Question 1: How does sustainability play within risk management as I see it as a wholly exclusive issue?

The international standard for risk management reminds us that all functional disciplines (e.g. quality, sustainability, environment, assets, etc.) should be focused on helping the organization meet its articulated objectives in uncertain times. In the webinar, I made the connection to sustainability (see Slide #8) by showing how this discipline has been successful in converting the positive “effects” (i.e. “opportunities”) to help reduce uncertainty and create a means of balancing the negative “effects” (i.e. “threats”) as part of the risk management process. Undoubtedly, quality also has a similar role when practiced in a proactive fashion. Please also refer to Slide #15 and Slide #23.

Question 2: What is the difference between effectiveness and efficacy? Don't they both refer to ability to achieve objectives?

ISO DIS 9001:2015 defines effectiveness (3.06) as “extent to which planned activities are realized and planned results are achieved.” Efficacy is defined as “the power to produce an effect.” They do indeed both refer to the ability of an organization to achieve its objectives.

Question 3: What is the intent here? I am hearing a lot about sustainability and dispersion between all business segments. We do not approach business that way as our quality system integrates all aspects.

ISO 9001:2015 defines quality management as “management with regard to quality.” ISO 14001:2015 defines environmental management as “management of environmental aspects, conformance to environmental compliance obligations and the ability to address risk associated with environmental threats and opportunities.” ISO 55000:2014 defines assets management as “coordinated activities of an organization to realize value from assets.” ISO 22310:2012 defines business continuity management as “part of the overall management system that establishes implements, operates, monitors, reviews, maintains and improves business continuity.” ISO 27000:2014 defines information security management as “a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives.” ISO 31000:2009 defines risk management as “coordinated activities to direct and control an organization with regard to risk.” Please refer to Slides #15 through #17 to see how risk management helps direct all of the organization’s management systems on a common platform for the purpose of helping an organization meet its objectives in uncertain times. See also the answer to Question #1 above.
Question 4: This type of approach may have the net negative that companies would exit as the perception becomes yet another layer to be in compliance, how do you answer to that?

No one will deny that we live in an “uncertain” world. The ability of an organization to meet its stated objectives amid this uncertainty is critical to its purpose and its strategic direction. The ISO 9004:2009 guidance points to quality as contributing to the sustained success of the organization. This document states, “A successful management system drives the development of an organization towards sustained success, in order to be one of the best performing, efficient and profitable organizations in its business sector.” “Risk-Based Thinking” will help an organization create a business delivery model that will be:

- Tailored to the level of risk associated with the organization’s context
- Aligned with other business risk management
- Comprehensive, systematic and structured,
- Embedded within all management systems
- Dynamic iterative and responsive to change.

This will enhance compliance, financial control, improved decision making, and efficient operations, effective processes and efficacious strategy. If an organization’s customer

Question 5: Can an organization be really certified on ISO 31000?


Question 6: What is the real cost? What is the net gain? What are the requirements and reporting structure that would be required for ISO 9001:2015?

All users of ISO 9001:2008 and the sector-specific quality standards (e.g. TL9000) will need to be certified to ISO 9001:2015 within three years from its release in 2015. This is a major revision and there are many changes from what you are using now. It is clear that the revision builds on what is already in place. I have been suggesting that the organization take the DIS (or FDIS once it is released) and place its current quality management system into the equivalency matrix that has been release by ISO/TC 176/SC2. If you begin now, you will have more than three years to benchmark your organization to the new ISO 9001:2015 format. By adopting the new elements of the management system and the “Risk-Based Thinking” found in the revised management system standard, you will be demonstrating your ability to evaluate your quality management performance (Section 9) and your ability to improve (Section 10). According to the first clause in Annex A (informative), you are not required to make changes in your existing reporting structure. However, this will be detrimental to your organization’s ability to improve alignment with other management system standards and the company’s enterprise risk management program. I would recommend that you become familiar with the eleven risk
management principles in ISO 31000:2009 and use them to guide your transition. ISO will be releasing a transition guide with the release of the final ISO 9001:2015 quality management system standard. They have placed an initial draft of that document on the ISO/TC 176/SC2 website. You might also wish to refer to ISO 9004:2009 as mentioned in the response to Question 5 above.

**Question 7: In one sentence how will “Risk-Based Thinking” help or detract from a company's bottom line?**

The most important principle (there are 11 principles in ISO 31000:2009) of risk management is that it delivers value to the organization.

**Question 8: How would you incorporate risk management in ISO 9001:2015?**

The technical management board and the joint technical coordination group of the International Organization of Standardization (ISO) have determined that all management systems will follow a new format (“high-level structure and common terminology) as defined in ISO Directive Annex SL. The mandatory incorporation of Annex SL in ISO 9001:2015 drives a risk-based approach to quality management that direct an organization to address opportunities and threats that need to be addressed to give assurance that the quality management system can achieve its intended results and that this will help the organization as a whole meet its stated objectives. Risk management is being incorporated into the revision of all the ISO management systems with the concept of “Risk-Based Thinking.” The guidance document (ISO Document N1222, July 2014) explains how risk is addressed in ISO 9001:2015. This document clearly cites ISO 31000:2009 and ISO TR 31004:2013 as “useful documents” for organizations seeking to make the transition to the revised standard. I would suggest you become familiar with the documents as well as the ISO information specific to the ISO 9001:2015 revision.

