good order as per National, State and Local requirements (as well as per American Code Enforcement or Municipal Regulations Enforcement). Planning also assumes the typical Naming of an Executive board, Objectives, Committees, Members, Officers, Duties, Authorities, Meetings, Evaluations and Amendments are in place and functioning according to a schedule. Planners are concerned with the operation of the organization and setting out the form, manner, or procedure in which a company or organization should be run. The NEW ISO9001:2015 planning criteria carefully considers the results of risk management within the overall context of the management system, and the development of plans, policies and procedures to address the physical and/or business consequences of residual risks (which are above

the thresholds of acceptance defined in several clauses) to the business, its assets, occupants. Plans may be standalone or consolidated but must be integrated, and it is critical to plan to fulfill Management System objectives as well as planning to address risk and optimize opportunities related to all stakeholders. Below is a comparison of some National Policy and Planning Standards versus the new ISO9001:2015 planning standard.

a. NSPD51/HSPD20/NRF/NIMS/CGC-1&2 PLANNING HIGHLIGHTS:

The directives NSPD51/HSPD20 specifically relate to the importance and mandate of establishing, developing and maintaining plans, processes, and guidelines that ensure Continuity of Operations including a TT&E program. The following highlighted planning requirements may generically relate to minimum Standards.

1. The business must plan for (and later conduct) a full "Business Process Analysis" which is derived from the (Business Scope - "Business Area Analysis"), and is a method of examining, identifying, and mapping the functional processes, work-flows, activities, personnel expertise, systems, data, and facilities inherent to the execution of a function or requirement.
2. The business should design a plan based upon inputs and information from the (Evaluations Section - "Business Impact Analysis"), and the THIRA process which will determine the risks, opportunities, and contexts that need to be planned for to ensure the management system can achieve its intended outcomes, prevent, or reduce undesired effects, and achieve continual improvement.
3. The Management System Plan is a plan created to systematize all processes, ensure quality monitoring of all components, and scheduled evaluations and improvements. The initial steps are generally to create and ensure integration among the following (Five) common types of plans:
    - Planned Procedures, which may include overviews, standard operating procedures, field operations guides, job aids, or other critical information needed for operations and responses.
    - Incident Management and Response Plans, (e.g. EOPs, warning systems, communications in support of incident management functions, and contingencies), the "management" component plans for how operations, logistics, resources and funds will support occupational health and safety, restoration of systems and structures, transitions, resumption and communications associated all conditions within the business including during an incident. The response component plans the reaction to the incident in an effort to: (TOP PRIORITY-protect personnel), assess the situation and property, stabilize the situation and conduct responses that support the viability of a business, coordinate and control crisis, and reduce or mitigate disruptions.
    - Preparedness Plans, which describe how training needs will be identified and conducted to ensure a safe environment, how resources will be obtained, and the facilities and equipment required for (e.g. evacuating or sheltering), will be leveraged to address the threats or hazards faced by the business. During formulation of the business preparedness plan the committee or Threat Assessment Team (TAT) will Identify Risks and Consequences (see THIRA reference), they will then Project Resource Needs by reviewing similar case histories and consulting individuals who have dealt with similar circumstances. They will then design a preparedness cycle which includes revising and optimizing the stages of planning, training, equipping, exercising, evaluating, and taking action such that they correct and/or mitigate events to the satisfaction of all stakeholders. Upon developing a plan to continually strengthen then maintain the relative state of a preparedness program, the business must question their current "Level of Preparedness" then reconsider preparedness in the context and complexity of various operating scenarios. In example, a disruption could render the organizations leaders incapable of fulfilling their duties, authorities and responsibilities, therefore, to improve preparedness level, the auditor may find that the organization could plan for

additional mentoring or drills (that represent the most likely incidents that may be encountered and/or order of succession changes that may result).
    - Corrective Action or Mitigation Plans, which include activities required to implement procedures based on lessons learned from actual incidents or training and exercises.
    - Recovery Plans, which describe the actions to be taken to facilitate short-term and long-term recover when issues occur.
4. Essential Functions as discussed in the Scope section (also see CGC-1 Annex D), the organization should plan to ensure it can perform its Essential Functions under all conditions, including relocation procedures, and attaining operational capability at all continuity facilities within the minimal acceptable period for essential function disruption. Identifying Essential Functions is critical to planning for Continuity of Operations during incidents.
5. Planning for Essential Records Management corresponds to (see CGC-1 Annex I), The IRS requires most businesses to retain certain hard copies 3 years up to indefinitely depending upon what it is or the circumstance. Additionally, many companies require hard copies as charts, diagrams, medical and dental records, while other records may become “digital only” (paperless) extending continuity requirements to include external access to a given records system.
6. Planning Human Resource Continuity corresponds to (see CGC-1 Annex j). This entails activating personnel who will assist with an incident, and supporting personnel who typically do not perform any element of continuity. Instructions, Procedures and Expectations generally take the form of an Occupant Emergency Plan (OEP), emergency equipment, supplies and alternative duties. The business should evaluate options that will safeguard and reduce the loss of life and minimize property damage and loss, including a protection plan to secure personnel, facilities, equipment, records related to personnel, and other assets critical to all personnel and the performance of essential functions by the personnel in the interim of a disruption. NIMS compatibility requirements for individuals fulfilling these functions should include certifying that personnel possesses at least the minimum level of training, experience, licensure, certification, and fitness to perform the relative duties and/or during a crisis response.
7. Planning Continuity Communications corresponds to (see CGC-1 Annex H), and is the ability to communicate under all conditions (discussed below in the Common Planning Problems section). Internal Risk Communication is the exchange of risk related information, concerns, perceptions, and preferences within an organization and between an organization and its external environment tying together the management system with the risk management functions. Risk communication planning requires consideration of (e.g. who is at risk, who do we communicate to about risk, what do we communicate about the risk magnitude or impacts, and how do we communicate about risk or obtain support for potential cascading events).
8. Planning Continuity Facilities and Operations, (see CGC-1 Annex G), enables the business to continue operating under a wide range of circumstances. This is not always an option for all Organizations, and incidents may be mitigated in other ways, such as ensuring that the objectives and responsibilities are fully delegated, there are backups, telework options, (off-site equipment, supplies, resources, assets), alternative systems and infrastructure available from which organizations can perform essential functions at all times. Backup resources are made available such that the organization may achieve the timely and orderly recovery and reconstitution from an emergency.
9. Ensure and validate continuity readiness through a dynamic and integrated continuity TT&E program and all-hazard operational capability if possible (this program reveals many issues including the human error element, and informs priorities by uncovering vulnerabilities, personnel issues, or other weaknesses). Subsequently, the new results obtained will inform priorities, resource allocation, equipment purchases, influence policy or program decisions, and become the basis for future education, training, and evaluation.
10. Improvement plans are formulated as issues are recorded and overcome through a Corrective Action Program that enhances quality, efficiency and readiness. The process of evaluating and

determining the organization's readiness posture (and for decision-making) regarding its corresponding actions (e.g. to increase its capabilities) may generate information used to produce new standard operating procedures (SOPs), and additions to emergency operations plans (EOPs). Establishing and integrating experts or other Organizations into a collaborative relationships program (as multiple entities associated with the business) may ensure that knowledge, experience, and additional options are explored (before, during and after an incident). Having a community of collaborative relationships may also extend communications and other systems support and functions availability in the advent that the organizations budget cannot support the complete spectrum of incident management options or actions on its own.

11. Planning for Devolution of Control and Direction, is important for a smooth transition and continuous productivity in normal circumstances, and is critical in major incidents, such that order and direction and authority within the organization are maintained.
12. Restoration, Recovery, Reconstitution, or Transitioning, (with the exception of data-backups, business recovery plans are difficult to create, unless an entire other facility exists). It is easier to state here that, this is the process whereby personnel are informed of when and how they will begin normal operations post-incident (either from the original facility, or as they move to a new facility), including performing safety checks, piecing together available equipment, establishing and maintaining essential functions, testing and updating the management system, and giving status updates to all stakeholders.

b. NEW ISO9001:2015 PLANNING STANDARDS:

The ISO9001:2015 plans contain 2 clauses that expect the business plans to contain actions that will address potential risk and opportunities, as well as a strategy to achieve their objectives. Identified risks, vulnerabilities, and contextual requirements, will be planned for and address as to who, what, how and when to proceed, under what authority and/or policy. The implication here is that a proactive and integrative risk management planning approach replaces (having a separate preventative action section) and reduces the need for corrective actions later on in the improvement plan.

1. Top Management & Committee Review plans: The planning process must be in a continuous feedback-loop with all other processes, align with business policies and objectives, and particularly the components of continual improvement including fact gathering of information from the customer (e.g. target time frames and assurances). Other review objectives may include specifications for control of the product (qualities and quantities), operations, finances, risk management practices, safety and security of (facilities, personnel, equipment and trade secrets, alerts and awareness topics), emergency/short-term/long-term and off-site resources and planning, information services, when and how to perform notifications, what corrective actions and preventive actions continue to be relevant, and what additions to make.
2. Planning Objectives: Risks and opportunities impact policies and objectives. The auditor checklist might generically include evaluation of whether the business has planned objectives that are in line with its policies, considers risks and opportunities, can measure what ought to be measured, are monitored, communicated, and updated or reported when needed. Planned objectives must be relevant to the functions and processes the business desires to utilize to achieve its purpose, outputs, and outcomes.
3. Risk Planning: This is planning for preparedness, response, priorities associated with the likelihood of occurrence, and how to prevent, avoid, eliminate, minimize or mitigate outcomes and consequences of events. Planning should including taking a risk-based assessment to determine internal requirements for safety, protective equipment, operational control, document control, and to evaluate and deliver the (type and extent) of controls appropriate to each external provider and all external provisions of goods and services including (what, who, how and when). The Auditor will require the Organization to ensure adequate plan mechanisms to prevent, or reduce, undesired effects, and ensure that it can achieve its intended outcomes and make continual improvements as the environment changes.

4. Quality Plan: Each business will consider what works best to produce the best outputs, products, services, and outcomes, given the variables of risk management, costs, efficiencies, and other parameters pertinent to their service or production niche, but is also beholden to (Local and National requirements, existing license requirements, certifications, and standards where pertinent).
5. Quality Policy: This policy includes all requirements related to the businesses license, certification, commitment of personnel, commitment of resources, commitment to protect business assets and process secrets. Changes to the policy related to ISO9001:2015 new structure (from Annex SL) will require updating policy documentation to reflect this new structure and the incorporation of detailed information for implementing "Risk-Based Thinking" policies. Elements of the business policy will relate to the business Scope, by detailing the boundaries of procedures related to minimum requirements for conforming products, objectives for safety, efficiency, improvements, reliability, continuity and requirements for satisfying customers.
6. Management Review Process: This technical component identifies each process as (e.g. adequate, effective, the need for changes, compliance issues, and opportunities for improvement). It is also related to reviewing records and maintaining a particular schedule of (who what when where why how) the performance evaluation will be conducted. Feedback from Evaluation components will also be reviewed and tie into Risk Management to make strategic decisions on how business risks will be treated (e.g. whether to mitigate, ignored, reduced, transfer, or avoided a given risk). The Risk Management review should incorporate components of THIRA, business area analysis, business impact analysis, risk communication, and risk-based decision making functions, to plan for the best possible contingencies, continuity options and business outcomes.
7. Quality Audit Procedures: This technical component relies upon objectives, scope, normative terms, definitions, and plans for quality, and delineates what to test and how to test it, including requirements of (e.g. system performance measurements, compliance, sampling, competency tests, and other variables unique to the business). Auditors will likely observe, how well, or how quickly an action can be performed and if it is reported or expressed in ways that can be observed during normal processes or abnormal circumstances to assure quality.
8. Quality Systems: (combined into the overall Quality Management System), businesses are expected to have a systematic approach to all aspects of their quality assurance program and quality procedures. This systematic approach includes Standardized Operating Procedures, and management systems that enable all of the business procedures to be evaluated for risk, reliability, customer satisfaction, as well as "outputs" being managed, tracked, sampled, validated, documented, audited, and controlled in other ways unique to the business.
9. Relationship Management: (previously called "Mutually beneficial supplier relationships") is assumed to be planned for and incorporated into the Quality Management System, (additional discussion is included in the common planning problems section below).

c. COMMON PLANNING PROBLEMS:

An expert I discussed Organization planning with stated that 4 facets of planning are regularly found to be weak among Non-government Businesses and Organizations as follows:

1. Communications Plans: In disaster scenarios, we can't always depend on the telephone, cell-phone, and internet, therefore the following actions can be taken to enhance this condition.
    - Interoperability: The business can implement communication mechanisms that will allow emergency management/response personnel and their affiliated organizations to communicate with the business and help the business communicate with its personnel or with their customers or partners across anywhere via voice, data, or video in real time, when needed and authorized.
    - Reliability / Flexibility / Scalability / Portability: businesses can ensure that regardless of cause, size, location, or complexity of an incident, communications systems are available that can withstand and continue to perform after damage or loss of infrastructure.

- Resiliency and Redundancy: Businesses can ensure multiple forms of communication devices and information systems (designed to function in any type of incident) are available. This includes backups, and extra resources to utilize in the event of a disaster. Businesses should not rely solely on a sophisticated but vulnerable network of support systems.

2. Multi-Facility Multi-Stakeholder Relationship Planning (as relates to Local Community Preparedness): The problem here is that businesses typically understand their roles, but do not understand the roles that other businesses and agencies will play in the scheme of an incident. A given business or individual may become the recipient of aid, or may become key to the local relief effort depending upon circumstance. The integration of a business into the community is complicated but begins with identifying and building relationships, and planning for multiple stakeholders, and response or aid capabilities. Said interaction with multiple stakeholders can validate assumptions about needs, capabilities, and potential reactions to a given incident. Organizations having knowledge about specialized resources that can be brought to bear in an emergency may become critical to the outcome. Local private-sector stakeholders who are involved in relief or have useful information may include NGOs (such as National VOAD, or American Red Cross) and other not-for-profit, faith-based, and community organizations. This knowledge might include Lists of shelters, feeding centers, and distribution centers, knowledge about special-needs populations, local business and industry representatives, knowledge about hazardous materials that are produced, stored, and/or transported in or near a given business. Also, knowledge about SPECIALIZED facilities, personnel, and equipment resources that could be used in an emergency, (e.g. local Amateur Radio Emergency Service, debris removal options or coordinators, suppliers of emergency equipment or trucks, or other experts such as building inspectors or Veterinarians for livestock injuries).
3. Participation, Human Resources, and Risk Management (as relates to Threat Hazard Identification Risk Analysis process): Organizations might identify risks, but often fail to adequately identify vulnerability or map their Personnel's Training to complexity or to the Level of capability required at the facility to meet the needs of a given incident. Organizations can address this by assigning Emergency duties to select personnel such as (e.g. designating specific COOP professionals to be activated in the event of an Emergency whom are adequately trained).
4. Knowledge Management (KM): The KM process describes the acquisition, assurance, representation, transformation, transfer and utilization of information supporting the Business, including (e.g. Environmental Sensing, Signal Detection and Monitoring, Organizational Learning or Sharing). Outside of Government Agencies, Knowledge components and Lessons Learned are frequently underutilized, because it is labor intensive and costly to continually monitor the relevant internal and external environment of the business, detect, communicate, document, and/or initiate appropriate actions related to all types of incidents. The Organizational Learning component of (KM) is the (development and support) of mechanisms that allow the business and its members to review and analyze documentation, gain insight and understanding (learning) from individual and shared experience, and the willingness and capability to identify successes and address failures for the purpose of organizational improvement.

7. SUPPORT: (mainly old content with a new structure, contains 5 clauses)
The organizations context, commitment, and planning, all feed into the requirements for providing support elements and functions to meet the organization's internal objectives, goals, and external obligations and dependencies. From an auditor's perspective, (internally) this may include availability of essential Resources, ensuring Competence, Awareness, Communication, Documented information, Creating and updating processes, maintaining options to Access and Control Information, and ensuring Business Continuity options. From a Local and National perspective (externally) this may include the importance of the organizations role to a given Emergency Support Function (ESF), role as critical infrastructure, support to a given supply chain, or other dependency (see the ESF reference below for details).

a. CLAUSE 7.1 Resources, I'm aware first hand that Franchises have many predefined options that they must adhere to, and therefore, a wide variety of resources and functions unique to a given business may be outlined here. Generally for all businesses, (from an Auditors perspective), the organization needs competent personnel to supply adequate resources that will enable deliver of its goods and services uninterrupted during all conditions. The business resources should be typed and inventoried, and contain NEWLY added contingencies or backup plans and capabilities. Essential resources are derived from the businesses EOP, OEP, THIRA, and process requirements, planned for and allocated.

b. CLAUSE 7.2 & 7.3 Competency and Awareness, (go hand in hand), and are relate to education, training, credentialing, record of errors or reported incidents, management of communications and evaluation of performance criteria for the most common scenarios. Auditors know that managers achieve awareness when they are in-tune with their internal and external business processes and environment, communicate effectively with their subordinates, and have adequate mechanisms to monitor and sample their business. Competency will be maximized in an environment that values quality, balances it against efficiency of processes, enhances employee satisfaction and retention, and ensures customer requirements are met, while integrating post-evaluation courses of action into a continuous feedback loop of optimization.

c. CLAUSE 7.4 Communications must be supported and are discussed further in (the plans section, in continuity, and below in coordination). Support may include (WHAT additional options or resources can be used, WHEN additional options may be used, and WHO are the additional support personnel the business may communicate with in a given circumstance). As a support aspect of this function, businesses assume responsibilities to procure extra resources and provide capabilities necessary to ensure they are able to maintain communications during incidents.

d. CLAUSE 7.5 Documented Information (discussed in planning, support, and in operations), requires personnel support, Information Security support, resources, storage, organization & maintenance & replacement, legal regulations and utilization policies, distribution, disposition, and other scheduled practices. The information will have backup contingencies, and should identify and designate who does what and when. An important way that documented information supports personnel (search and rescue) is through maintenance of a list of all personnel who can enter the building and a mechanism to identify (who's currently in the building) in the event of an incident.

NOTE-4: CGC-1 gives pertinent examples of support and coordination that non-Federal organizations may undertake include: Collaborating to incorporate capabilities of other entities into the organization's continuity planning and exercise activities to the extent possible; Coordinating on risk assessments to identify hazards relevant to the organization's mission and location; Partnering with these entities to develop continuity plans that are coordinated to the extent possible; Participating in Continuity Working Groups (CWGs), information sharing, training, and exercises, as appropriate; Coordinating OEPs, shelter-in-place plans, and regional and local evacuation plans; Participating in existing alert and notification networks and credentialing initiatives, as appropriate; Working together to identify interdependencies and ensuring resiliency with critical infrastructure and services at all levels; Coordinating continuity resource and security requirements, as appropriate; Participating in other coordinating activities, as appropriate.

8. OPERATIONS: (mainly old content with a new structure)

Effective operational control requires a systemic approach to understanding the business processes within the context of (e.g. the organization's objectives, scope, culture, beliefs, resources, organizational structure, clients and other stakeholders). Business-wide processes, programs, and structures, should be aligned and integrated with the overall Management System. The main focus is on Operational planning, implementation and control of processes, and auditing to ensure consistency with plans created in Clause-6, (e.g. such as planning process criteria, controlling the processes within the criteria, controlling planned change, addressing unintended change, and addressing emergencies and risks) as necessary.

a. A business's current operating procedures are expected to contain NEWLY implemented Risk Management practices as part of the "Risk-Based Thinking" requirement of ISO9001:2015.
b. This section/clause may also include aspects from ISO9001:2008 (old clause 7 objectives) listed here as business and project Objectives and Plans for what use to be called "Product Realization," and typically contains information such as: Customers, designs, growth, development, tasks to be completed, verifications, purchasing, schedules of availability, and time-lines for review and renewals.
c. With regard to "Control of External Provision of Goods and Services," the organization is required to take a risk-based approach to determine the type and extent of controls appropriate to each external provider and account for all external provision of goods and services. This sub-section represents service support functions for many organizations, and addresses all forms of external provisions. Therefore, whether it's by Third Party Administration or by purchasing from a supplier (through the outsourcing of processes and functions of the organization), everything should be documented and accounted for and controlled through the Quality Management System.
d. The "5 common types of plans" are put to ACTION in operations (see the above Plan section for details). As the business processes begin to fulfill each of its objectives, and as these plans unfold, the typical components of an organizations SOP must integrate well with the EOP to adequately manage risk and safeguard operations. To ensure safety, the business may include additional designs or develop additional occupant safety strategies, Emergency Preparedness and Response options, and additional mechanisms to monitor and sample all processes.

9. PERFORMANCE EVALUATION: (previously part of clause 8)

Each component of the organization is evaluated in the context of the current circumstances with which it is operating, processes as they occur, its policies, objectives, plans, and scope. A TT&E program is mandatory for Government Agencies to ensure obsolete plans do not provide a false sense of preparedness, and is used in ISO9001 certified businesses for similar purposes as well. The performance evaluation is a process that must be supported by mechanisms that allow for collection, analysis, conclusions, and reports such that corrective actions can be taken and incorporated into future revisions of all pertinent procedures. Auditors will be looking at What, How, and When an organization is monitoring its processes, conducting QA, taking measurements, conducting internal analysis, evaluation practices and personnel, creating documentation, the management review process, and other actions specific to the organization. Typical components of evaluation may include the following.

a. CLAUSE 9.1 Monitoring, Measuring, Analysis and Evaluation: The Management System Internal Evaluation process (compliance check), is usually a scheduled process that helps determine if the all processes are going according to plan and each component is in compliance with the requirements of the organization and considers measurements and samples as feedback-loop inputs from every process, risk management analysis, and corporate quality planning and to ensure the current standard is met and is effectively implemented and maintained.
b. The Internal Audit: (as a product evaluation), relates to the outputs, outcomes, goods and services as well as validation the processes involved. Products may also be audited for quality through processes of analyzing, measuring, sampling, and in some cases evaluation of (nonconformities and corrective actions versus past issues), as well as consideration of in-house or third-party issues such as (e.g. preservation, packaging, transportation or delivery methods). Reports are then created, acted upon, retained, and become inputs into the next round of evaluation. Many other aspects of the business are audited as deemed relevant and necessary to assure satisfactory evidence of good standing, and rule out potential violations.
c. Periodic Risk Evaluation: planned for as a part of the proactive prevention mechanisms that ensure safety and conformity and feeds into the overall Quality Management System. This considers the Business Area Analysis (in the Scope Section) and the planning conducted to ensure adequate Risk Assessment, and Business Impact Analysis.
    1. The Risk Assessment – CPG 201 THIRA can be utilized to identify (or anticipate events or sudden changes to the operational environment), analyze potential threats, hazards and

vulnerabilities that can impact the business and evaluate the context, the response capabilities, and the existing or potential controls that can reduce risks. Risk assessment requires consideration of what can go wrong (identification), what is the likelihood that it will go wrong (facts, statistics, probabilities), what are the consequences (minor, moderate, severe), and what controls may be brought to bear.

2. Business Impact Analysis – This involves applying the results of the risk assessment (or THIRA process if used), to the Business Process Analysis results to determine potential consequences or impacts that will be used to enhance or improve identification, prevention, preparedness, response, recovery, and to control continuity and restoration capabilities that will protect the business, occupants, and functions in the event of an incident. The business impact analysis requires consideration of how potential threats and hazards will impact business functions, sub-functions and processes, the validity and context of hazards, the competency of personnel, and the status of controls that are currently in place. This process aims to match a contingency with each issue affecting an organization's ability to perform essential functions, deal with personnel changes, deal with communication issues, ensure policy changes enhance the business, guard against the impact of mechanical failures or external provisioning changes or environmental changes, and various other impacts of (or during) an incident. Analysis also includes the inputs from the Management Review, this evaluation looks at whether the management system is suitable, adequate, and effective on the context of various conditions. It may also involve conducting further Evaluation of the management system, facilities, personnel, supply chain and other aspects of the business. Analysis also includes Periodic Customer Feedback (internal and external customers), and ensures requirements are met and satisfaction is achieved.
3. GAP analysis and transition assessments: This analysis may be conducted for several reasons. In the context of ISO certification, the business will check their current status against planned future change (such as the transition to NEW ISO9001:2015 requirements) then identify ways to correct and/or communicate all gaps and issues found to relevant stakeholders. Another type of transition analysis relates to ensuring gaps are addressed when a business is affected by an incident and must move to another location. Analysis also includes evaluation of other non-critical elements of the Organization (as seen within the above Planning section), and although these elements may be important to the business, they may or may not be a high priority item on the Auditors agenda.

10. IMPROVEMENT: (previously part of Clause 8)

This clause looks at how nonconformities and corrective actions should be managed to achieve continual improvement. The target objectives are to achieve conformity and customer satisfaction through opportunities and the use of a Quality Management System, that utilizes a standardized framework, environmental controls, infrastructure and process adjustments, technologies, and other methods to establish a sustainable healthy state which is dynamically optimized and maintained over time to ensure, compliance, efficiency, and appropriate resource/asset management. In the short-term nonconforming products are identified and corrective actions are taken. In the long-term Quality Management System is involved in a feedback-loop, ideally informing technical committees, who will update all business processes including the quality control manual, create and maintain documentation and other records that will improve the business policies, quality, efficiency, and management systems over time. In some instances where a business cannot finance a given backup or continuity contingency, the Quality Management System may enable mechanisms to improve outcomes or mitigate issues via other ways and means.

a. ISO9001:2015 NEW Opportunities:
    1. By considering associated risks throughout a process, it may be possible to improve upon the businesses products, services, and outcomes throughout each stage of the process.
    2. Risk Management analytical processes always provide opportunity to collaborate with others (especially while negotiating Public-Private relationships or the creation of Memorandums of Understanding, or Mutual Aid Agreements).

3. I believe DHS/FEMA may be able to support business transitions to the new standard through education and training, which could be made more available to businesses to achieve successful creation of the Risk Assessment component of the NEW ISO9001:2015 standard, or optimize continuity plans, or for other mutual benefits.
4. Auditing of the Risk Management components of a given businesses Quality Management Systems may provide insight into vulnerabilities or other issues, that would in-turn be addressed accordingly, and improve safety and stability, while providing nationally relevant data about the business.

b. ISO9001:2015 NEW Improvements:

The business will make improvements to the safety and security of the facility by conducting "Risk-Based Decision Making," which draws upon the results of the risk assessment, business area analysis, and business impact analysis, then proceeds to further improve upon the risk management strategy (risk reduction, risk transfer, risk avoidance, acceptable risk), as well as context, and objectives and the allocation of resources to meet those objectives. Risk-based decision making is a continual process that requires continual COMMUNICATION (dialogue with all stakeholders), and input from the (evaluations, samples, and monitoring of the business). Risk decisions will require adjustments, made related to economic, public relations, and other impacts of current circumstance and previous decisions made and implemented. Risk-based decision making requires the consideration of whether the risk may be reduced, the availability of interventions (controls) to reduce risk, combination of controls that "make sense" in the context of the organization, prevention policies, objectives, and readiness or continuity posture. The THIRA corrective action template may be used here to work through implementation of new controls or actions. I also note here that two clauses (not only address preventive action) but go above and beyond as a proactive impetus (and input) for improvement.

1. Clause 4.1 – The business will determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its management system." The management review and improvement processes will capture this information and utilize it to improve.
2. Clause 6.1 – The business will plan for the risks and opportunities that need to be addressed to assure the management system can achieve its intended outcomes, prevent, or reduce undesired effects, and achieve continual improvement. The business will implement these plans, review information as it is collected, and evaluate options that will reduce or mitigating disruptions to operations, and enhance stability.

c. ISO9001:2015 Transition:

Implementation of the NEW changes successfully will require businesses to conduct and evaluate the results of GAP analysis/transition assessments from the old ISO9001:2008 to the NEW ISO9001:2015 standard. The Business must taking a fresh look at the Management System, creating a plan to meet the capability and process targets, change their documentation to reflect the new structure, and begin NEW monitoring of processes and for nonconformance, weaknesses or other unforeseen vulnerabilities (also see the Rudimentary Next Steps section).

NOTE-5: Risk was previously a Preventive Action clause in the former ISO9001's, but is now integrated throughout the standard. Incorporation of "risk management" mechanisms is recommended under the premise that organizations who maintain a risk-based approach are more likely to achieve their objectives, because they are more capable of being proactive (rather than being reactive) to adverse events due to the fact that prevention is automatic incorporated into a risk-based management system.

ISO9001:2015 LEGAL IMPLICATIONS OF NON-COMPLIANCE OR NON-CONFORMANCE:

Auditors will utilize information from within the 10 clauses as a clear and concise list of objective evidence to identify and confirm the presents of safety issues, inefficiencies, policy issues, and nonconforming goods and services. Legal evaluation will likely include the organizations goals and intended outcomes, internal and external issues, previous auditor negative remarks, record of injuries, violations, or compliance issues, relationship with relevant stakeholders and the history of fulfilling their requirements within the scope of the business management system. Additionally, Quality Management System compliance information can be accessed in lawsuits through legal discovery (e.g. Technical Files, Annex I Checklist, Harmonized Standards, Declaration of Conformity, Notified Body Certifications, and Surveillance Audits). One basis for this is ISO17021:2011 Conformity assessment – which entails the requirements for bodies providing audit and certification of management systems. Several cases have established legal precedent through the Machinery Directive and other broad industrial safety compliance issues. Also, the requirement "Control of monitoring and measuring equipment" leaves room for expansion into many other areas of (gross negligence or dereliction) whereby clear standards had been established, and licenses were issued under the expectancy of conformity with that industrial standard. Quality Management Systems are now (additionally) being used by many Businesses to ensure Product Liability Exposure control and for Product Liability Avoidance as well. As an everyday practice businesses should strive to achieve compliance (in any regard) because systematized risk management practices have been found to keep employees safe, improve customer confidence, ensure greater knowledge and preparedness, increases the probability of reaching objectives, and reduces the probability of nonconforming results or litigation.

NOTE-6: During the transition period, the ISO9001 Auditing Practices Group (APG) will begin working with those who desire to achieve the new certification. The ISO9001APG are quality management system (QMS) experts, auditors and practitioners, who will be drawn from the International Accreditation Forum (IAF) and the ISO Technical Committee 176 Quality Management and Quality Assurance (ISO/TC 176).

OTHER STATUTORY AND REGULATION REQUIREMENTS:

Many business requirements are on a case-by-case basis and beyond those of Annex SL framework, and the scope of this document.

RUDIMENTARY TRANSITION STEPS TO CONSIDER:

The FDIS of ISO9001:2015 is released, therefore, Emergency Managers & Government Officials, and other subject matter experts have until September 2015 to evaluate the above statements, evaluate changes to the New ISO9001:2015 release, and levy their final requests for improvement of the ISO as relates to integration of Private-sector partners, enhancing community resilience, advancing their INTERESTS, and evaluating other arguments made within this topic.

a. Business must carefully consider the 10 clauses discussed herein (and within Annex SL Framework), identify gaps that may occur, take into account and reflect these changes within businesses processes as they are evaluated during the transition FROM ISO9001:2008 to ISO9001:2015.
b. To facilitate effective organizational implementation of the ISO9001:2015 standard, businesses must utilize a Process Approach (with work instructions) that enables analysis of project designs, evaluates objectives and inputs (requirements) and expected outputs (clients satisfied with a conforming product), documents management responsibilities, manages resources effectively, measures process improvement, implements protective and preventive actions (controls, inspections, reporting, tracking, removal or disposition), as well as the (e.g. skills, knowledge and competence of personnel) engaged in the processes.
c. Business Documentation revisions should demonstrate the new structure and functions of ISO9001:2015 as per the complex environments in which the organization operates. This may involve re-mapping what roles the business offers with respect to the services and resources they

provide to their customers and the degree to which these customers rely on the business to provide said services and resources (this is especially important during a disaster). In the disaster scenario, the typing, nature, and quantity of backup resources, contingency plans, and provisions becomes a very important part of customer requirements and satisfaction (and should be mapped accordingly).

d. ISO9001:2015 NEW Risk Management (risk-based thinking) provision:
Risk as the effect of uncertainty on an expected result can be assessed using DHS/FEMA CPG-201 the THIRA process, and continuity evaluated using principles from CGC-1 guidance. If the risk assessment results demonstrate any potential deviation from expected outcomes, they must be PLANNED for to assure safety and conformity. The planning involves IDENTIFYING and PRIORITIZING what deviations could happen, what their effects might be, and the likelihood of the deviation occurring in a variety of CONTEXTS. During planning, managers should consider the definitions component of Risk-Based Thinking as being important to describe (what's acceptable and what's unacceptable risk or probability), and what are the advantages or disadvantages (or trade-offs) involved in the options available to them. Businesses must strive to apply a Process Approach to risk management and control all processes to avoid adverse outcomes, secondary and other impacts to all stakeholders. Additionally, it is important to consider the scope and boundaries of the business and the design of RESPONSE and READINESS mechanisms to monitor, warn, interdict, (save lives), avoid conflicts, eliminate risk, and maintain COOP processes to recover or transition to a new facility all together. Auditors will likely assess the businesses establishment of a proactive culture of prevention and improvement, and ability to monitor and verify the effectiveness of the actions, consistently implement processes that contain the least risk to all stakeholders and least impact on the quality of goods or services.

