DOI: 10.1111/risa.14292

ORIGINAL ARTICLE

Lessons identified from applications of the Risk Analysis Quality Test Release 1.0

Robert Waller[1,2,3] | **Margaret Coleman**[4] | **Samuel Denard**[5] | **Emma Soane**[6]

[1]Protect Heritage Corp., Ottawa, Ontario, Canada

[2]Canadian Museum of Nature, Ottawa, ON, Canada

[3]Art Conservation Program, Queen's University, Kingston, Ontario, Canada

[4]Coleman Scientific Consulting, Groton, New York, USA

[5]Empirical Products & Services, Houston, Texas, USA

[6]Department of Management, The London School of Economics and Political Science, London, UK

Correspondence
Robert Waller, Protect Heritage Corp., 622 Simoneau Way, Ottawa, ON, K4A1P4, Canada.
Email: rw@protectheritage.com

Abstract

The Risk Analysis Quality Test Release 1.0 (RAQT1.0) was developed as a framework to encourage mutual understanding between technical risk analysts and risk management decision makers of risk assessment quality indicators. The initial version (release 1.0) was published by the Society for Risk Analysis (SRA) in 2020 with the intent of learning from early test applications whether the approach was useful and whether changes in approach or contents would be helpful. The results of applications across three diverse fields are reported here. The applications include both retrospective evaluations of past risk assessments and prospective guidance on the design of future risk assessment projects or systems. The fields represented include Quantitative Microbial Risk Assessment, Cultural Property Risk Analysis, and Software Development Cyber Risk Analysis. The RAQT1.0 proved helpful for identifying shortcomings in all applications. Ways in which the RAQT1.0 might be improved are also identified.

KEYWORDS
cultural property risk analysis, cyber risk analysis, microbial risk analysis, risk analysis quality

1 | INTRODUCTION

Beginning in 2015, members of the Applied Risk Management Specialty Group (ARMSG) of the Society for Risk Analysis (SRA) identified a strategic concern: a lack of mutual understanding between technical risk analysts and risk management decision makers about what are important markers of quality in risk assessments. To address that strategic concern, the issue of meeting essential risk analysis quality requirements was identified as a promising initiative and might serve as a bridge to facilitate such mutual understanding. A series of SRA webinars and roundtable panels at Annual Meetings were convened to explore and organize a set of risk quality characteristics. In the course of that work, the ARMSG identified a list of 76 observed shortfalls in technical risk analyses. Each shortfall was reworded into a criterion of risk analysis quality, then into a question asking if an evaluated risk analysis satisfies that criterion, with answers "yes," "no," or "NA" not applicable. Those 76 questions comprise the Risk Analysis Quality Test Release 1.0 (RAQT1.0) (Lathrop et al., 2020), as approved for publication by the SRA Council in 2020 and available on the SRA website, Resources tab, https://www.sra.org/resources/.

The 76 RAQT1.0 questions are organized into 15 groupings as shown in Table 1.

The questions within these categories can be used prospectively, in planning and executing the myriad of considerations to complete a quality risk assessment, or be applied retrospectively, to assess the quality of an existing risk assessment.

This research provides lessons learned from early, comprehensive, and diverse applications of the RAQT1.0. These reflect both the diversity of applications to which the RAQT1.0 has so far been applied and also, to the authors' knowledge, more than half of all comprehensive applications to date. It is evident that there is no single way it might be used in practice. Retrospectively (Section 2), cases evaluate: two microbial risk analyses; and the quality of a pair of recent applications of the Cultural Property Risk Analysis Model (CPRAM). Prospective applications (Section 3) consider the use of the RAQT1.0 to aid: the design of a project to identify and evaluate benefits, risks, and costs associated with possible alternative storage solutions for a large mammal collection; and two cases relating to the control of process cyber risk arising from software development (SD). Section 4 is a discussion of lessons identified through these early,

TABLE 1 Topic-related groupings into which the 76 Risk Analysis Quality Test Release 1.0 (RAQT1.0) questions are organized.

A.	Framing the Analysis and Its Interface with Decision Making
B.	Capturing the Risk Generating Process (RGP)
C.	Communication
D.	Stakeholder Involvement
E.	Assumptions and Scope Boundary Issues
F.	Proactive Creation of Alternative Courses of Action
G.	Basis of Knowledge
H.	Data Limitations
I.	Analysis Limitations
J.	Uncertainty
K.	Consideration of Alternative Analysis Approaches
L.	Robustness and Resilience of Action Strategies
M.	Model and Analysis Validation and Documentation
N.	Reporting
O.	Budget and Schedule Adequacy

comprehensive and detailed applications and implications for further applications of, and potential improvements to, the RAQT1.0.

2 | RETROSPECTIVE APPLICATIONS

2.1 | Analyzing two quantitative microbial risk assessments (QMRAs)

The RAQT1.0 was applied to two past QMRAs (FDA/FSIS, 2003; FSANZ, 2009). These QMRAs were selected for analysis using the RAQT1.0 tool based on engagement of SRA members for nearly a decade on the topic of "disagreements regarding health risks of raw and pasteurized human and bovine milks," as well as familiarity of the RAQT1.0 testers (Coleman and Ross) with these complex documents and the scientific literature.

The Food and Drug Administration & Food Safety & Inspection Service (FDA/FSIS) QMRA estimated relative risks of severe listeriosis in 23 ready-to-eat foods for US consumers (FDA/FSIS, 2003), though the RAQT1.0 testing described here focused on two of the 23 foods, raw and pasteurized milks. The Food Standards Australia New Zealand (FSANZ) QMRA estimated risks of illnesses associated with four major foodborne pathogens in raw milk for consumers in Australia and New Zealand (*Campylobacter*, *Listeria monocytogenes*, pathogenic *Escherichia coli*, and *Salmonella*) (FSANZ, 2009). Both QMRAs, in our opinion, represent milestone efforts early in the development of this field, and both were subject to high variability in data quality and quantity. Significant gaps in knowledge remain for many of the food-pathogen pairs considered (Booth, 2021; Farber et al., 2021; Dietert et al., 2021; Sebastianski et al., 2022).

