Experiential Activities for Risk Management Education

Michael E. Whitman, Ph.D., CISM, CISSP
Kennesaw State University
Kennesaw, GA, USA
mwhitman@kennesaw.edu

Robert L. Chaput, MA, CISSP, HCISSP, CRISC, C|EH, CIPP/US
Clearwater Compliance, LLC
Nashville, TN, USA
bob.chaput@clearwatercompliance.com

***Abstract*—A core premise in the instruction of Information Security/Cybersecurity is that risk management is a cornerstone of security management, as evidenced in the promotion of GRC (Governance, Risk Management and Compliance) as the strategic triad in the trade press. While a theoretical exploration of risk management is important, the provision of an experiential activity to support the theory is valuable in cementing the knowledge in students. This paper will discuss popular risk management methodologies and examine a number of tools to support the instruction of the more common methodologies by instructors without substantial cost or learning curve.**

Keywords—Risk Management, Risk Assessment, Information Security Education, Cybersecurity Education, Experiential Education Background

I. Introduction

With the well-documented increase in demand for Information Security / Cybersecurity Professionals, there is a corresponding increase in academic program offering degrees in security related fields, as evidenced in the increase in Center of Academic Excellence Designated Schools [1]. Risk Management (RM) is commonly taught as part of security curriculum. RM is the identification, assessment and remediation of risk to an organization's information assets and systems [2] and is recognized as critical to the organization's security program [3, 4, 5]. While professional certifications like the CISSP, CRISC and CISM have theoretical RM content, and while current standards such as NIST and ISO promote the need for RM, there is little available to assist the instructor in developing RM curriculum, especially if the instructor seeks to provide hands-on experiential activities.

This paper examines common RM methodologies promoted by key standards organizations and offers alternatives the instructor can use to implement an experiential component with their RM theoretical instruction.

II. Popular Risk Management Approaches

There are a few RM methodologies and standards an instructor can select when developing curriculum. While there are some academic frameworks for teaching RM [e.g. 5], they lack widespread adoption and the formal support of standards-based approaches. The challenge is to select a methodology that is widely accepted enough to provide a foundation for students in their career, yet suitable for use as an instructional tool.

A. Qualitative versus Quantitative Risk Assessment

Before examining the current available RM methodologies suitable for use in information security instruction, the first fundamental question is whether to use qualitative or quantitative valuations. RM begins with an expectation that, unless mandated, one should never spend more to protect an information asset than it is worth. Risk assessment (RA) is the first major component of RM – first you find the risk and then you address it. Some RA calculations used in the popular Cost-Benefit Analysis (CBA) expect the user to value of an asset. The challenge becomes how do you *accurately* calculate the value of an information asset. Using a purely quantitative approach means the organization must assign an accurate dollar value for each of its information assets. Yet there is little in the literature that shows any real success in doing just that [6]. As a result, many organizations chose a simplistic qualitative assessment – such as a scale of "very valuable" to "not valuable at all", also implemented in some RA tools. This approach can result in an oversimplification of information asset values, which introduces problems in prioritizing RM efforts. If the organization has multiple assets with the same value, and limited funds, which assets should be protected first?

The natural evolution is to use a hybrid method of valuing information assets (or threats) using tools like weighted tables. In a weighted table approach, the organization develops categories to compare assets, such as:

- Which information asset is the most critical to the success of the organization?
- Which information asset generates the most revenue?
- Which information asset generates the highest profitability?
- Which information asset is the most expensive to replace?
- Which information asset is the most expensive to protect?

979-8-6974-5784-9/20/$26.00 ©2020 CISSE

- Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability? [2]

These categories are then weighted, with each asset assigned a value per category, with values calculated as the sum of category weights times values. The result is not purely quantitative nor purely qualitative, simplifying assessment, but resulting in a more granular comparison.

B. Generally Accepted Risk Management Methods

RM principles date back to the 1983 publication "Risk Assessment in the Federal Government: Managing the Process" known as the "Red Book" [7]. NIST SP 800-30 "Risk Management Guide for Information Technology Systems" provided the foundation for most U.S. government RM efforts [8]. The now retired SP 800-30 version of RM the following steps:

1. System Characterization – identification of information assets and understand of systems to identify vulnerabilities.
2. Threat Identification – examination of the threat environment for threats with the potential to impact systems and assets.
3. Vulnerability Identification – comparison of threats to assets, and identification of vulnerabilities.
4. Control Analysis – identification and examination of current controls for each Threat/Vulnerability/Asset (TVA) triple.
5. Likelihood Determination – calculation of the probability that a particular threat could exploit a particular vulnerability in an information asset, using a simple qualitative scale.
6. Impact Analysis – determination of the outcome or impact of a successful attack within a given TVA triple.
7. Risk Determination – calculation of risk of each TVA triple by combining likelihood and impact.
8. Control Recommendations – based on the residual risk, the recommendation of additional controls.
9. Results Documentation – documentation and review of the results of the RM process [8].