e. Coordinating ISO9001:2015 Business standards with DHS/FEMA APPROVED continuity, security, preparedness, and resilience standards:
Businesses should carefully consider the impact the new standard will have on Leadership and relationships, and conduct further research and evaluation of suggested educational topics from FEMA's website, with consideration of their role in a given community (also see reference links provided at the end of this topic). Risk Management can be handled in many ways. The model and standard your business will require depends upon the nature of your organization. Congress through the Dept. of Homeland Security (DHS), has directed the creation of "PS-Prep" which enables business safety practices to be enhanced through the following three DHS-approved Standard certification options:

1. NFPA 1600: (2007/2010 editions): Disaster and Emergency Management and Business Continuity. This standard is for businesses seeking a holistic approach to preparedness; it addresses organization management, risk assessment, prevention, mitigation, resource management, response, continuity, and recovery.
2. ASIS SPC.1-2009: Organizational Resilience and Security Preparedness and Continuity Management. This standard is for businesses looking for the steps necessary to prevent, prepare for, and respond to disruptive incidents; it promotes survival and ensures organizational resilience.
3. ISO 22301:2012 Societal Security, Business Continuity Management Systems. This standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

NOTE-7: For more information about how to participate, be sure to see PS-Prep website links (in the Reference section at the end of this topic).

FINAL IMPRESSIONS:

The future appears to hold plenty more standardization practices, and opportunities for improvements, uniformity, integration, and small step-wise enhancements to our overall National Resilience. ISO9001:2015 certification has been reworked to make the most sense during the “Technological Age” we live in, by emphasizing integrative Quality Management Systems that organize and improve business efficiency, preparedness, quality, opportunities, and other facets that collectively improve their stability, financial standing, and resilience. Much of this topic was devoted to demonstrating the benefits of operating a business under the new Annex SL framework, the similarities the new ISO9001:2015 standard shares with National Standards, and the implication that (IF) the NEW risk management component is properly addressed by businesses, (THEN) the entire community and in some instances the entire Nation may achieve and enjoy improvement. Furthermore, if we can gain a consensus that this preliminary theory is valid and the arguments or evidence (both presented and available) are sufficient to make a case for action, then I would suggest that said action (ought to be) the proactive identification and engagement of said businesses to ensure that they align with National standards (by utilize DHS/FEMA recommended available educational/training products), and/or take additional actions pursuant to additional certifications, credentials, and Agreements or Memorandums of Understanding, to the benefit of all parties. Said agreements are pursuant to enhancement of our overall capabilities in the event of major disasters, but I also believe that cultivating these relationships will likely yield a climate of additional trust, (between Governing officials and the Private sector), and I will restate here that I believe it will generate “new data” and insights regarding the business processes, new feeds for other projects, and options to be further explored as “Usability Cases” for future research and development projects (e.g. our technology industries). This “new data” (from auditable business records, reports, and other sources) may also provide the answers to some of our toughest questions related to integration of Open Source information into systems that contribute to non-obvious relationship analysis (beyond the scope of this topic). Having stated, the importance of the new ISO9001:2015 requirements (and emphasizing the analysis of risk with context and the Process Approach with inputs, outputs, outcomes and other quality requirements), it becomes obvious, intuitive, and necessary that these evaluation practices guide the overall quality practices of a business (regardless) of formal inclusion in past or present ISO9001 standards. For every regulation created, litigation can potentially follow, which ensures compliance or loss of privilege, and restoration of losses to those affected by nonconforming products. For businesses who comply perfectly with the ISO9001 Standards (as checked by official auditors), they may enjoy protection, and exemption from prosecution in many cases, having complied and performed all due diligence expected of them. Unified frameworks, systems and ONGOING COMMUNICATION are critical to maintaining integration of all stakeholders into the National Resilience calculus. Therefore, I would additionally state here, that (regardless of ISO9001 certification or not), it may be prudent to enhance (both awareness and delivery) of DHS/FEMA previously stated educational materials to ALL businesses, such that access is enhanced, confidence and trust is elevated, and integration into local capability which feeds into National Resilience, may be possible. These stated practices should aid ALL businesses in loss prevention or mitigation during incidents (that would otherwise result in a deficit of products, services and negative outcomes for customers). Once businesses are on-board and understand CGC-1, THIRA, and other guidance and standards, risks will be identified, plans can be created to prepare, prevent, protect, mitigate, and respond more effectively (and uniformly) which in-turn enhances the overall quality and stability of business processes, products, and services for the benefit of all stakeholders. At some point Local Emergency Personnel or NIMS may factor these major businesses into the preparedness calculus, in which case, the business must be dependable and conduct regular assessments and audits to yield verifiable records (which may be used as “Status of Aid” updates) during the first 1-3 days of an incident. The degree to which a business is adaptive to the requirements of the Standard (including risk assessment), and conforms to the (Annex SL framework) during implementation of ISO9001:2015, may affect the relationship to customers or Public-Private Partnerships (who require it). As the New audits of the Risk Assessment portion of the ISO9001:2015 standard provide researchers and investigators with a new pool of business data, (and organizations undergo “usability studies”) the eligible for Public-Private partnerships (and value as providers of capabilities and resources via mutual aid agreements) will become more clear (I believe) in the next 3-5 years. This relationship may be further enhanced by businesses participating in the recommended

PS-Prep options. Whether businesses achieve partnerships with local or national government (or no level of partnership), overall the ISO9001:2015 Quality Management System standard will produce many positive effects that further stabilizes our National supply chain, improve goods and services, and protects businesses, dependencies, and all those who rely on them. Leaving off where I began, I wish to restate that ISO9001 was re-examined this year by me because Risk Assessment has been improved this year and is more compatible with other aspects of our U.S. National Security apparatus through Annex SL, and I believe this will greatly enhance safety at many businesses once implemented, and particularly if ISO9001 is adopted by schools they will enjoy improved readiness.