Analysis of both QMRAs by two independent microbiologists, one from the United States and the other from Australia, identified shortfalls in all 15 categories of RAQT1.0 questions and for each of 76 specific questions. The most serious shortfalls observed from the viewpoints of microbiology and epidemiology were associated with the RAQT1.0 Category G, Basis of Knowledge, particularly failures of both QMRAs to "clearly communicate to decision makers where limitations of knowledge (and its basis and strength) call for risk management strategies that take those limitations into account."

The questions within the Basis of Knowledge topic are consistent with international consensus principles and guidelines for QMRA (CAC, 1999) that both QMRAs cited. However, while both QMRAs claimed to follow the Codex Alimentarius Commission (CAC) principles and guidelines (see Supplementary Table S1 in CAC, 1999), both exhibited shortfalls in all seven Basis of Knowledge questions. Notable shortfalls included: use of sound science (e.g., best available scientific evidence for modeling microbiology ecology, considering relevant factors including competing microbes naturally present in foods); the use of transparent, unbiased processes for documenting assumptions, data, and analysis; and the need to document the influence of estimates and assumptions on estimated risk and uncertainty.

This case demonstrated important aspects of the utility of the tool in retrospective analysis: evaluating how well the CAC principles and guidelines were applied for past QMRAs; and when CAC principles on reassessment (e.g., comparing to independent epidemiologic data on human illness) and reevaluation (e.g., replacing assumptions with data; Latorre et al., 2011; Stasiewicz et al., 2014) warrant application.

Another important aspect highlighted by application of the RAQT1.0 was the need to update incorrect assumptions about pathogen prevalence, levels, and growth in raw milk made in past QMRAs, because claims about raw and pasteurized milks were not supported by rigorous data. For example, the FDA/FSIS QMRA did not acknowledge then-available studies on natural microbes present in raw foods that suppress or eliminate pathogens (IFT, 2001), despite the latter study having been commissioned by FDA and completed 2 years before finalization of this QMRA. Documentation on the Basis of Knowledge for the FDA/FSIS QMRA included the assumption that growth of the pathogen *L. monocytogenes* is equivalent in raw and pasteurized milks, despite citing a study (Northolt et al., 1988) that documented significantly lower growth rates in raw milk. In the body of the report, FDA/FSIS specifies use of an "average" growth rate of 0.257 per day (slope of exponential portion of growth curve of pathogen density and time) for both raw and pasteurized milks, while Appendix 8 documented individual rates of 0.085 per day for raw milk and 0.407 per day for pasteurized milk (adjusted to 5°C, tab. III-8). The appropriateness of pooling significantly different rates was not addressed, and pooling imposed an overestimation bias for raw milk and an underestimation bias for pasteurized milk.

Similarly, the FSANZ QMRA also did not cite available data on the prevalence and levels of pathogens in raw milk produced in New Zealand (Hill et al., 2012; 2007–2008 sampling), as well as seven additional studies conducted in Canada, the United Kingdom, and the United States and prior to 2006. FSANZ based campylobacteriosis, pathogenic *E. coli*, and salmonellosis assessments on the assumption that prevalence and levels of the respective pathogens in bovine feces were statistically predictive of prevalence and levels in raw milk, without robust data demonstrating predictive power and uncertainties. For listeriosis, the FSANZ QMRA assumed that prevalence and levels of the pathogen reported in a 1995 study of prepasteurized milk produced for the pasteurized milk market in Scotland were representative of prevalence and levels of the pathogen in raw milk produced for direct human consumption in Australia and New Zealand more than a decade later.

Inappropriate pooling, incomplete documentation of available evidence, and unsupported assumptions appeared to influence outcomes in the direction of a pro-pasteurization bias.

Two other categories of RAQT1.0 questions are of note. For Category A, framing the analysis and its interface with decision making, and Category F, creation of alternative courses of action, the RAQT1.0 application identified a disconnect between the analyses with decision making. Neither QMRA indicated that alternatives were developed and tested to simulate risk reductions (e.g., production practices, sanitation and hygiene, Hazard Analysis and Critical Control Point or HACCP, monitoring indicators and pathogens, and maintaining cold chain). While these shortfalls may have resulted from an internally or externally imposed scope or resource constraint, it is flagged as an analysis quality issue by the RAQT1.0.

Moreover, systematic evaluation of the FDA/FSIS QMRA, particularly regarding Categories A and F, resulted in discovery of risk management and risk communication statements previously overlooked by both independent microbiologists. The FDA/FSIS QMRA reported both raw and pasteurized milks as high-risk foods but categorized raw milk as a "priority candidate for continued avoidance," while pasteurized milk was categorized as a "priority candidate for more study to confirm model predictions or identify factors not captured by current models that would reduce risk." The basis for assigning "avoidance" and "more study" to two foods both ranked high risk was not specified.

For Category D, Stakeholder Involvement, neither QMRA documented engagement of stakeholders regarding data and analysis limitations nor alternative risk management options for milks. An opportunity for public comment was provided for the FDA/FSIS QMRA in 2001 through publication of a draft QMRA and a draft risk management action plan in the Federal Register (66FR5515). Regarding Category J, Uncertainty, neither QMRA addressed crucial uncertainties nor provided alternative scenarios for intentionally conservative assumptions that overestimated risk and underestimated uncertainty.

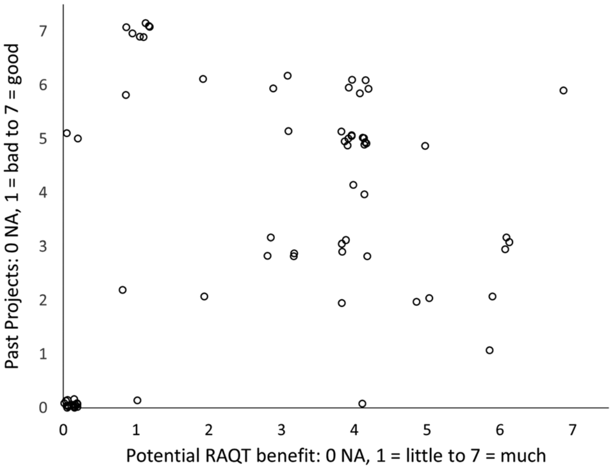

FIGURE 1 Judgments of past practice quality and of potential benefit of focusing improvement based on Risk Analysis Quality Test Release 1.0 (RAQT1.0) questions. Points have been offset by random amounts up to 0.4 to reduce overlaps. NA, not applicable.