The "likelihood/probability" and "impact/consequences" approach is common in RM methodologies, as illustrated above and in the CISSP common body of knowledge [2, 9, 14, 16, 19, 23].

C. The NIST Risk Management Framework

With the publication of SP 800-30, Revision 1 in 2011, NIST began promoting its Risk Management Framework (RMF) as the preferred methodology for performing RM. According to SP - NIST Special Publication 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations [11], there are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the process and six main steps, as shown in Figure 1.

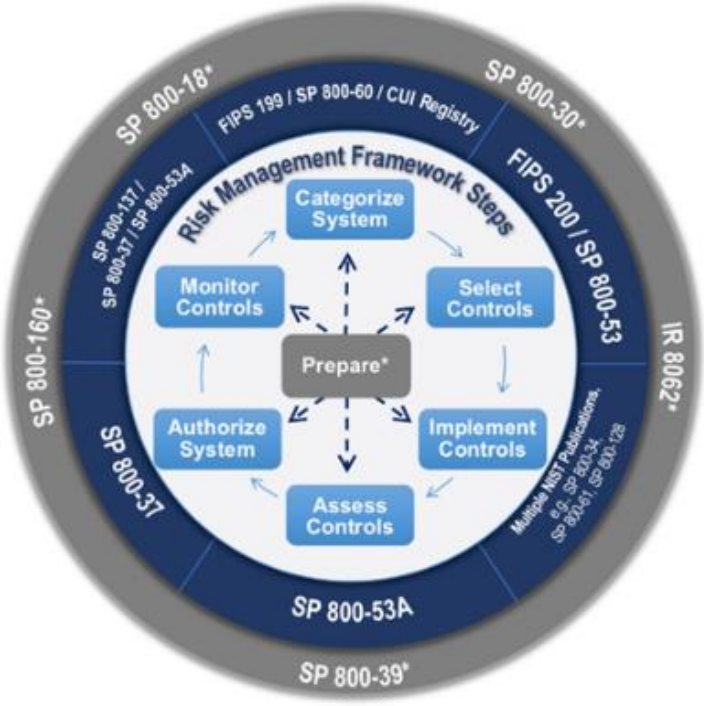

Fig. 1. NIST Risk Management Framework [12].

There are several NIST publications that address aspects of the RMF applicable to both government and non-government organizations, useful in formulating coursework [See 10, 11, 12 & 13]. One of the benefits of using NIST documents as an instructional foundation is the availability of the NIST library (http://csrc.nist.gov) to faculty and students alike.

D. The ISO Approach to Risk Management

The International Organization for Standardization (ISO; www.iso.org) has two closely related standards for RM. ISO 31000 focuses on general business risk, while ISO 27005 focuses on information security RM. The RM methodology is virtually identical in these standards.

1) ISO 31000: 2018

The ISO RM approach involves two major phases as shown in Figure 2. The RM Framework involves the development and design of the overall RM effort - the *planning* phase. The RM Process is the conduct of an iteration of risk assessment and treatment - the *doing* phase.

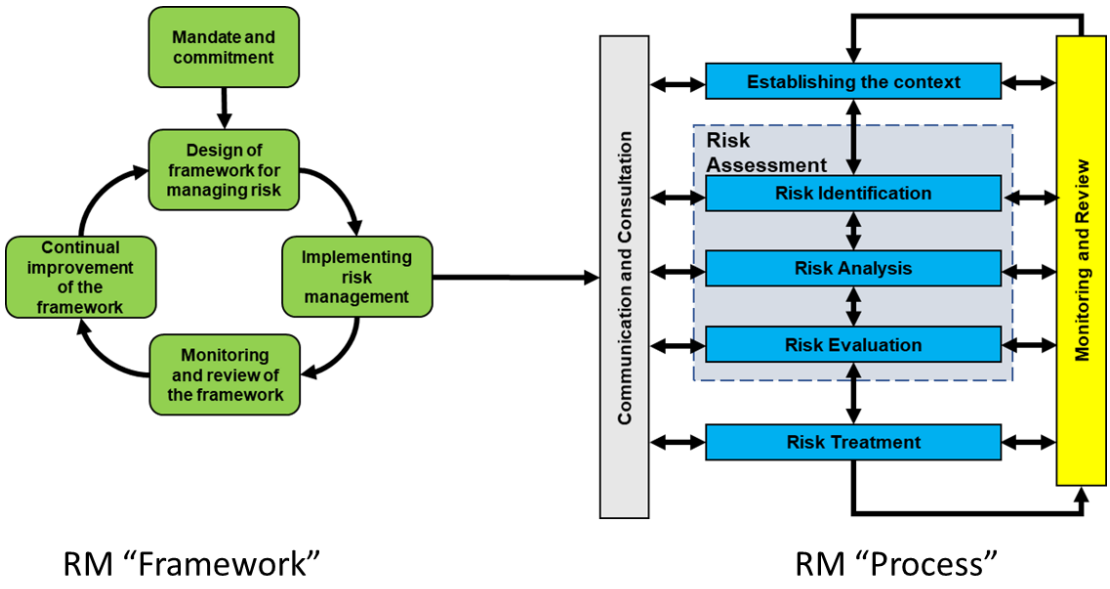

Fig. 2. ISO 31000: 2018 Approach to Risk Management [14].

The ISO RM Framework includes "integrating, designing, implementing, evaluating and improving risk management across the organization" [14], guided by leadership and commitment of the organization.

The RM Process begins with defining the RM project, its scope, personnel, resources and determine who will conduct and manage the RM project. From there the RM methodology involves two main phases. The first is Risk Assessment, which includes Risk Identification to determine the location of information assets at risk; Risk Analysis to determine the level of risk present in those information assets; and Risk Evaluation to assess whether the level of risk present exceeds the organization's risk threshold or whether additional treatment is needed. This step is followed by the second phase - Risk Treatment which is the application of additional controls to reduce risk to an acceptable level, or the decision to remove the asset from the threat environment [14].

Throughout the RM Process there is constant monitoring and review of the process and communication with organizational decision makers concerning progress, as well as formal documentation of each step in the process [14].

2) ISO 27005: 2018-07

ISO 27005:2018-07 focuses specifically on information security RM. Currently, the 27005 approach is an adaptation of the 31000 approach, focusing more extensively on the RM Process. The standard does provide a more granular look at RM, calling out risk acceptance as a separate step, as shown in Figure 3. This approach provides an easier means to educate students with, as it clarifies risk decision points that support the determination of whether the risk efforts are acceptance, or whether another iteration is needed [15].

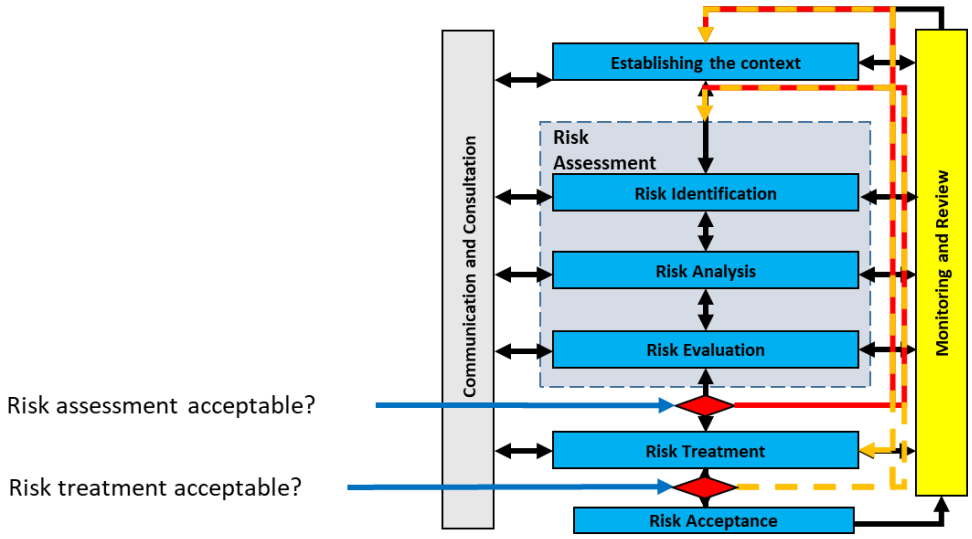

Fig. 3. ISO 27005 Approach to Risk Management [15].

E. Factor Analysis of Information Risk (FAIR)

FAIR was developed by Jack A. Jones to help organizations understand, analyze, and measure information risk. Projected outcomes are more cost-effective information RM, greater credibility for the InfoSec profession, and a foundation from which to develop a scientific approach to RM [16].

FAIR's framework comprises four stages: 1) Identify scenario components; 2) Evaluate Loss Event Frequency (LEF); 3) Evaluate Probable Loss Magnitude (PLM); and 4) Derive and articulate Risk. FAIR's likelihood is "Loss Event Frequency" and impact is "Loss Magnitude", determining and using these values to define an asset's level of risk, as shown in Figure 4.

In its early days, FAIR was a pen-and-paper exercise involving a series of qualitative values to indicate key inputs. These values were put into tables, which provided subsequent values used to determine risk levels on scales of "Severe" to "Low", also shown in Figure 4. In 2014, FAIR became an Open Group international RM standard and rebranded as Open FAIR™. In 2015, CXOWARE became RiskLens and the FAIR Institute was created [17].

F. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

There are other RM models available, many of which have been abandoned or discarded, including the Carnegie Mellon University Software Engineering Institute's OCTAVE methods. OCTAVE was promoted in three variants – OCTAVE for large organizations, OCTAVE-S for small organizations, and OCTAVE Allegro for concentrated RA.

OCTAVE involved a three-phase approach of 1) build asset-based threat profiles; 2) identify infrastructure vulnerabilities, and 3) develop security strategy and plans [20]. OCTAVE Allegro streamlined the risk assessment portion of OCTAVE and provided easy to use forms to use in the assessment [19]. As such OCTAVE Allegro can still serve as an effective paper-based exercise for the instruction of risk assessment

(See https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=309051).

III. Experimental Support for RM Instruction

While it is generally accepted that the use of hands-on components in the instruction of security is a positive approach [20, 21], literature that describe this approach in RA/RM instruction is virtually non-existent.

A. Paper-Based Exercises

As mentioned earlier, OCTAVE Allegro is one method of using a pen-and-paper exercise to support the risk assessment process. While more complicated than other approaches, it is a realistic and usable exercise in risk assessment. OCTAVE Allegro includes worksheets and questionnaires to perform risk assessment against an academic case organization, or real-world organization in the event of service-learning assignments [19].

In addition, the original FAIR Basic Risk Assessment Guide provides an excellent tutorial for students to use to calculate risk qualitatively. While no longer supported by the FAIR Institute, this approach allows the instructor to present the fundamentals of identifying and evaluating risk for an asset [16].

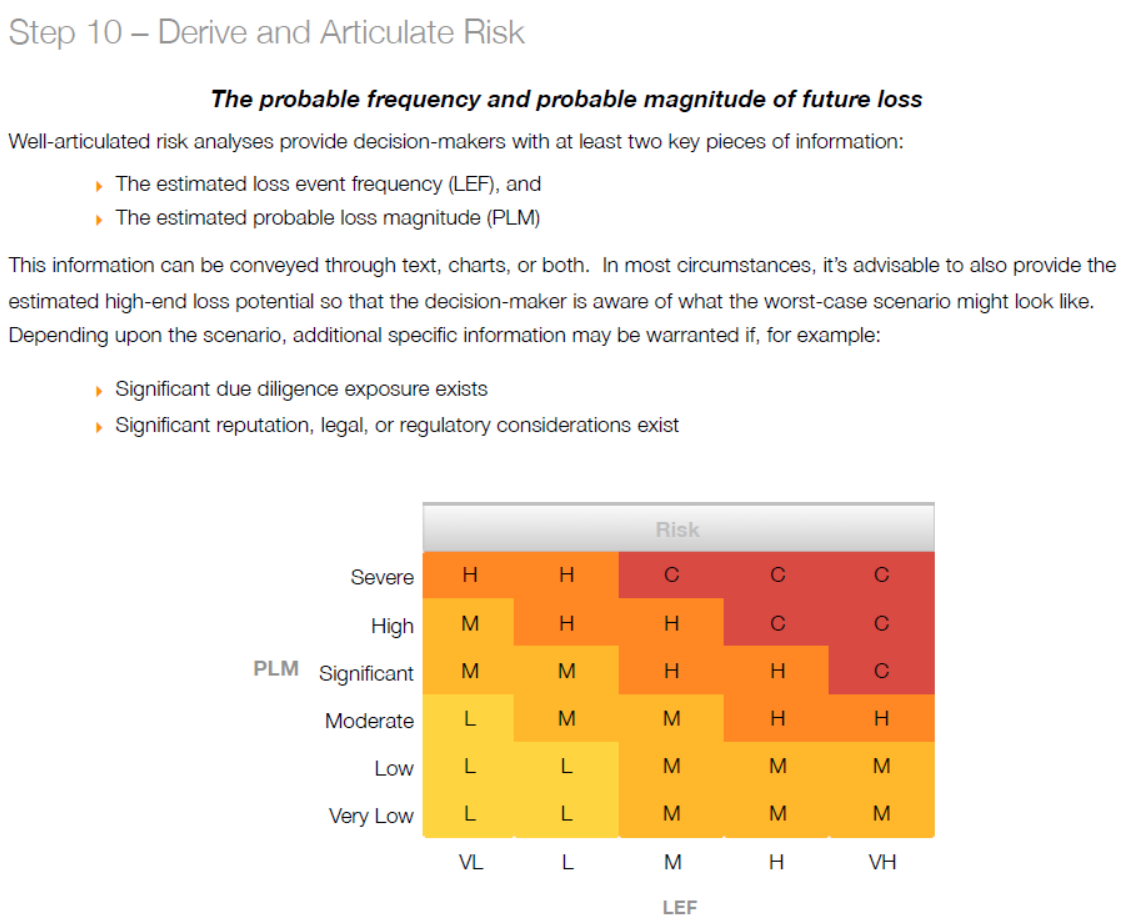

Fig. 4. FAIR Calculation of Risk [16].

B. *Software-Based Exercises*

For a more advanced and real-world approach to teaching risk assessment, two organizations have offered academic partnerships allowing the use of their Web-based products in the classroom.

1) *RiskLens & FAIR*

Risk Lens, with the FAIR Institute offer FAIR-U - a training tool based on the commercial version of the RiskLens Platform (https://www.fairinstitute.org/fair-university-curriculum). FAIR-U provides several risk assessment scenarios and is focused on training and education of the FAIR approach. The application is provided free of charge with a self-registration function. In addition, Risk Lens offers a video-based training course for the use of FAIR [See 22].

As shown in Figure 5, the application is very visual with representations of the values of the FAIR methodology presented for each scenario (such as a phishing attack resulting in a database breach). For a given scenario, the student enters several of the initial values, resulting in an annual loss exposure. Comparison of this exposure between threat/asset pairs would allow prioritization of remediation effort. For the most part, once a student has been taught this methodology, completing the tables is effectively straightforward estimation. What is not included in the software is assistance in the identification of information assets, and the understanding of the actual vulnerabilities associated with them. It does make a very effective tutorial on likelihood and impact once the terms are translated into the FAIR terminology.

2) *Clearwater & IRM|Pro®*

For those instructors looking for a more robust and more formal approach to performing risk assessment, Clearwater's Information Risk Management | Professional (IRM|Pro®) is a leading RM platform. While not widely advertised, Clearwater provides full complimentary access to IRM|Pro® to academic institutions to support the instruction of RM. Currently Kennesaw State University uses this application in two undergraduate and three graduate security management courses.

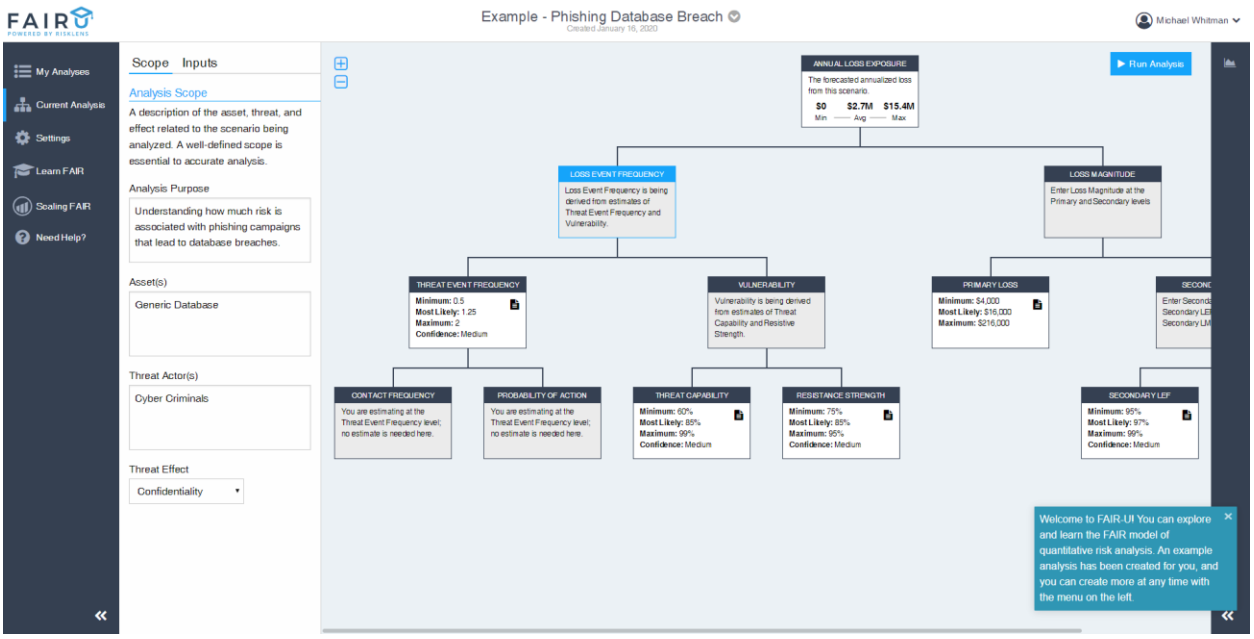

Fig. 5. FAIR-U Risk Analysis Training Application [23].

Perhaps the strongest endorsement of the product is its foundation in the NIST RM methodology, having been developed based on NIST SP 800-30 [9, 11]. While the application has improved on some of the qualitative categories used in the assessment of likelihood and impact, many definitions and examples from the SP are available in help screens.

In teaching risk assessment using this application, the instructor could provide a case organization, complete with information on information assets and supporting systems. As shown in Figure 6, users identify, then enter and describe their information assets.

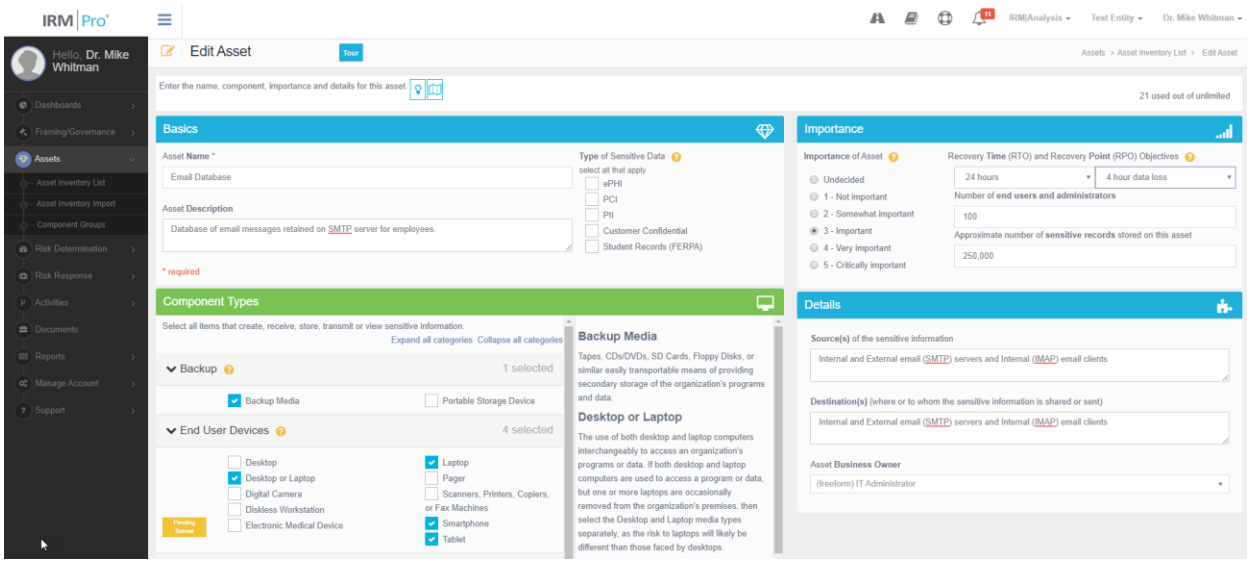

Fig. 6. Clearwater IRM|Pro® Asset Entry [24].

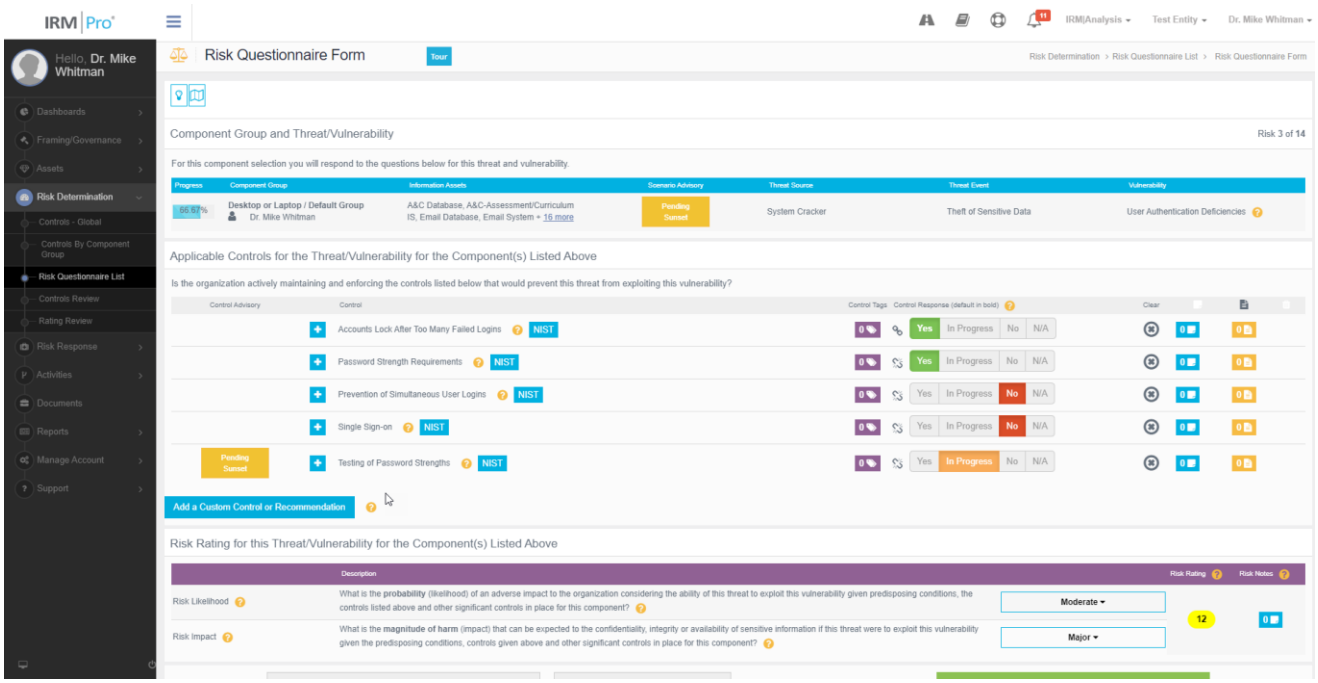

Fig. 7. Clearwater IRM|Pro® Risk Questionnaire [24].

The application separates information assets from the systems that store, process and access them. In order to manage the scope and scale of an academic project, it is recommended to limit projects to a few information assets. The application ties into the NIST SP 800-53 control structures [25], building the threat/vulnerability/asset triples commonly taught, as shown in Figure 7. In this application, users specify the current controls and safeguard implemented by selecting from available options in a Risk Questionnaire. Once all control statuses are indicated, users can specify the likelihood and impact using the scales provided.

The next step of the project involves the assignment of additional controls for TVA triples that have a current risk level exceeding the organization's risk threshold. The application allows the user to perform a risk response – projecting additional controls the organization would deploy and then estimating the residual risk if those controls were implemented. While the application can track the implementation of the controls and revision of the level of risk, a student's project typically ends with the estimation of risk response. Students can export reports for submission with their assignments.

The advantages of IRM|Pro®, beyond its foundation in NIST methodology, are in the easily understood implementation of RA assessment. Users are not expected to brainstorm the threat/asset scenarios, but simply identify the assets, define how the assets are accessed, and then answer questions as to the organization's current protection of those assets. The bulk of the work is performed by the software. The application takes the assets entered, creates TVA triples for each asset and then asks for input from the user. Once the user enters the current protection strategies, they are prompted as to whether additional security controls could be implemented based on NIST recommendations. After determining likely additional controls, the user then estimates the level of organizational risk that would exist after the additional controls are implemented, resulting in a risk reduction. The software is robust enough to allow the organization to track the implementation of these additional controls and has a sophisticated dashboard interface to oversee the current risk profile and improvement plans for the entire enterprise.

Since IRM|Pro® is designed as an enterprise solution, administration for an academic environment is trivial. At the beginning of the term, the instructor submits an Excel file with the student roster and institutional email and a support technician loads the course, clearing the work of previous classes. Each student is assigned to their own "entity", which the instructor can easily view, and thus grade, though a single drop-down menu option from their account.

Because IRM|Pro® is a commercial application, the largest drawback for classroom use is the need to provide detailed instructions for students. Clearwater does not provide training tutorials. Clearwater also updates its software regularly and without warning, which is both an advantage and a disadvantage for its use in academic instruction.

IV. Summary

Teaching RM can be challenging, especially without an experiential exercise to enforce the theoretical concepts. With the use of experiential exercises, students can gain a deeper understanding and appreciation for the complexity and importance of a RM project, especially in the assessment of risk. Students can gain even more from applying these academic exercises to the real-world using approaches like service-learning to conduct risk assessments on actual organizations [26].