QUESTIONS FOR THE READER:

1. Do Cross-Cutting opportunities exist, whereby DHS/FEMA education and training resources may be utilized to offer specialized support for the transition of businesses to the new ISO9001:2015 standard, and in-turn augment uniform operating conditions between FEMA and Private sector Businesses, with regard to mutual aid and risk management procedures?
2. (IDEAL OPTION) Can PS-Prep help businesses implement ISO9001:2015 through (one of the three) offered Standard options, such that businesses will integrate more uniformly with National Standards:
a. NFPA 1600: Disaster/Emergency Management/Business Continuity
b. ASIS International SPC.1-2009: Organizational Resilience / Security Preparedness / Continuity Management
c. ISO 22301:2012: Societal Security-Business Continuity Management Systems
3. Can FEMA “IS454 Risk Management” educational coursework provide the education or training necessary to meet the requirements of the “Risk-Based Thinking” components that have been NEWLY integrated into the ISO9001:2015 standard?
4. Can DHS/FEMA CPG201 guidance provide the necessary template to generically conduct the THIRA assessment, and implement them as required by the NEW ISO9001:2015 standard?
5. Can DHS/FEMA CPG101 guidance provide the necessary template to revise and integrate Risk Management components into a business’s EOP as required by the NEW ISO9001:2015 standard?
6. Can DHS/FEMA CGC-1 provide (comprehensive enough) Continuity Guidance and a template for businesses to achieve a functional program or will they require a PS-Prep option?
7. As this topic is a preliminary draft, I would very much appreciate it if the reader could point out any/all errors in facts, inference, or otherwise, so that I may improve upon this information continuously going forward with new versions.

DISCLOSURES AND DISCLAIMER:

I am not an expert on ISO9001. This information was presented as objectively as possible, and I am not linked to the promotion of ISO9001 by any means. This document should be regarded as educational only, and any arguments given here that imply NIMS should “integration” ISO9001 certified businesses should be thought of as “food for thought,” and only to be considered on a case-by-case basis. As a requirement, I undertook ISO9001 virtual training, (just like most people do), and received some other special training (OJT), and Code of Federal Regulations related education along the way as well. I am most familiar with this topic as it pertains to (my own business divisions), and with ISO9001 in the crisis recovery setting of hospitals, and the FDA’s Quality System Regulation and Conformity of blood component products under the CFR as both Food and Drug requirements. I’ve also extensively considered ISO9001 related implications for (my own partnerships), as well as Food-Drug-Vaccination Safety requirements, and in the context of risks management related to threats, hazards, and disaster scenarios. During preliminary research on this specific subject matter I found no comparable articles, therefore (although this topic is intentionally kept generalized), this may contain some novel discourse. This document contains inference and portions of documentation from an information product used by ATL Prevention Research L.L.C., and will most definitely be subject to change, revisions, and updates. During my research, I carefully considered credible scientific studies of ISO9001, which all demonstrated benefits, (most were interested in growth and profits), but notably ISO9001 was shown to be (strongly correlated with very low employee death rates). Additional “scientific studies” appear to support the argument that ISO9001 benefits the

public and our Government, and as such, public policy should be modified to support and/or subsidize quality programs. The chose to omit said “scientific data” (from this document) and not discuss policy changes (as conclusions), is based upon the finding of (potential basis for bias) as well as many confounding factors related to various data sources such as (e.g. safety- businesses with low employee death rates many times had low rates before adopting ISO9001, and/or many personnel may not be willing to step forward and report incidents externally or to auditors because this could lead to the potential revocation/forfeiture of the certification, both conditions and others may alter statistics in ways that cannot be accounted for). Also, during my research, I took minor issue with what I call a “Propaganda and rally effect” in that, the ISO9001 creators, working groups, and Auditors all have “a stake in the buy-in” of businesses to maintain their ISO9001 certification, which means it is in their financial interest to (increase the number of ISO9001 certified businesses), and as such they appear to be exercising a good deal of “self-promotion” by posting multiple references on multiple websites that accentuate the facts or give numerous positive generalizations about ISO9001, so much so, that (the reader may forget that the true basis for greatness in any business is always the people who work hard to achieve and maintain it). One challenge I found while narrowing this topic is that upon researching quality, safety and risk management, each sub-topic eventually leads to all other topics within the massive umbrella of preparedness and resilience topics. As such, one complication was eliminated from this document, and was related to a large analytical section on the subject of ISO9001 certified business NIMS compatibility and integration as a PPP. This content was removed because CI/KR business entities would not necessarily want to disclose their standards, processes, or practices to (the public ISO9001 Auditors) as this could give bad actors a map of what, how, and when to exploit the entity/business, and may further identify a chain of coordination and how to disrupt capabilities within a given Geographic area. Also, integration principles related to other ISO9001 certified (non-CI/KR businesses) overwhelmed the article and the basis for incorporating the additional hypothetical material in support of the (over reaching original theory given above) resulted in potential errors in inference, and prediction required (too many assumptions to pass the Occam’s Razor principle). No integration heuristic was found, but rather, all research seems to suggest that (whether a business is ISO9001 certified or not, all evaluations of NIMS compatibility must be conducted independently on a case-by case basis), and undergo periodic re-evaluations as well. Therefore, for brevity sake, this is not an all-inclusive presentation, and I’ve represented the core information in a format derived from ISO9001:2015 FDIS (and other sources described below), and articulated it in a way that I believe many businesses and stakeholders will benefit from. Version-1 of this topic was created after the review of ~210 references most closely related to ISO9001:2015 or its implications, and used only internal to my business Technology Dept. This Preliminary Version-1.3E is an (experimental) sub-portion of the original, containing educational and partially “retrospective meta-resources and meta-knowledge” in that, multiple secondary resources (information and statistics about the validity of information, and knowledge about knowledge) were used, to enable ascertainment of patterns and some level of consensus regarding what is factual and most valid (and important) to present to organizations and stakeholders. Additionally, I took advice from 2 experts, and watched videos to get a feel for the auditing process that businesses may experience. Viewing videos can give businesses a sense of the audit process, (general criteria should be relatively standard), but it is also fair to say that not all of my conclusions about auditors will bear high-yield results, as all auditors differ a bit, and will likely handle each business on a case-by case basis. This information assumes a target audience that requires ISO9001 certification, but also may be used by any serious business personnel or stakeholder whom desires to understand structure and principles used to implement and control a business and its processes, functions, and systems including outcomes during an incident. I’m sharing this information with (Emergency Management or Response stakeholders and others) because I believe it contains cross-cutting opportunities for businesses to utilize DHS/FEMA educational materials, and it sheds light on processes critical to enhancement of (business, community and National) resilience. As per usually, the point of submitting this information is for people TO USE IT and improve, and therefore, (for my part), there is no limitation to disperse, duplicate, or utilize this information in any way they wish. I’ve also placed additional references at the end of this document to further assist the readers (whom these requirements may pertain to), or those whom desire to improve their knowledge, or a given process or management system.

