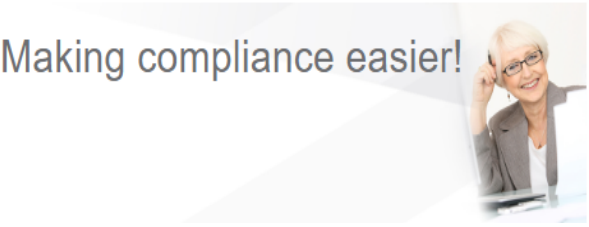
HIPAA Survival Guide



EXPRESSO®
The Risk Assessment Express

HSG Subscription Plan
Expresso®
Datasheet

Table of Contents

Introduction

Expresso® is the HIPAA Survival Guide's All-In-One HIPAA (and other compliance regimes) Risk Assessment Software enables organizations to easily perform risk assessments and prepare risk mitigation processes without the need for expensive consultants. Expresso is pre-populated with (T)hreats, (V)ulnerabilities (T/V pairs), and potential business (I)mpacts to an organization making the calculation of (R)isks easier than the tedious process competitors offer. Expresso® provides the ability to ***create a Risk Assessment in hours not days***. In addition to Threats, Vulnerabilities and Impacts, Expresso® comes pre-populated with Controls that cover **all** Security Rule implementation specifications. It also enables the ability to document notes for a Risk or Security Asset.

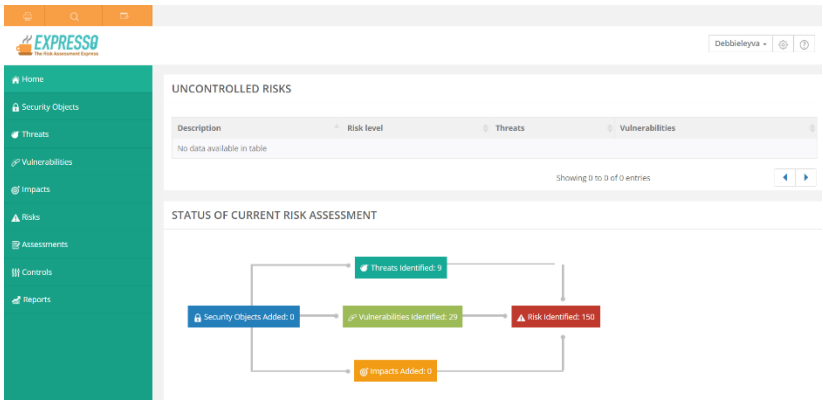


Figure 1 Expresso® Home

Expresso® rationalizes the National Institute of Standards and Technology (NIST) methodology[1] in a manner that makes it accessible to lay persons. Expresso® also provides a level of mastery over Risk Assessments as you conduct more of them over time. The ability to create policies, procedures, and tracking mechanisms for Risk Assessments, using model remediation documentation, provides Visible Demonstrable Evidence (VDE) of Risk Mitigation compliance, which may ***avoid implications of Willful Neglect***, should an audit, breach, or lawsuit trigger an investigation of your HIPAA compliance initiative.

The NIST methodology enables Expresso® to be used across multiple compliance regimes. Currently, Expresso® supports HIPAA and the EU's GDPR.

[1] *See* NIST SP800-30 Rev. 1

Major Features

The following summarizes Expresso®'s principal features:

- Enables multiple Risk Assessments over time;
- Permits copying Risk Assessments from year-to-year, from quarter-to-quarter, or as often as the user requires;
- Comes pre-populated with known Threats and Vulnerabilities for easier pairing of the two—the user can also add their own Risks as the threat landscape changes over time;
- Provides the ability to bulk import Security Objects (people, places, assets, processes and other things to which Security Controls are applied);
- Categorizes Security Objects with a user-defined taxonomy so that identification and Controls can be applied at various levels of classification;
- Contains a Compliance Repository where a user can maintain a *single version of the truth* (i.e. all the organization's ***visible, demonstrable, evidence of compliance***).
- Model Mitigation documentation enables tracking results of Controls applied in the remediation step; and
- Expresso® is based on an authoritative methodology (e.g. NIST SP 800-30 Rev. 1) to meet or exceed regulatory compliance objectives; and
- Provides comprehensive reporting to view reports online, print to PDF or export to CSV/Excel.

Risk Assessments

The NIST Risk Assessment methodology embodies an Agile life cycle approach and reminds its audiences that there is no need to attempt the impossible (i.e. there are no perfect Risk Assessments). Quite the contrary, the NIST methodology acknowledges that "risk assessments are often not precise instruments of measurement" and therefore our admonishment that the most important thing you can do is "get started"; because Risk Assessments are something that your Organization will improve upon over time (i.e. as you recursively weave Risk Assessments into your organizational DNA to attack this "wicked problem").

HIPAA

Expresso® 2.0 comes out-of-the-box ready to be used for HIPAA Risk Assessments. We have pre-loaded Threats, Vulnerabilities and the resulting Risks which cover all Security Rule implementation specifications ("Controls"). Your job is to assign a subjective value of High, Medium, or Low to each Risk and assess the Impact to your organization if a specific Threat exploits its respective Vulnerability. Once you have identified a sub-set of High Risks, you should begin remediating and

implementing Controls. Our Subscription Plan offerings assist you in the remediation process by providing training, checklists, frameworks, tools, model templates and more (i.e. out-of-the-box Controls). When you purchase the Subscription Plan, we guide you through your first Risk Assessment with Expresso® and we support your efforts with live support.

GDPR

If you purchase our Subscription Plan for HIPAA, you can add a "GDPR Module" that will allow you to perform a Data Protection Impact Assessment for the EU's GDPR. Because the NIST methodology is compliance regime agnostic, Expresso® can support any compliance regime with the appropriate "load file."