2.2 | Retrospective application to cultural property risk analysis

The RAQT1.0 was applied in two distinct ways to cultural property risk analysis. With respect to the CPRAM (Waller, 2003, 2008, 2019), the first application was primarily retrospective in evaluating past practices but was also prospective in determining priorities for improving ongoing practice. The CPRAM, as represented by two applications completed in 2021, is evaluated against each of the 76 questions.

In the first application, the set of 76 questions were scored (0, not applicable; 1 to 7, bad to good) to evaluate how well, or poorly, the two applications of the CPRAM met expectations set by the RAQT1.0. A similar scale was applied for the question of how much benefit is expected by improving the CPRAM model with respect to each of the 76 RAQT1.0 questions (0, not applicable; 1 to 7, little to much). Both scales were constructed to encode the subjective assessment of the practitioner involved (Waller). While it would have been preferable to involve other stakeholders, especially client representatives, this was not possible given their other responsibilities and priorities. The results are depicted in a scatter graph in Figure 1.

Only point locations are shown as it is the nature of the distribution, rather than the identity of specific questions, that the chart intends to illustrate. A large cluster ($n = 20$) is seen near the origin (0,0) representing questions that were not relevant to the kind of risk identification, definition, ranking, and screening that the CPRAM is designed for. Furthermore, 42% ($n = 32$) of the questions scored just a 0 or 1 for potential benefit, suggesting that preliminary filtering of questions to those applicable to the purpose of risk identification, ranking, and screening could have significantly reduced the work to complete this evaluation.

There is a cloud of RAQT1.0 questions that are intermediate in both how well they were satisfied in the CPRAM

TABLE 2 Risk Analysis Quality Test Release 1.0 (RAQT1.0) questions leading to highest priorities for improving the Cultural Property Risk Analysis Model (CPRAM).

RAQT1.0 question	Past practice 1–7[a]	Potential benefit 1–7[b]	Explanation
H2: Are the data managed with an adequate data management system that assures each piece of data is accurately logged, and that appropriate levels of QA/QC are maintained, including the ability to demonstrate that adequate level of QA/QC to a third party?	1	6	Complex sets of Excel workbooks provide many opportunities for undetected errors. Links identify critical factors controlled by diverse areas of functional responsibility. Those links are incomplete or are not reliably maintained.
G4.2: Is the role and importance of potential surprises and unforeseen events (e.g., Black Swans) considered?	2	6	This is left in the hands of various areas of functional responsibility and accountability and not addressed within the CPRAM. Could be improved but at the cost of a substantial scope extension.
A1.1: Is the goal of the analysis clear and clearly announced?	3	6	Goal was clear to core participants but less to other participants. High-level accessible reminders, possibly infographics may help.
G3: In cases where limitations of knowledge call for risk management strategies that take those limitations into account, has that been communicated to risk management decision makers in language they can understand and apply?	3	6	Communicated principally by use of upper probable bounds (UPB), but ways of setting UPB can be inconsistent. While this is considered adequate for single specific risks it loses value for considering relative importance among many risks.
N1: Are key terms defined?	3	6	They are but should be provided in a more consistently convenient appendix.
G2: Is the strength of knowledge characterized in terms of its adequacy to support the risk management decisions to be supported?	6	7	Yes, overall characterized as “best current understanding.” Could be improved by characterizing uncertainty within each assessed specific risk.

[a] Scale was defined as 1 = bad to 7 = good.

[b] Scale was defined as 1 = little and 7 = much.

applications and how much further attention to each question could benefit future applications. In the top left quadrant are questions which the CPRAM scores well on and for which further emphasis would have little benefit to future applications. Most significant, along the right side, are the questions that appeared to highlight shortcomings in the two recent CPRAM applications. Each of these was judged to indicate priorities for improvements by modifying the CPRAM. These six items with potential benefit scores of 6 or 7 are listed in Table 2.

3 | PROSPECTIVE APPLICATIONS

3.1 | Planning a project to identify options and evaluate their benefits, risks, and costs

In a prospective context, the RAQT1.0 was used to aid the design of a project to identify and evaluate benefits, risks, and costs associated with possible alternative storage solutions for a large mammal collection. RAQT1.0 was used prospectively to guide planning of a project to identify options for a collection storage upgrade and evaluate the benefits, risks, and costs of those options. The plan was developed by a recent master’s level graduate in a Kress fellowship internship at the Smithsonian Institution, Melissa King. The project considered the need to, and options for, the best storage system employed for the Smithsonian Institution’s National Museum of Natural History’s collection of large vertebrate taxidermy and skeletal items. For this work, “best” was defined as providing the most cost-effective preservation of research value while facilitating easy access.

While recognizing that over 100 specific risks might require some form of assessment, based on received knowledge and experience, some of the main risks were thought to include fluctuating relative humidity, water damage from leaks, physical damage from unauthorized access or accidental contact, insect or vertebrate pests, light, dust, gaseous pollutants, security, and fire. A full ontology and taxonomy of generic and specific risks, consistent with the Hierarchical Holographic Modeling approach (Haimes, 1981; Haimes et al., 2002), was available within the CPRAM (Waller, 2019).

At an early stage in developing the project, the RAQT1.0 was reviewed question by question for inspiration and insights about how analyses should be scoped, structured, executed, and reported. The set of RAQT1.0 questions were categorized as highly applicable and useful 71% (n = 54), applicable but marginally useful 17% (n = 13), and not applicable to this project 12% (n = 9). The 54 questions judged useful in this application were subdivided into nonexclusive categories as relevant to: planning stage 25% (n = 19), execution stage 20% (n = 15), and report stage 33% (n = 25).