Whichever approach an instructor selects, it is important to ensure they follow an established methodology that the student can take with them into the workplace, as a student completing a course that includes RM may find themselves applying lessons learned in the classroom on the job.

References

[1] NIETP. NSA/DHS National CAE in Cyber Defense Designated Institutions, Accessed 1/05/2020 from https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm (n.d.).

[2] Whitman, M.E. and Mattord, H.J. Management of Information Security, 6th ed. Cengage Learning, Inc., Boston, MA, 02210 (2019).

[3] Baskerville, R. Risk analysis: an interpretive feasibility tool in justifying information systems security, European Journal of Information Systems, Vol. 1 No. 2, pp. 121-130 (1991).

[4] Shedden, P., Ruighaver, A.B. and Ahmad, A. Risk management standards – the perception of ease of use, Journal of Information Systems Security, Vol. 6 No. 3 (2010).

[5] Spears, J.L. and Barki, H. User participation in information systems security risk management, MIS Quarterly, Vol. 34 No. 3, p. 503 (2010).

[6] Wangen, G., Snekkenes, E., and Hallstensen, C. A framework for estimating information security risk assessment method completeness. International Journal of Information Security, Vol. 17, No. 6, pp. 681-699 (2018).

[7] Greenberg, M., Goldstein, B.D., Anderson, E., Dourson, M., Landis, W, and North, D.W. Whither Risk Assessment: New Challenges and Opportunities a Third of a Century After the Red Book, Risk Analysis, Vol. 35, No. 11, pp. 1959-1968 (2015).

[8] Stoneburner, G., Goguen, A. and Feringa, A. NIST SP 800-30, Guide for Conducting Risk Assessments, Accessed 1/16/2020 from https://doi.org/10.6028/NIST.SP.800-30 (2002).

[9] Hernandez, S (Ed.) Official ISC2 Guide to the CISSP CBK, 3rd ed., CRC Press, Boca Raton, FL, 33487 (2013).

[10] NIST JTF. NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments, Accessed 1/16/2020 from https://doi.org/10.6028/NIST.SP.800-30r1 (2012).

[11] NIST JTF. NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Accessed 1/16/2020 from https://doi.org/10.6028/NIST.SP.800-37r2 (2018).

[12] NIST JTFTI. NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View. Accessed 1/16/2020 from https://csrc.nist.gov/publications/detail/sp/800-39/final (2011).

[13] NIST. Risk Management Framework, Accessed 1/16/2020 from https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview (n.d.).

[14] ISO 31000 Risk Management – Guidelines, 2nd ed. Vernier, Geneva (2018).

[15] ISO/IEC 27005 Information technology — Security techniques — Information security risk management, 3rd ed. Vernier, Geneva (2018).

[16] FAIR Basic Risk Assessment Guide, Accessed 7/1/2013 from www.risk managementinsight.com/media/documents (2010).

[17] RiskLens. CXOWARE Becomes RiskLens, Accessed 1/15/2020 from https://www.prnewswire.com/news-releases/cxoware-becomes-risklens-aligning-with-mission-to-empower-organizations-to-manage-cyber-risk-from-the-business-perspective-300109155.html (2015).

[18] Alberts, C., Dorofee, A., Stevens, J. and Woody, C. Introduction to the OCTAVE Approach Carnegie Mellon University, Software Engineering Institute, Accessed 1/15/2020 from https://http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419 (2003).

[19] Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, TECHNICAL REPORT CMU/SEI-2007-TR-012, Carnegie Mellon University, Software Engineering Institute, Accessed 1/15/2020 from https://http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419 (2007).

[20] Sharma, S.K. and Sefchek, J. Teaching information systems security courses: A hands-on approach. Computers and Security, Vol. 26, No. 4, pp. 290-299 (2007).

[21] Murthy, N. Teaching Computer Security with a Hands-On Component, R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 204–210 (2013).

[22] FAIR. Announcing the First Video-Based Training Course for FAIR. Downloaded from https://www.risklens.com/blog/announcing-the-first-video-based-training-course-for-fair/ on 05/29/2020 (2017).

[23] FAIR. FAIR-U The Risk Analysis Training Application based on FAIR. Downloaded from https://www.fairinstitute.org/fair-u on 1/16/2020 (n.d.).

[24] Clearwater Information Risk Management, Accessed 01/16/20 from https://software.clearwatercompliance.com/ (n.d.).

[25] NIST JTF. NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, Accessed 1/16/2020 from https://doi.org/10.6028/NIST.SP.800-53r4 (2017).

[26] Spears, J.L. Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course, Journal of Information Systems Education, Vol. 29, No. 4, pp. 183-201 (2018).