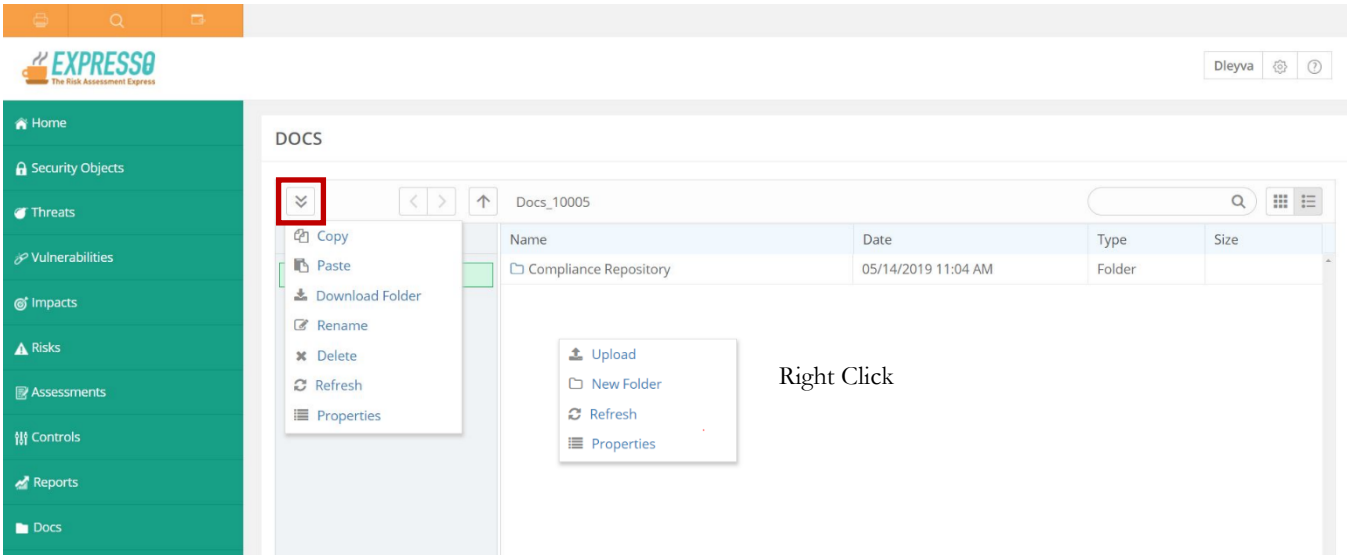
Other Compliance Regimes

As discussed above, future use of Expresso® may support additional compliance regimes as market demands warrant (e.g. PCIDSS, SOX, etc.).

Compliance Repository ("Docs")

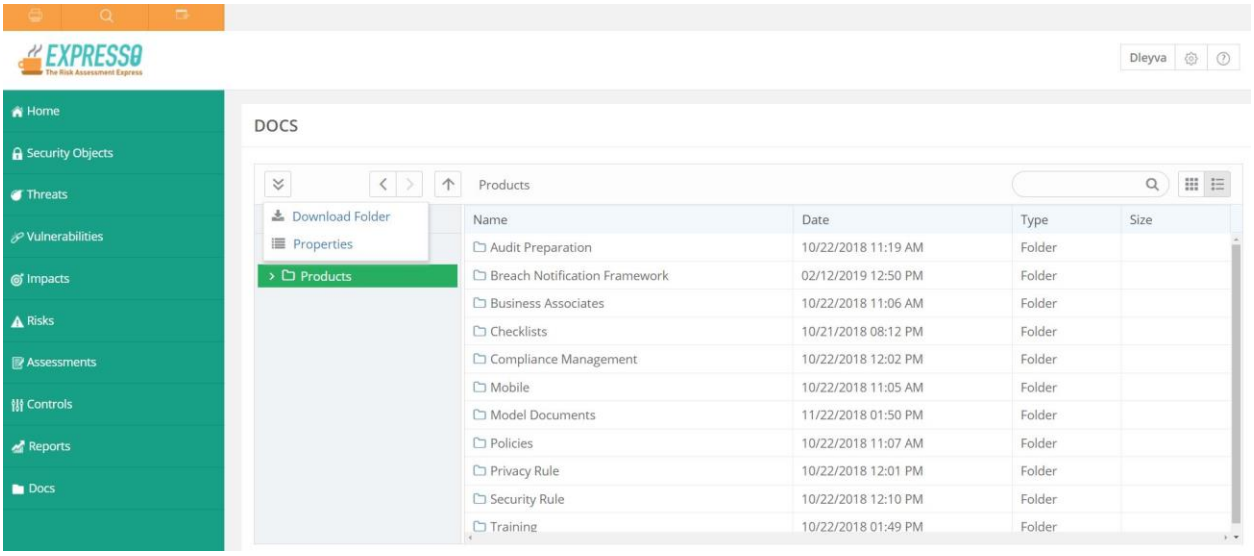
Expresso® now includes Docs, a Compliance Repository ("Repository") where a single version of the truth can be stored and enables online access to the HIPAA Survival Guide's products (see below). Documents representing your visible, demonstrable, evidence of compliance can be uploaded from your network after they have been vetted by your staff. Documents may also be dragged and dropped from one Compliance Repository folder to another. Just click on the file and drag it to the desired location. With all your visible, demonstrable, evidence in one place you will always be ready when an auditor comes calling.

Repository Menus are shown below.



Facilitated Product Access

Expresso® includes facilitated access to all our Products making it easier to find the Product you need when you need it. Get quick access to 50+ training modules, model documents (e.g. policies and contracts), checklists, frameworks and tools.



Summary

The HIPPA Survival Guide with Expresso® has what you need to maintain your HIPAA Compliance.