Subsets of about 10 of the 76 questions were seen to be most important for each of three project phases. As is common for relative importance across a population where that importance is a result of multiple factors, this is consistent with a Pareto ratio between 80:20 and 90:10, suggesting

TABLE 3 Examples of the Risk Analysis Quality Test Release 1.0 (RAQT1.0) questions significantly impacting the project plan.

RAQT1.0 question	Project context interpretation	Impact on project planning
D1: Are all stakeholders systematically and effectively identified, consulted, and engaged, in such a way that all stakeholders would agree that they were effectively consulted and engaged?	Is there a comprehensive list of stakeholders and interested parties and have ways to appropriately communicate and or involve these people in the project been established?	Extensive effort to establish a comprehensive list of stakeholders followed by adoption of the RACI framework (Responsible, Accountable, Consulted, and Informed; IIBA, 2015) to guide dissemination of information according to stakeholder needs and interests.
F1. Are alternative courses of action systematically generated through a process of proactive, goal-focused creation?	Are we limiting the range of storage solutions through museum context group-think limitations?	Conducted a brainstorming session with representatives of external perspectives to ensure the greatest possible diversity of options is identified.
G4: Is the role and importance of potential surprises and unforeseen events (e.g., Black Swans) considered?	Have as many situation-specific risks as possible been identified and merged with CPRAM's established set of risk definitions?	Surveyed stakeholders about their perceived risks to this collection, especially those peculiar to this collection in this situation, was crucial for identifying and defining difficult to foresee risks.

focusing on a limited subset of questions in each application will be efficacious. This suggests identifying relevant subsets of questions for various applications could be helpful.

Notably, the RAQT1.0 appeared not useful in the hands of either a risk analyst or a risk manager alone. It proved useful when it was adopted as a key element in the interface between risk analyst and risk manager, that is, used by both together. For effective communication between the consulting risk analyst and the project planner, most of the questions had to be reworded to be meaningfully interpreted in the context of this project. Table 3 provides three examples of RAQT1.0 questions that clearly added value to the project plan and how they were reinterpreted for this project.

3.2 | Applications to software development (SD)

There will always exist risk of an SD process resulting in software products posing unacceptable levels of risk to users or systems (Charette, 2005; Goseva-Popstojanova & Hamill, 2009; IBM Security, 2022). The SD process requires that process risk be analyzed/managed in two ways:

- The security requirement set that defines the software to be developed must be comprehensive and clear to all stakeholders.
- Because SD is a lengthy process, the requirement set's fulfillment throughout the process must be repeatedly verified.

Two research efforts explored the RAQT1.0′s applicability to both these concerns.

3.2.1 | Process risk analysis quality

The first effort hypothesized that the RAQT1.0 could meaningfully measure secure SD process risk quality. Computer programs are created by writing statements in a programming language. Collectively, those thousands or millions of statements cause the software to perform as required. The requirements are also statements; but they are written, in formally structured natural language, to specify features/capabilities and attributes that the software must possess.

Writing and enforcing security-related requirements is a prerequisite for the computer program's having security capabilities. It follows that, at any stage of the computer program's development, the degree of implementation of the security requirements is a measure of the security capabilities that the computer program will eventually have. For example, all security-related requirements having been implemented imply maximum security capability, and minimum operational risk. Any incompletely or improperly implemented security-related requirement is a vulnerability because, if deployed, it reduces security capability and increases operational risk.

Enforcement is not only inspection to find vulnerabilities but also vulnerability remediation. In that sense, enforcement is both risk analysis and management. And both involve many factors, including budget, schedule, human resources, and organizational politics. It follows that the risk analysis and management quality can have a large impact on the operational risk; and their application needs to be assessed. Because the risk analysis is done during the development process well before the operational risk takes effect, it can be referred to as process risk analysis (Denard, 2022).

To test the hypothesis, the 76 RAQT1.0 questions were applied to the requirements-based process risk mechanism. Presumably, if enough answers made sense and were probative, then the hypothesis would be true. Although the RAQT1.0 allows three responses to each question: "Yes," "No," and "Not Applicable" (NA), in this application, "Not Applicable" was interpreted as a "No," resulting in a more critical, demanding scoring. Note that the requirements set's author administered the RAQT1.0; the results may reflect inadvertent bias and RAQT1.0 administration inexperience. After conversion of "NA" to "No" responses, the counts of responses were 64 Yes and 12 No. This result implies that the

TABLE 4 The Risk Analysis Quality Test Release 1.0 (RAQT1.0) assessment of secure software development (SD) requirements as a risk analysis tool: Clear responses.

Question	Answer	Explanation
A.1.1: Is the goal of the analysis clear and clearly announced?	Y	The goal of an SD project is to produce an ideal end product. The goal of an SD project risk analysis (in this case, based on a minimum, necessary, and sufficient (MNS) requirements set) is twofold: (1) to ensure that each requirement has been satisfied for a given development project, where it is assumed that such satisfaction will yield an ideal product, and (2) to ensure stakeholder internalization of the requirements so that future/other development projects are increasingly likely to yield their ideal products.
M.1.0: Is the model and analysis fully validated, by normal standards of validation in the area of practice that applies?	Y	The requirements are draft input to a public standard (SAE, 2023) that will be available for public scrutiny and revision. Such consensus gathering is common engineering practice.

RAQT is applicable to process risk analysis assessment and that lends credibility to this use of security requirements as a process analysis tool. Two examples of such questions are shown in Table 4.

However, 12 of the questions were not so accommodating. Some were clearly "No" answers while others were difficult to evaluate in this context. Other assessors might have scored these as not applicable, but to maintain the critical, demanding scoring, these were set to "No." Table 5 lists the 12 RAQT1.0 questions that led to negative responses.

3.2.2 | Treating RAQT1.0 as a development project enables results scoring and comparison

The second research effort was a component of a larger research project that sought to develop a quantitative model of development (Denard, 2021), SD being an example. That model, the Statistical Agent-based Model of Development and Evaluation (SAbMDE), treats development as the sequential stepwise assembly of an end product from a set of components. These steps will involve a multitude of decisions. A "correct" decision sequence will produce a desired end product (DEP). SAbMDE enables calculation of project properties including effort estimates (Denard et al., 2020a) and process risk (Denard et al., 2020b).

The emergence of the RAQT1.0 created a SAbMDE validation opportunity. Over the course of an SD project, stakeholders will require project status periodically. It follows that process risk will be analyzed periodically; and an RAQT1.0 assessment may accompany each analysis. Early in the SD project, project metrics will be poor because some aspects of the developing project will be incomplete or unknown. As the SD project progresses, these aspects will clarify, the metrics will likely change, and stakeholders will want to understand that change. The same can be said of the periodic process analysis and repeated RAQT1.0 assessment results; in other words, the process analysis and RAQT1.0 results develop along with the SD project.

This research effort used SAbMDE to model how RAQT1.0 results can develop. The objective was an RAQT1.0 results set wherein each question had been answered "Yes" and had been reported in the best way. This procedure produced raw results that included scoring detail for each question and summary scoring values for the RAQT1.0 as a whole.

The generally positive results from both research efforts suggest that the RAQT1.0 can fulfill both management concerns listed at the start of this section. The results indicate that the RAQT1.0 can be used for process risk assessment, preferably after the issues identified in Table 5 are resolved. This work also indicates that an appropriate secure SD requirements list facilitates process risk analysis.

We also identify a number of implications for these types of applications:

- In the case of SD, the RAQT1.0 will need to be administered multiple times during a development project, both periodically and ad hoc.
- To make this practical and achievable RAQT1.0 administration duration will need to be much shorter than a project's duration. One day for RAQT1.0 review for each 2-week cycle of programming is thought to be practicable.
- The RAQT1.0 will likely be applied to risk analyses produced by both amateur and professional risk analysts.
- Because software is often built in a modular fashion, multiple RAQT1.0 result sets will likely be combined and reviewed by the relevant stakeholders; so, an easy and fair way to compare RAQT1.0 results is needed.
- The procedures for asking and answering each RAQT1.0 question should be simple and unambiguous. When there is ambiguity, there should be a procedure for resolving it.
- Grading each RAQT1.0 question's answer and report text will require judgment on the part of the grader.
- To ensure consistency in the administration and scoring of the RAQT1.0 (both inter- and intraproject), RAQT1.0 training and certification is needed; or, at least, an administration guidance document.

4 | LESSONS IDENTIFIED AND DISCUSSION

In this research, the questions that form RAQT1.0 were applied both retrospectively and prospectively to cases within diverse sectors, that is, in both planning and executing a

TABLE 5 The Risk Analysis Quality Test Release 1.0 (RAQT1.0) assessment of secure software development (SD) requirements as a risk analysis tool: Negative answers.

Question	Answer	Explanation
A.1.2: Is the risk/cost of falling short of that goal described?	N	The requirements themselves, as currently written, do not describe the risk/cost of falling short of the goal. The requirements are minimally and formally stated mandates. However, the justification and reasoning that went into the drafting of those statements/mandates do describe the risk/cost. In addition, the documented status of each requirement's implementation is a test and a measure of the developing software system's progress toward its ideal end product. Because these requirements are implemented by an organization's stakeholders, the requirements' consistent use within and across projects depends on each stakeholder's internalization not just of the requirement statement but also the requirement's justification and reasoning, its spirit. Therefore, the risk analysis of each requirement should include some measure of how much stakeholders' skills and will have advanced.
A.5.0: Is the risk analysis positioned appropriately in the organization chart of the client?	N	The premise of the requirements development effort was that SD security requirements were not sufficiently visible or internalized by stakeholders at all organizational levels. The requirements development effort hopes to improve that situation. Momentum supporting this effort is building and includes White House Executive Orders (Biden, 2023), CISA (Cybersecurity & Infrastructure Security Agency, 2021) and the National Institute of Standards and Technology (NIST, 2011) recommendations, DOD-mandated Cybersecurity Maturity Model Certification (CMMC, 2023) audits, law enforcement collaboration with the private sector (e.g., Infragard; FBI, 2023), and more (Krasner, 2021).
B.1.2: Is each scenario spelled out with the causes of change and types of change?	N	There are reasons and justifications for each requirement; and there can be many examples and experience-based explanations that inform those reasons and justifications. However, specific scenarios are not spelled out for each requirement. Process risk is not scenario-based as is operational risk.
B.1.3: Are potential hazards/events/scenarios "not on the list" (surprises, unanticipated events, often referred to as Black Swans) explicitly addressed?	N	As implied by the B.1.2 answer text, the requirements do not specifically consider operational Black Swan hazards. Nor do they fully address black swan scenarios that affect the development process itself. However, the requirements do address the fault tolerance and resilience of the operational system.
B.1.4: Are the implications of such hazards/events/scenarios for risk management explicitly described?	N	The basic premise: If a requirement is adequately implemented, the hazards that inform the requirement cannot occur. Each requirement's justifications and reasoning may discuss related hazard implications.
C.2.0: Have all considerations for effective risk communication been applied to assure adequacy of risk communication between analysts and decision makers?	N	The requirements set includes requirements that specify that certain operational inter-stakeholder communications occur, their frequency, and their content. However, individual requirements do not explicitly state their communication criteria. More importantly, despite the premise that operational vulnerabilities begin in the minds of development stakeholders, the requirements themselves do not communicate to the stakeholders that premise or its value.
E.1.0: Are all important assumptions, and the implications of each such assumption for risk management, listed systematically in language clear to risk management decision makers?	N	The reasons and justifications noted in the B.1.2 answer text describe the requirement's existentially important assumptions. However, a requirement's use in a project may rely on additional project-specific assumptions; the requirements set does not address these.
E.2.0: Each significant assumption may include a risk that that assumption deviates from the actual Risk Generating Process in such a way that the consequences and implications of that assumption are important. For each significant assumption, has that risk been evaluated and has that risk and its possible consequences and implications been made clear to the risk management decision makers?	N	As implied by the B.1.2 answer text, the project-specific assumption deviations are also not addressed by the requirements set.
E.3.0: Are all important scope boundary issues, and the implications of each scope boundary issue for risk management, been listed systematically in language clear to risk management decision makers?	N	Ideally, the requirements set's scope will include every aspect of a project to which the requirements set can be technically applied. However, the scope may be limited by practical considerations such as organizational boundaries, IP ownership, stakeholder consensus, and the like.
G.3.0: In cases where limitations of knowledge call for risk management strategies that take those limitations into account, has that been communicated to risk management decision makers in language they can understand and apply?	N	The reasons and justifications associated with each requirement are an *a priori* attempt to communicate effectively; however, this question asks about postcommunication effectiveness verification.

(Continues)

TABLE 5 (Continued)

Question	Answer	Explanation
G.7.0: Has there been explicit consideration of the possibility that some events have been disregarded because of very low probabilities, although those probabilities are based on critical assumptions?	N	The requirements themselves do not explicitly consider their alternate or partial application/enforcement; however, the stakeholders who apply/enforce the requirements must do so. In addition, the reasons and justifications associated with each requirement are an *a priori* attempt to communicate effectively; however, this question asks about postcommunication effectiveness verification.

quality risk assessment and in assessing the quality of existing risk assessments and the need for updating.

All applications drawn from three very different fields demonstrate the usefulness of the RAQT1.0 for reflecting on, and potentially improving, existing or proposed risk analysis practices. Still, the initial release of the RAQT1.0 was not intended to be the last word in understanding the quality of risk assessments vis à vis improving the effectiveness of risk management. It is a first attempt at codifying essential characteristics of quality risk assessment. The test applications described above have demonstrated its broad applicability, but also bring attention to ways in which improvements would be at least beneficial and possibly necessary.

When applying the RAQT1.0 prospectively to guide the planning of an options identification and evaluation project, it did not appear useful in the hands of either a risk analyst or a risk manager alone. To be useful, it needed to be used by both together, adopted as a key element in the interface between risk analyst and risk manager. The importance of using the RAQT1.0 within that interface cannot be overstated. It will, however, require that questions be expressed in ways that can be not just comprehended, but mutually understood by both risk analysts and risk management decision makers. As was seen in Section 3.1 “Planning a project to identify options and evaluate their benefits, risks, and costs,” some questions would appear to benefit from rewording to be less technocratic and facilitate differing interpretations in specific contexts. Overly technocratic wording for questions was an impediment to establishing a shared understanding between the risk analyst and risk management decision makers. Rewording questions to capture the concept in terms more readily understood by diverse audiences might encourage further applications. For example, Table 4 offers suggestions for more understandable expressions in one context.

In terms of process, the RAQT1.0 suggests each question be met with one of three responses: yes, no, or not applicable (NA). Yet, users of the RAQT1.0, even if a trained team of multidisciplinary risk practitioners, may be unable to decide how to respond to each question. Alternatively, encouraging the use of interpretive scales for assessing the importance of each question for a particular application, as illustrated in Figure 1, would enable more nuanced interpretations and support priority setting for corrections and improvements.

A further process issue arose for the two independent microbiologists applying the RAQT1.0 to QMRAs. They undertook the arduous task of conducting comprehensive and systematic reviews of the literature available before and after publication of the QMRA reports to address shortfalls in Basis of Knowledge, not just for the microbiology literature, but also for studies relevant to the disconnects noted between the analyses and decision making and risk communication. This work extended the time and energy required for the microbiologists to fully address the RAQT1.0 questions regarding previous and subsequent risk management and risk communication decisions and assumptions. Lessons learned from these applications to QMRAs will inform and guide the work to be reported in more detail by Coleman and Ross (in preparation).

In general, the RAQT1.0 case for both QMRAs proved useful for: (1) retrospectively opening dialogue about the qualities of evidence and analysis within QMRAs; (2) identifying when reassessment and reevaluation are warranted; (3) prospective planning for design and external reviews for future QMRAs; and (4) beginning broad deliberations with diverse stakeholders to improve design of QMRAs and, hence, evidence-based risk management.

A broader challenge in cultural property care is proliferation of risk-based approaches not built on risk analysis understandings. In the cultural property management field, *inter alia*, this problem may arise from a sense of responsibility for minimization of all risks, despite their relative significance, as well as the Dunning–Kruger effect (Kruger & Dunning, 1999), leading to mistaken impressions of self-competency in risk analysis. From the risk analysis side, a lack of codified professional standards contributes to the problem. Application of the RAQT1.0 retrospectively, prospectively, or both all offer opportunities for reducing these problems.

For both retrospective and prospective applications, reducing or eliminating the need for considering questions that are irrelevant to the application could save much time and effort in applying the RAQT1.0. One solution to this shortcoming is to provide a scheme for filtering the questions by their relevance to evaluating how “fit for purpose” the risk assessment is relative to the risk management challenge the assessment is designed to address. Possibly, one or more questions focused on how well the risk assessment fits the purpose of the risk management exercise could be posed first, then used to filter which of the more technical questions should be addressed.

Another insight can be drawn by comparing the RAQT applications presented here with perspectives from the corporate culture literature. The use of the RAQT1.0, and any future iterations, bring the additional benefit of translating the risk analysis process into a form of riskwork that involves a series of day-to-day activities carried out by managers to create reflections on the meaning of risks (Power, 2016).

Riskwork extends risk management that seeks to balance governing risks, avoiding harm, and exploring opportunities (Society for Risk Analysis, 2018) by encouraging reflections on risks that embrace their complexities and uncertainties (Hardy et al., 2020). For example, freedom to speak up and report risks is key to achieving high-quality risk assessments and is facilitated by access to technology that enables straightforward reporting and analysis of risk (Palermo, 2016). The use of risk maps to plot the expected probability and impact of risks is more valuable when accompanied by riskwork processes that foster collaboration and support project execution (Jørgensen & Jordan, 2016). Similarly, analysts' and decision makers' collective use of the RAQT is a form of riskwork that would foster shared understanding of risks and risk analysis quality.

In summary, the RAQT1.0 has been shown to be useful for highlighting shortfalls and areas for improvement in risk assessment, risk management, and risk analysis which encompasses both. The RAQT1.0 also provides a means to stimulate broader reflections on risks and riskwork. We do note, however, that test applications were arduous, thus raising a question for more widespread adoption from a cost–benefit perspective. With both prospective and retrospective assessment of quality in risk analysis of critical importance, the lessons discussed here could lead to improvements embodied in RAQT2.0.

ACKNOWLEDGMENTS

The authors thank John Lathrop for contributing introductory text and helpful comments throughout the preparation of this paper. We gratefully acknowledge Patricia Larkin and Richard Williams who provided valuable feedback on an earlier version of this work. We appreciate and have benefited from comments by four anonymous reviewers. Coleman acknowledges Tom Ross and Richard Williams for their contributions to the Society for Risk Analysis (SRA) roundtable and workshop on which Section 2 is partly based. Waller acknowledges the contributions of many contributing to the two applications of the Cultural Property Risk Analysis Model (CPRAM) evaluated in Section 3. These include staff of the Canadian Museum of History, especially Wanda McWilliams, Rebecca Latourell, Christine Quinn, Patrice Rémillard, Tinisha Simard, Stefanie St-Jean, Susannah Warren and staff at the Carnegie Museum of Natural History, especially Suzanne McClaren, Gretchen Anderson, and Marion Burgwin, as well as Emily Higginson and Moya Dumville of Protect Heritage Corp. For the work on planning the evaluation of collection storage upgrade options, Waller thanks his principal collaborator, Melissa King, Samuel H. Kress Foundation, and colleagues at the Smithsonian Institution, especially Rebecca Kaczkowski, Catharine Hawks, and Evan Cooney for their contributions to the work described in Section 3.2.

ORCID

Robert Waller https://orcid.org/0000-0002-9500-4113
Margaret Coleman https://orcid.org/0000-0001-8185-1736
Samuel Denard https://orcid.org/0000-0002-0655-590X
Emma Soane https://orcid.org/0000-0001-6090-1212

REFERENCES

Biden, J. R. (2023). *National cybersecurity strategy*. Washington, DC, USA. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Booth, M. (2021). Letter from FSANZ Chief Executive Officer to Ms Rebecca Freer, Australian Milk Movement, dated 16 March, 2021. Personal communication provided by Ms. Freer and available as Appendix B in the report at the link: https://static1.squarespace.com/static/5632b842e4b06192191af6e3/t/61e0af4cf338d8254a79b1b5/1642114903180/CSCreportFSANZ2009critique14October2021.pdf

Charette, R. N. (2005). Why software fails. *IEEE Spectrum*. https://spectrum.ieee.org/why-software-fails

Codex Alimentarius Commission (CAC). (1999). *Principles and guidelines for the conduct of microbiological risk assessment* (CAC/GL-30). https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url= https://%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FStandards%252FCXG%2B30-1999%252FCXG_030e_2014.pdf

Cybersecurity & Infrastructure Security Agency. (2021). *Software bill of materials* | CISA. Retrieved from https://www.cisa.gov/sbom

Denard, S. (2021). *Development cycle modeling and risk calculation* (PhD dissertation). Texas Tech University.

Denard, S. (2022). *Software development process risk analysis*. Paper presented at the Society for Risk Analysis Annual Meeting 2022, Tampa, Florida, USA.

Denard, S., Ertas, A., Mengel, S., & Ekwaro-Osire, S. (2020a). Development cycle modeling: Resource estimation. *Applied Sciences*, *10*(14), 5013. https://doi.org/10.3390/app10145013

Denard, S., Ertas, A., Mengel, S., & Ekwaro-Osire, S. (2020b). Development cycle modeling: Process risk. *Applied Sciences*, *10*(15), 5082. https://doi.org/10.3390/app10155082

Dietert, R. R., Coleman, M. E., North, D. W., & Stephenson, M. M. (2021). Nourishing the human Holobiont to reduce the risk of non-communicable diseases: A cow's milk evidence map example. *Applied Microbiology*, *2*(1), 25–52. https://www.mdpi.com/2673-8007/2/1/3

DOD CIO. (2023). *Cybersecurity Maturity Model Certification (CMMC) Program*. https://dodcio.defense.gov/CMMC/About/

Farber, J. M., Zwietering, M., Wiedmann, M., Schaffner, D., Hedberg, C. W., Harrison, M. A., Hartnett, E., Chapman, B., Donnelly, C. W., Goodburn, K. E., & Gummalla, S. (2021). Alternative approaches to the risk management of *Listeria monocytogenes* in low risk foods. *Food Control*, *123*, 107601.

Federal Bureau of Investigation (FBI). (2023). *InfraGard*. https://www.infragard.org

Food and Drug Administration & Food Safety & Inspection Service (FDA/FSIS). (2003). *Quantitative assessment of relative risk to public health from foodborne* Listeria monocytogenes *among selected categories of ready-to-eat foods*. https://www.fda.gov/food/cfsan-risk-safety-assessments/quantitative-assessment-relative-risk-public-health-foodborne-listeria-monocytogenes-among-selected; https://www.fda.gov/food/cfsan-risk-safety-assessments/listeria-monocytogenes-risk-assessment-questions-and-answers

Food Standards Australia New Zealand (FSANZ). (2009). *Microbiological risk assessment of raw cow milk. Risk assessment microbiology section*. https://www.foodstandards.gov.au/code/proposals/documents/p1007%20ppps%20for%20raw%20milk%201ar%20sd1%20cow%20milk%20risk%20assessment.pdf

Goseva-Popstojanova, K., & Hamill, M. (2009). *Software faults, failures, and fixes: Lessons learned from a large NASA mission*. https://www.nasa.gov/centers/ivv/pdf/585637main_SWFaultsFailuresFixes.pdf

Haimes, Y. Y. (1981). Hierarchical holographic modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, *11*(9), 606–617.

Haimes, Y. Y., Kaplan, S., & Lambert, J. H. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis*, *22*(2), 383–397.

