EXPRESSO

The Risk Assessment Express

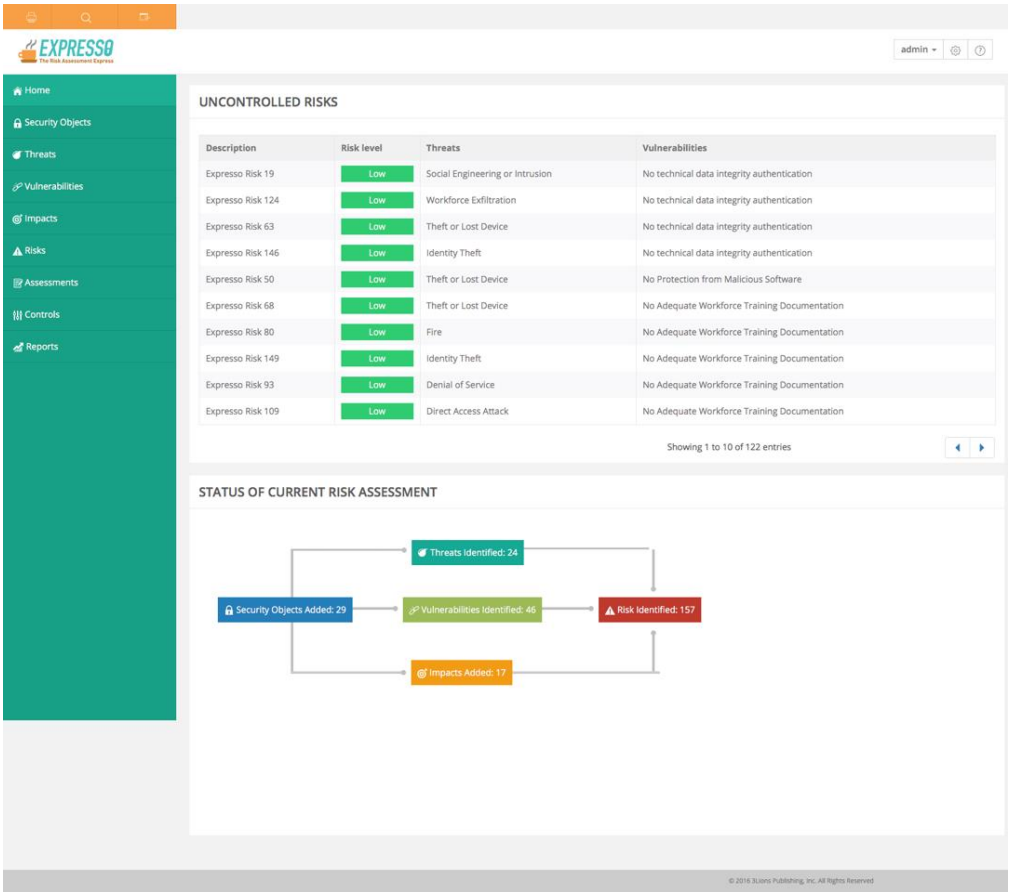
HIPAA Survival Guide

3Lions Publishing, Inc.

Table of Contents

Introduction

What is Expresso? Expresso is a software-as-a-service ("SaaS") that embodies the National Institute of Standards and Technology (NIST) seven (7) step process for performing Risk Assessments. Expresso builds on the NIST foundation to facilitate performing Risk Assessments by rationalizing the NIST methodology in a manner that makes it accessible to lay persons. What QuickBooks Online ("QBO") did for accounting Expresso does for Risk Assessments. QBO did not eliminate all the work associated with accounting, but transformed accounting from a necessary evil, something to be avoided at all costs and/or handed over to a third party, to something that a business person could master at some basic to intermediate level.

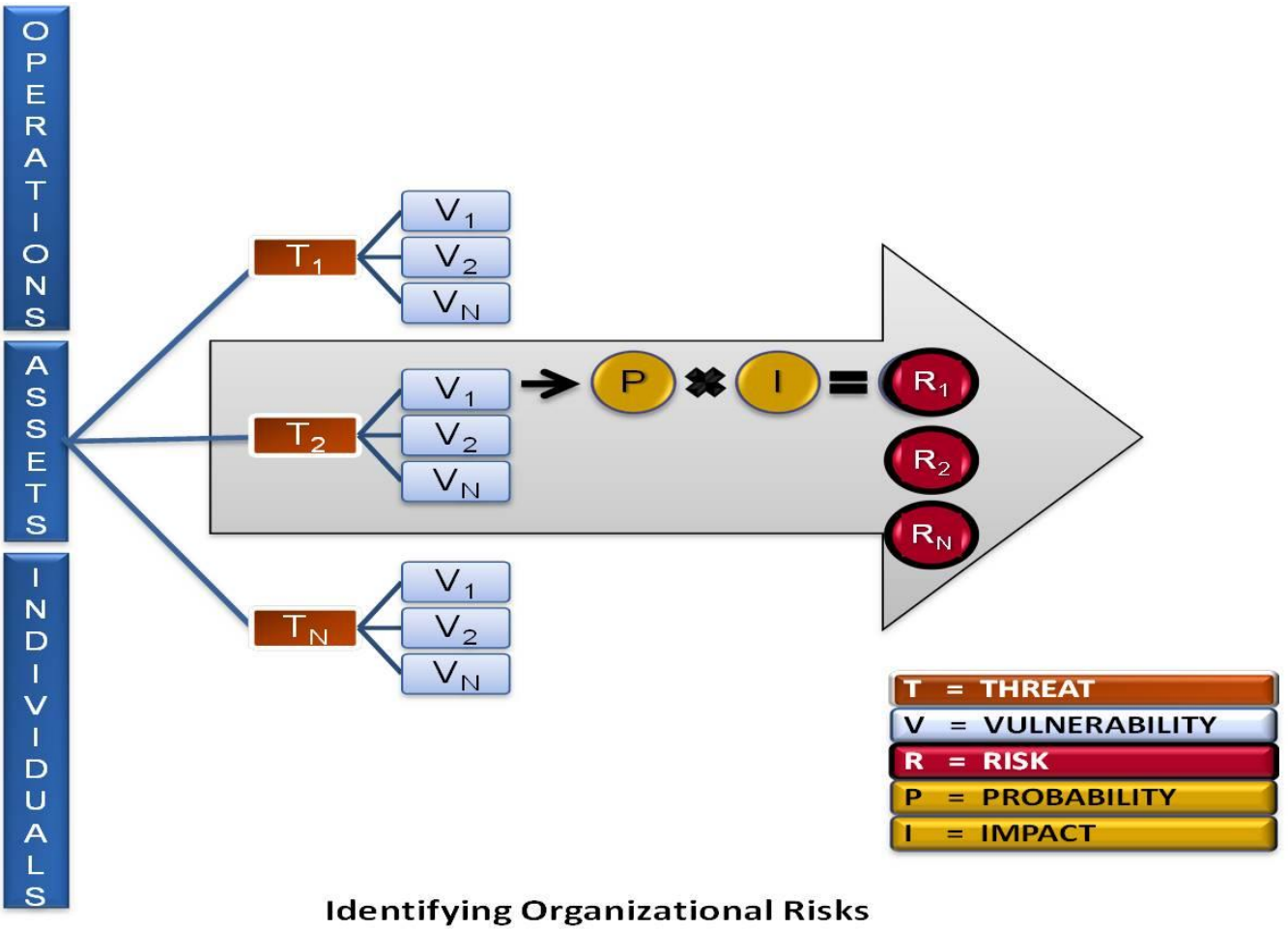


Expresso comes pre-populated with (T)hreats, (V)ulnerabilities, and potential business (I)mpacts to your organization—making the calculation of (R)isks easier than the tedious process that our competitors offer. In addition to pre-populating Threats, Vulnerabilities and Impacts, Expresso comes pre-populated with Controls the cover all Security Rule implementation specifications. Expresso also allows you to modify all pre-populated data in a manner that best fits your organization. The following list summarizes Expresso's principal features. Expresso:

- allows you to bulk import Security Objects (people, places, assets, processes and other things that Security Controls are applied to);
- comes pre-populated with known threats and vulnerabilities to allow for easier pairing of the two;

- allows Security Objects to be categorized via a user defined taxonomy so that Controls can be applied at various levels of classification;
- allows you to retain instances of past Risk Assessments for reporting purposes;
- allows for tracking the results of the Controls applied in the remediation step; and
- is based on an authoritative methodology (e.g. NIST SP 800-30) so as to meet regulatory compliance objectives.

Expresso "productizes" the equation and the process that emerges from the NIST methodology as depicted in the graphic below. It is sold as part of the HIPAA Survival Guide's Subscription Plan.



Identifying Organizational Risks

Benefits

1. Pre-populated (T)hreats, (V)ulnerabilities, (I)mpacts, (R)isks, and (C)ontrols ("TVRCs"): that allows you to perform a Risk Assessment in hours, instead of weeks or months;
2. The ability to capture an unlimited number of Risk Assessments over time in order to show visible, demonstrable evidence of past compliance;
3. The ability to import Security Objects (e.g. people, processes, PCs, servers, networks, applications, databases, physical plant, etc.) from your existing systems thereby minimizing the amount of data entry required;
4. Tracking mechanism(s) for capturing Risk Assessment process results in the form of predefined reports: the measurement;

5. The ability to import (T)hreats and (V)ulnerabilities from authenticated sources: leveraging industry data where available;
6. The ability to directly link to the full source code of Security Rule Controls on the HIPAA Survival Guide website;
7. Scalability, reliability, and availability built-in out-of-the-box using Microsoft's cloud platform Azure; and
8. Much, much more, including a UI that was built for ease of use and clarity that increases your Risk Assessment productivity on day one.

Approach & Methodology

Expresso adopts an agile compliance methodology that allows a customer to eat the Risk Assessment elephant one bite at a time. There is no regulatory requirement that dictates the comprehensiveness of a Risk Assessment each time one is required. In fact, NIST has the following to say pursuant to this topic:

> There are no specific requirements with regard to: (i) the formality, rigor, or level of detail that characterizes any particular risk assessment; (ii) the methodologies, tools, and techniques used to conduct such risk assessments; or (iii) the format and content of assessment results and any associated reporting mechanisms. Organizations have maximum flexibility on how risk assessments are conducted and are encouraged to apply the guidance in this document so that the various needs of organizations can be addressed and the risk assessment activities can be integrated into broader organizational risk management processes.[1]

Therefore, the most important thing you can do with Expresso is to get started—which means as a practical matter, that you likely won't have all your Security Objects loaded nor every potential threat/vulnerability pair identified. The requirement is that you make a "good faith" effort to perform a Risk Assessment and that you continue to improve on the rigor and quality of your assessments going forward.

Build a Risk Assessment Presence

It's critical that all stakeholders, from the C-Suite to the most recent addition to your Workforce, recognize the importance of performing regular assessments. The threat landscape is changing much too quickly for Risk Assessments to be seen as merely an Information Technology issue. In fact, the consensus is that such a narrow view of Risk Assessments is likely to fail.

Analyze Results

You can't manage what you don't measure—at least not in a competent and professional manner. A Risk Assessment is an analysis step where you identify Security Controls to be implemented in order to reduce Risks levels to those that are "reasonable and appropriate" for an organization of your size, complexity, etc. It stands to reason that once you have identified the required Controls you must implement them as part of your Risk

[1] *See* NIST SP 800-30 Rev. 1 p. 9.

Management program and subsequently track their effectiveness. Expresso allows you to update the status of a Risk once the implemented Controls have yielded results.

Summary

To summarize, Expresso dramatically reduces the pain associated with performing Risk Assessments and provides the internal and external reports necessary to show visible demonstrable evidence of both regulatory compliance and a commitment to protecting unauthorized access to your information.