APPENDIX-A: ASSOCIATED ARTICLES AND DISCUSSIONS

USCSRH.COM:
http://www.uscsrh.com/featured-article.html
U.S. COMMUNITY SAFETY AND RESILIENCE HUB AT IDEASCALE
http://uscsrh.ideascale.com/a/dtd/ISO9001-2015-NEW-QMS-Framework-Requirements-and-Implications/115501-29117
QUADRENIAL HOMELAND SECURITY REVIEW AT IDEASCALE:
http://qhsr.ideascale.com/a/dtd/ISO9001-2015-NEW-QMS-Framework-Requirements-and-Implications/515012-24279
DHS SCIENCE AND TECHNOLOGY AT IDEASCALE:
http://scitech.ideascale.com/a/dtd/INCENTIVIZE-PRIVATE-SECTOR-IMPLEMENTATION-OF-ISO9001-QMS-STANDARDS/522538-30851
FEMA IDEASCALE:
http://fema.ideascale.com/a/dtd/NEW-ISO9001-2015-Implications-for-the-National-Preparedness-Goal/502135-14692
FEMA NATIONAL PREPAREDNESS COMMUNITY:
http://community.fema.govdelivery.com/connect.ti/readynpm/messageshowthread?threadid=51822
ACADEMIA.EDU:
https://www.academia.edu/s/1817642815/iso9001-2015-new-qms-framework-requirements-and-implications

ENHANCE VISIBILITY AT
GOOGLE PLUS:
https://plus.google.com/106731425731740877144
DOCS.COM:
https://docs.com/aaronlittlefield/6665/iso9001-2015-new-qms-framework-requirements-and

APPENDIX-B: REFERENCES SPECIFIC TO THIS ISO9001 TOPIC

ASSOCIATED COMPREHENSIVE BUSINESS CONTINUITY & PREPAREDNESS RESOURCE LIST:
I preemptively created a useful list, and as this discussion evolves, I will continue to keep and update a long list of Business Continuity resources spanning all agencies (and available to the Public) here:
http://uscsrh.ideascale.com/a/dtd/The-USCSRH-Business-Continuity-and-Preparedness-Resource-List/109280-29117

OFFICIAL ISO9001:2015 PROJECT WEBSITE:
http://www.iso.org/iso/iso9001_revision

ISO9001 APG: (REPOSITORY OF LINKED WEB RESOURCES)
http://isotc.iso.org/livelink/livelink?func=ll&objId=3541460&objAction=browse

(2014) ISO DIRECTIVES INCLUDING ANNEX SL:
http://www.iso.org/sites/directives/directives.html#toc_marker-76

OFFICIAL YOUTUBE ISO9001:2015 VIDEO DISCUSSION OF UPDATES: (~7 minutes)
https://www.youtube.com/embed/1JIMyvpP0tw

ISO9001 TRAINING CENTER: (Clause 7.6 Control of monitoring and measuring equipment)
http://www.isorequirements.com/iso_9001_7.6_control_of_monitoring_and_measuring_equipment.html

ISO STANDARDS IN ACTION:
http://www.iso.org/iso/home/news_index/iso-in-action.htm

NIST COMPARISON OF THE BALDRIGE CRITERIA VERSUS ISO9001:
http://www.nist.gov/baldrige/about/faqs_baldrige_iso.cfm

RECOMMENDED COOP/SAFETY/PREPAREDNESS CURRICULUMS OR CERTIFICATIONS:

(2014) DHS/FEMA (new) PS-Prep options with certification:
https://www.fema.gov/about-ps-preptm
http://www.fema.gov/program-resources
http://www.fema.gov/pdf/privatesector/FEMA_PS-Prep_One-Pager_Generic.pdf

National Fire Protection Association: (NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs)
http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600

ASIS SPC.1-2009: (Organizational Resilience Security, Preparedness, Continuity Management Systems)
http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf

ISO 22301:2012: (Societal security, Business continuity management systems)
http://www.iso.org/iso/catalogue_detail?csnumber=50038

FEMA COOP Level-I & Level-II courses/training:
http://training.fema.gov/programs/coop/

FEMA Business Crisis and Continuity Management:
http://www.training.fema.gov/hiedu/docs/busind/bccm%20-%20course%20syllabus.doc

ABOUT STANDARDS DEVELOPMENT ORGANIZATIONS:

International Accreditation Forum:
http://iaf.nu/search.php?q=iso+9001&submit.x=0&submit.y=0

ISO TC 176 HOME PAGE: “Quality Management and Quality Assurance”
http://isotc.iso.org/livelink/livelink/open/tc176

QSIT Inspections Guide:
http://www.fda.gov/downloads/ICECI/Inspections/InspectionGuides/UCM085938.pdf

American National Standards Institute (ANSI):
http://en.wikipedia.org/wiki/American_National_Standards_Institute

List of Technical SDO’s:
http://en.wikipedia.org/wiki/List_of_technical_standard_organisations

ISO Technical Committees Website Links Reference:
http://en.wikipedia.org/wiki/List_of_ISO_technical_committees

OTHER SAFETY REFERENCES:

Emergency Operations Risk Assessment:
http://uscsrh.ideascale.com/a/dtd/POST-3-EMERGENCY-OPERATIONS-RISK-ASSESSMENTS/64705-29117

Workplace Violence References:
http://uscsrh.ideascale.com/a/dtd/IDEAS-TO-MITIGATE-SCHOOL-WORKPLACE-GUN-VIOLENCE-SCENARIOS/62728-29117
http://uscsrh.ideascale.com/a/dtd/PRIORITY-TERRORIST-ATTACK-MITIGATION-REFERENCE-MANUALS/103079-29117

A New Approach to Emergency Operations Plan Partnerships: (Discusses a free solution in such a way as to (limit the concern of attacks or hacking of Government systems)
http://uscsrh.ideascale.com/a/dtd/A-New-Approach-to-Emergency-Operations-Plan-Partnerships/72166-29117

Emergency Essential Functions:
http://www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf

Continuity Guidance Circular (CGC-1):
http://www.fema.gov/media-library-data/1386609058803-b084a7230663249ab1d6da4b6472e691/CGC-1-Signed-July-2013.pdf

Continuity Guidance Circular (CGC-2):
http://www.fema.gov/pdf/about/org/ncp/coop/cont_guidance2.pdf

CPG101 Developing and Maintaining EOP's:
http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

EOP Process and analysis support tool:
http://www.fema.gov/pdf/about/divisions/npd/CPG_101_v2_past.pdf

CPG 201 THIRA:
http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

National Security Directive 51/Homeland Security Directive 20 (NSPD – 51/HSPD -20):
http://emilms.fema.gov/IS548/CMGR0102110t.htm

NIMS Resource Typing, Credentialing, Mutual Aid Information:
https://www.fema.gov/resource-management-mutual-aid

Resource Typing Library Tool (RTLT):
https://rtlt.ptaccenter.org
http://www.fema.gov/resourcemanagement

IRIS, current version 5.0:
https://www.ptaccenter.org/iris

Deployable Resources:
http://www.emacweb.org/index.php/mutualaidresources/deployableresources

ISO31000:2009 Risk Management:
http://en.wikipedia.org/wiki/ISO_31000
https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

Lay Theories Lead to Coordination Neglect:
http://faculty-gsb.stanford.edu/heath/documents/ROB-Coord%20Neglect.pdf