Hanson, H., Whitfield, Y., Lee, C., Badiani, T., Minielly, C., Fenik, J., Makrostergios, T., Kopko, C., Majury, A., Hillyer, E., Fortuna, L., Maki, A., Murphy, A., Lombos, M., Zittermann, S., Yu, Y., Hill, K., Kong, A., Sharma, D., & Warshawsky, B. (2019). *Listeria monocytogenes* associated with pasteurized chocolate milk, Ontario, Canada. *Emerging Infectious Diseases*, *25*(3), 581–584.

Hardy, C., Maguire, S., Power, M., & Tsoukas, H. (2020). Organizing risk: Organization and management theory for the risk society. *Academy of Management Annals*, *14*(2), 1032–1066.

Hill, B., Smythe, B., Lindsay, D., & Shepherd, J. (2012). Microbiology of raw milk in New Zealand. *International Journal of Food Microbiology*, *157*(2), 305–308.

IBM Security. (2022). *Cost of a data breach report 2022*. Armonk, NY. https://www.ibm.com/reports/data-breach

IFT. (2001). *A report of the Institute of Food Technologists for the Food and Drug Administration of the United States Department of Health and Human Services* (IFT/FDA Contract No. 223-98-2333, Task Order No. 4, 109 pp). Institute of Food Technologists.

IIBA. (2015). *A guide to the business analysis body of knowledge* (Babok Guide). International Institute of Business Analysis.

Jørgensen, L., & Jordan, S. (2016). Risk mapping: Day-to-day riskwork in inter-organizational project management. In M. Power (Ed.), *Riskwork: Essays on the organizational life of risk management* (pp. 50–71). Oxford University Press.

Krasner, H. (2021). *The cost of poor software quality in the US: A 2020 report*. Milford, MA, USA. https://www.it-cisq.org/the-cost-of-poor-software-quality-in-the-us-a-2020-report.htm

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, *77*(6), 1121–1134. https://www.avaresearch.com/files/UnskilledAndUnawareOfIt.pdf

Lathrop, J., Roed, W., Ackerlund, S., Waller, R., Aven, T., Flage, R., Hetou, G., Belzer, R., Wilkins, A., Trevan, T., Yellman, T., Simon, T., Dikmen, I., Denard, S., Soane, E., Smith, T., Decker, D., Larkin, P., & Dyer, R. (2020). *SRA Risk analysis quality test release 1.0*. Society for Risk Analysis. https://www.sra.org/resources/risk-analysis-quality-test/

Latorre, A. A., Pradhan, A. K., Van Kessel, J. A., Karns, J. S., Boor, K. J., Rice, D. H., Mangione, K. J., Gröhn, Y. T., & Schukken, Y. H. (2011). Quantitative risk assessment of listeriosis due to consumption of raw milk. *Journal of Food Protection*, *74*(8), 1268–1281.

NIST. (2011). *Managing information security risk*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Northolt, M. D., Beckers, H. J., Vecht, U., Toepoel, L., Soentoro, P. S. S., & Wisselink, H. J. (1988). *Listeria monocytogenes*: Heat resistance and behaviour during storage of milk and whey and making of Dutch types of cheese. *Netherlands Milk and Dairy Journal*, *42*, 207–219.

Oikonomou, G., Addis, M. F., Chassard, C., Nader-Macias, M. E. F., Grant, I., Delbès, C., Bogni, C. I., Le Loir, Y., & Even, S. (2020). Milk microbiota: What are we exactly talking about? *Frontiers in Microbiology*, *11*, 60.

Palermo, T. (2016). Technoculture: Risk reporting and analysis at a large airline. In M. Power (Ed.), *Riskwork: Essays on the organizational life of risk management and decision economics* (pp. 150–171). Oxford University Press.

Power, M. (2016). Introduction—Riskwork: The organizational life of risk management. In M. Power (Ed.), *Riskwork: Essays on the organizational life of risk management and decision economics* (pp. 1–25). Oxford University Press.

SAE International G-32 Cyber Physical Systems Security Committee. (2023). *Cyber physical systems security software assurance JA6678*. https://www.sae.org/standards/content/ja6678/

Sebastianski, M., Bridger, N. A., Featherstone, R. M., & Robinson, J. L. (2022). Disease outbreaks linked to pasteurized and unpasteurized dairy products in Canada and the United States: A systematic review. *Canadian Journal of Public Health*, *113*(4), 569–578.

Society for Risk Analysis. (2018). *Glossary*. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Stasiewicz, M. J., Martin, N., Laue, S., Gröhn, Y. T., Boor, K. J., & Wiedmann, M. (2014). Responding to bioterror concerns by increasing milk pasteurization temperature would increase estimated annual deaths from listeriosis. *Journal of Food Protection*, *77*(5), 696–705.

Waller, R. (2003). *Cultural property risk analysis model: Development and application to preventive conservation at the Canadian Museum of Nature*. Göteborg Studies in Conservation 13, ISSN 0284–6578; ISBN 91-7346-475-9. Göteborg Acta Universitatis Gothoburgensis, Göteborg. xvi + 189 p.p.

Waller, R. (2008). Comprehensive risk assessment: Applying the cultural property risk analysis model to the Canadian Museum of Nature. In I. Linkov, E. Ferguson, & V. S. Magar (Eds.), *Real time and deliberative decision making* (pp. 179–190). NATO Science for Peace and Security Series-C: Environmental Security. Springer.

Waller, R. (2019). Collection risk assessment. In L. Elkin & C. A. Norris (Eds.), *Preventive conservation: Collection storage* (pp. 59–90). Society for the Preservation of Natural History; American Institute for Conservation of Historic and Artistic Works; Smithsonian Institution; The George Washington University Museum Studies Program. ISBN 978-0-9978679-2-3.

How to cite this article: Waller, R., Coleman, M., Denard, S., & Soane, E. (2024). Lessons identified from applications of the Risk Analysis Quality Test Release 1.0. *Risk Analysis*, 1–10. https://doi.org/10.1111/risa.14292