**Question 9: Sustainability is currently understood to be dealing with Green Corporation and reducing carbon footprint. Is there a changed interpretation now to deal with Risk Management?**

Sustainability (and Social Responsibility) has many definitions depending on the perspective used by the person creating the definition. The example you cite is from someone concerned with climate change. Sustainability can be defined from the perspective of an organization seeking to meet its objectives in an uncertain world. “Sustainability is the capability of an organization to transparently manage its responsibilities for environmental stewardship, social well-being, and economic prosperity over the long term while engaging its stakeholders.” Risk management is already defined from the perspective on an organization: “coordinated activities to direct and control an organization with regard to risk” (defined in Slide #6). In ISO 9001:2015, management is defined as “coordinated activities to direct and control an organization.”
Question 10: Sustainability and Quality are not the same. It can be said over and over does not mean that they are the same. They are segments for consideration of how a company operates.

Sustainability and quality are considered to be different operating “functions” within an organization. Each function can have its own management system. Risk-based thinking has created a single, unique numbering system (these are the rows in Slide #16) that enables different functions (these are the columns in Slide #17) to share information on a uniform platform. Sustainability and quality are functions in the middle row of Slide #15 along with finance, operations, environment, health & safety, information management, etc. You can see that risk management supports strategic decision making and the setting of objectives in the organization (the top row). As you state, these are segments for consideration of how an organization is managed (see Slide # 23).

Question 11: Opportunities may also have uncertainties/threats. Does the framework have a requirement to handle these as well? Can you also give an example for Opportunity, because I am unsure how would someone determine something as an Opportunity or not.

Opportunities and threats come from the effects of uncertainty. The fourth principle states, “Risk management explicitly takes account of uncertainty, the nature of uncertainty, and how it can be addressed.” Uncertainty is defined as “the state, even partial, of deficiency of information related to, understanding or knowledge of an event (or decision), its consequence, or likelihood.” What makes risk management unique is that it specifically addresses the effect of uncertainty on objectives. The generic strategy for opportunities and threats (my Slide #20) can be successfully only when the nature and source of that uncertainty is understood. When analyzing opportunities and threats, sensitivity studies should be used to understand the actual influence of the actions on uncertainty. It is always best to ask, “What are the assumptions here?” and “What are the uncertainties associated with the assumptions?” As you know from “systems thinking,” everything is linked to everything else. This is precisely why one functional discipline in an organization should not approach risk management alone (see my answer to question 10).

Opportunities are positive effects that are recognized when evaluating the information collected when determining the context of your organization in Section 4.1 of ISO 9001:2015. Opportunities can help the organization reduce uncertainty and be in a better position to meet the stated objectives of the organization often found in the company’s mission statement and objectives set lower in the organization that support the mission statement. The ISO guidance document on “Risk-Based Thinking” has some good examples of opportunities.

Question 12: The fundamental aspect of smart risk mgmt. is intelligent prioritization, using various tools e.g. FEMA, to evaluate various risks. What pointers would you give on optimizing such a prioritization process?

ISO 9001:2015 directs an organization to identify opportunities and threats (unfortunately the ISO DIS 9001:2015 is still using the term “risks and opportunities” – an investment term) in Section 4. Section 6.1 has the organization determine actions to address these opportunities and threats (the term as used in ISO DIS 14001:2015). The organization will then prioritize both the opportunities and threats perhaps using a risk matrix as shown on my Slide #19. There are a number of guidance documents related to ISO 31000:2009 that provide lots of ideas for optimizing the prioritization process. It is important to have ONE prioritization system than can handle both the opportunities and the threats (see my Slide #20). The risk assessment process that is described in ISO 31010:2009 is used to address the significant risks from the prioritization process (see my Slide #30).

Question 13: ISO generally requires a lot of documentation to be maintained... Will the new framework reduce some of the efforts for people...? Lot of disconnects and gaps happen because of the size of documentation.

The ISO 9001:2008 terms (“documented procedure” and “record,”) have been replaced with the term, “documented information.” The new term is defined as “information determined by the organization as being necessary for the effectiveness of the quality management system.” It notes that the extent of documented information for a quality management system can differ from one organization to another. The applicable principle here is “risk management is tailored.” ISO will be releasing a Technical Report (ISO/TR 10013) that will provide guidance for meeting this requirement. ISO will also release a transition guide to help with the transition. This may be an opportunity for your firm to “reduce the efforts for people” as you state in the question.

Question 14: Shouldn't risk be accounted for in setting strategic objectives which would minimize / mitigate the risk to reaching strategic objectives?

Yes! In the opening section of ISO 9001:2015 (4.1 Understanding the organization and its context), the organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended results of its quality management system. Understanding the context and the needs of the organization’s stakeholders and customers (i.e. still called “interested parties in the DIS version) is central to an organization being capable of meeting its objectives. The internal context is often evaluated using a SWOT (i.e. strengths, weaknesses, opportunities and threats) tool. The external context is often evaluated with a PESTLE (i.e. political, economic, socio-cultural, technological, legal and environmental) tool followed by a SWOT on each category. These tools have long been used as a means of introducing risk management (opportunities and threats) into the strategic objective-setting activity of any organization. This may appear to be a new area to ISO 9001. This greater focus on risk will mean that an organization will need to demonstrate how this requirement is being met. The extent and formality of the risk-based approach needed in a particular organization will be influenced by its context.
Question 15: What are the additional expectations from “Risk-Based Thinking” in ISO 9001:2015 to address “Preventive Actions”?

“Risk-Based Thinking” seeks to establish a systematic approach to risk in the organization rather than treating it as a component of a quality management system. As a result, specific requirements for “preventive actions” have been removed from this ISO 9001 revision. According to the guidance used by those revising this standard, an organization becomes proactive rather than purely reactive by preventing or reducing undesired effects and promoting continual improvement in every element of the standard. Preventive action is automatic when all of the management system standards are “risk-based.” This is a great example of how “Risk-Based Thinking” is building on what you already have in place.

ISO 9001:2015 Guidance:
http://isotc.iso.org/livelink/livelink/open/tc176SC2public

Risk-Based Thinking Guidance:

Transition Guidance: