IRM | Pro

Safeguard Information

Exclusive Endorsement

CLEARWATER COMPLIANCE

Focused on assisting customers to implement their HIPAA Privacy, Security, and cybersecurity programs

Jon Stone, MPA, CRISC, HCISPP, PMP

- +30 years in Healthcare
- +25 years of product/software development and strategic leadership for security and compliance for companies such as CIGNA, Healthways and Optum

Jon Stone, MPA, CRISC, HCISPP, PMP
Vice President of Product Innovation
Jon.Stone@ClearwaterCompliance.com
615-210-9612

Clearwater has worked with nearly 500 C[illegible]

SENTARA®

Anchorage Community Mental Health Services, Inc.

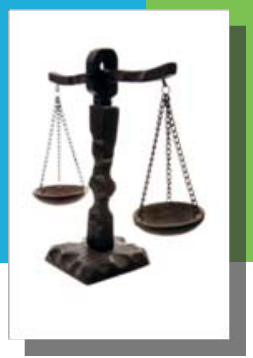
"Clearwater will be instrumental in helping us avoid future fines by remaining compliant with privacy and HIPAA regulations. Clearwater's software is also providing us with a framework for managing our risk across other business lines like administration, safety and compliance – even finance!"

Jon Watkins
CFO
Anchorage

What do the HIPAA regulations require?

45 C.F.R. §164.308(a)(8)

Evaluation … Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule…



45 C.F.R. §164.308(a)(1)(i) Standard: Security Management Process

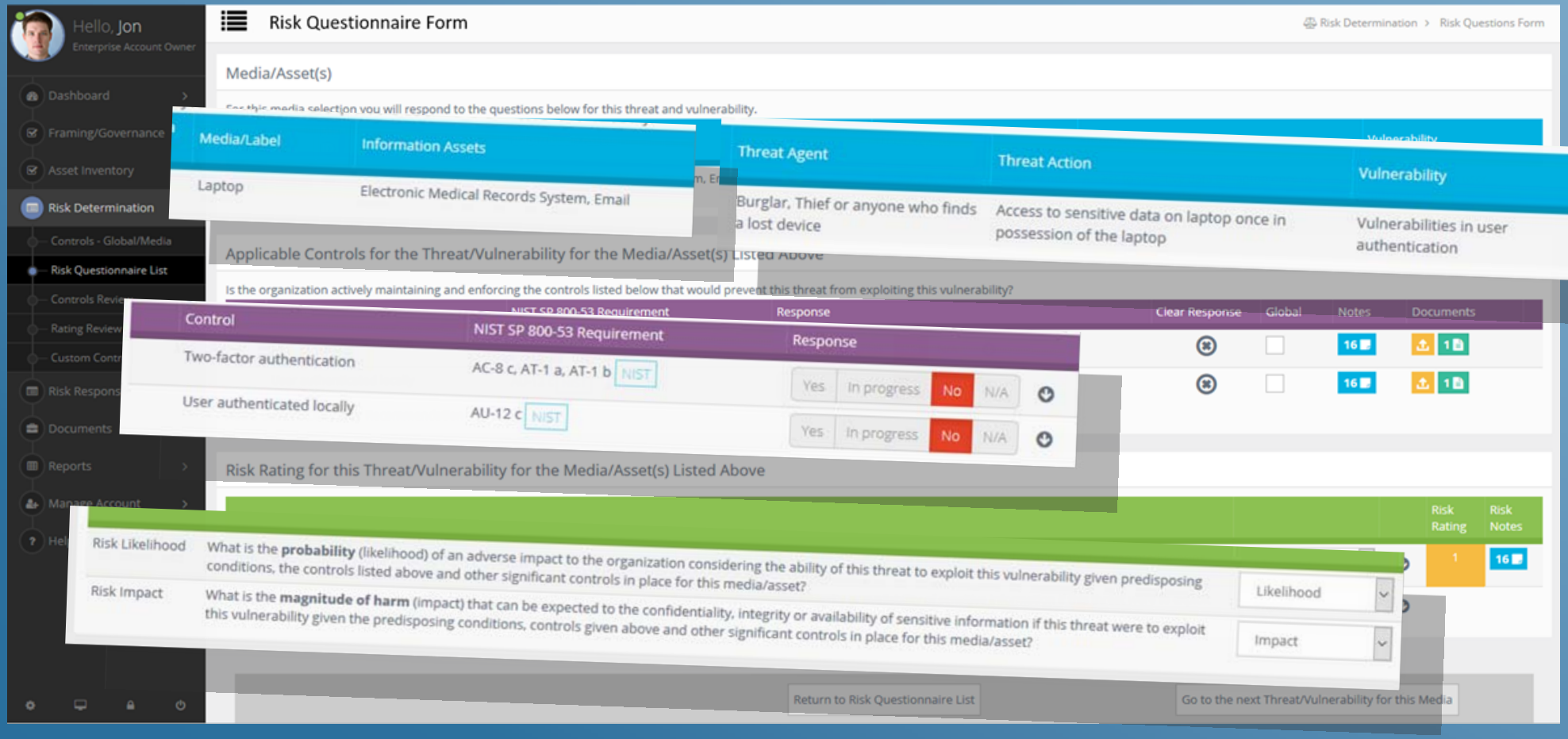
(A) Risk analysis … assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

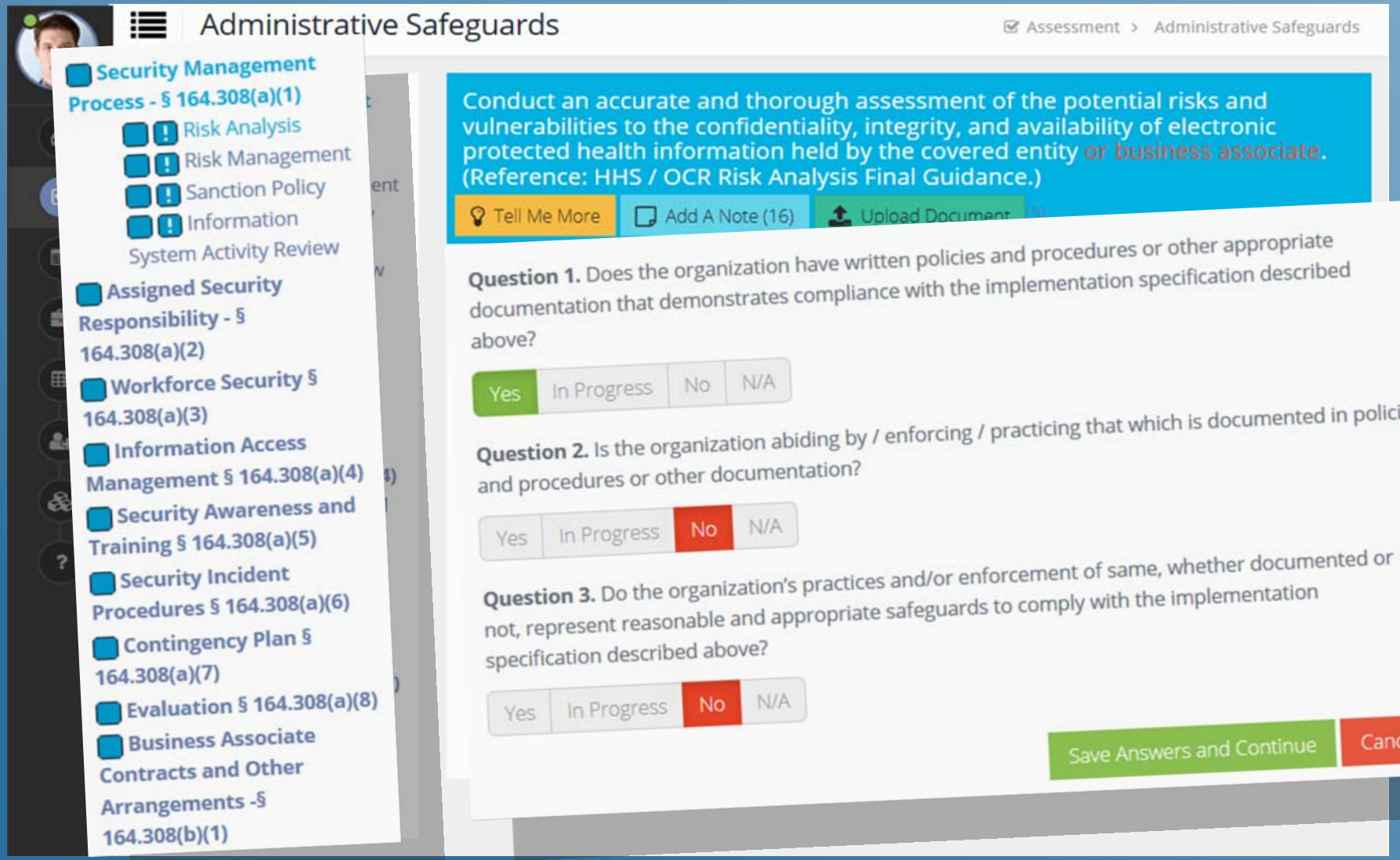
- Compliance Gap Assessment
- Documentation
- HHS OCR Guidance Letter
- NIST Standards


IRM
Pro
Safeguard Information

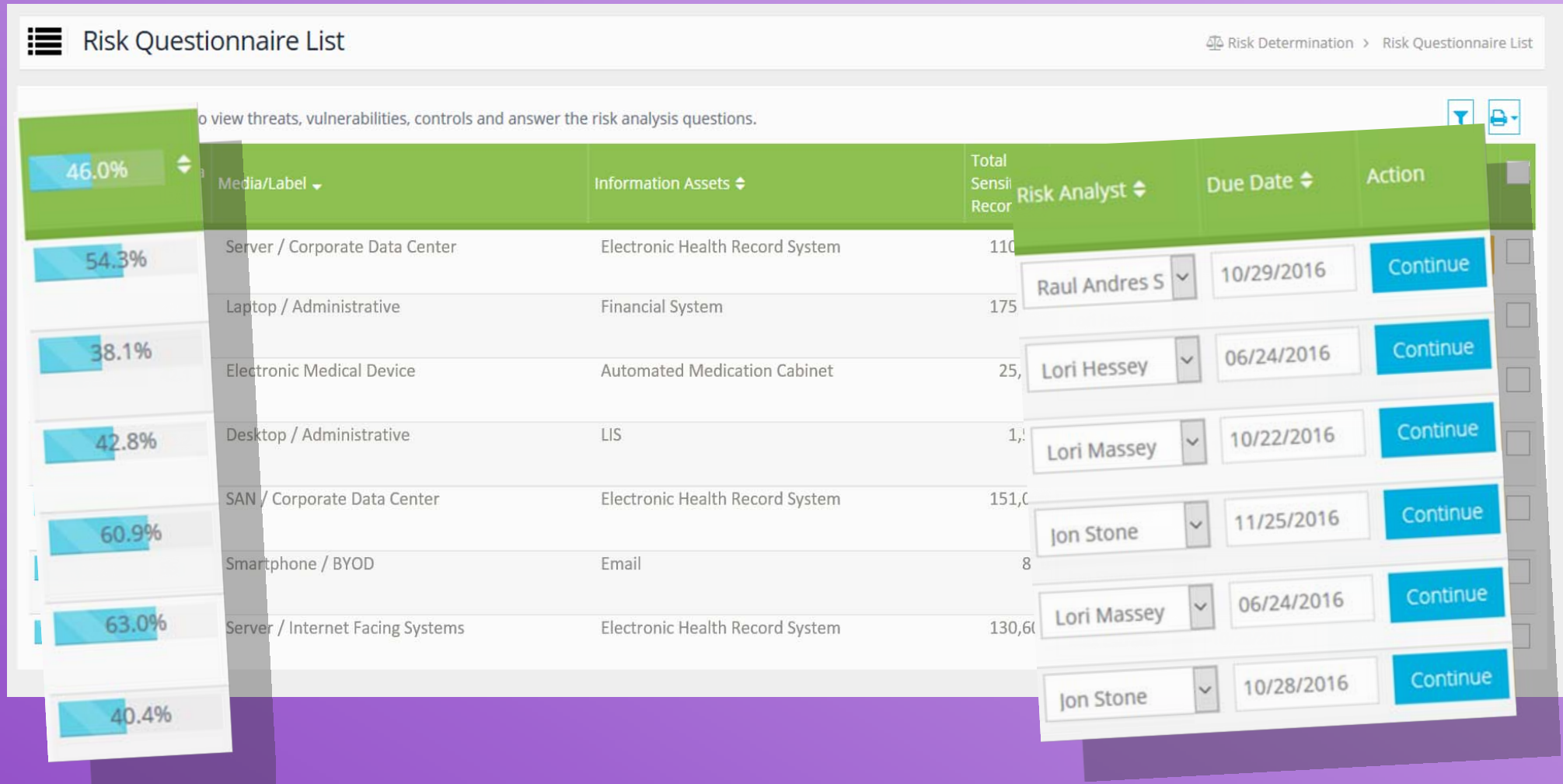
Start Fast - Easy Implementation

Remove Guesswork - Expert System


Hello, Jon
Enterprise Account Owner
Dashboard
Framing/Governance
Asset Inventory
Risk Determination
Controls - Global/Media
Risk Questionnaire List
Controls Revie
Rating Review
Custom Contr
Risk Respons
Documents
Reports
Manage Account
Risk Questionnaire Form
Risk Determination > Risk Questions Form
Media/Asset(s)
Media/Label
Information Assets
Laptop
Electronic Medical Records System, Email
Threat Agent
Threat Action
Vulnerability
Burglar, Thief or anyone who finds a lost device
Access to sensitive data on laptop once in possession of the laptop
Vulnerabilities in user authentication
Applicable Controls for the Threat/Vulnerability for the Media/Asset(s) Listed Above
Is the organization actively maintaining and enforcing the controls listed below that would prevent this threat from exploiting this vulnerability?
Control
NIST SP 800-53 Requirement
Response
Clear Response
Global
Notes
Documents
Two-factor authentication
AC-8 c, AT-1 a, AT-1 b NIST
Yes
In progress
No
N/A
User authenticated locally
AU-12 c NIST
Risk Rating for this Threat/Vulnerability for the Media/Asset(s) Listed Above
Risk Rating
Risk Notes
Risk Likelihood
What is the probability (likelihood) of an adverse impact to the organization considering the ability of this threat to exploit this vulnerability given predisposing conditions, the controls listed above and other significant controls in place for this media/asset?
Likelihood
Risk Impact
What is the magnitude of harm (impact) that can be expected to the confidentiality, integrity or availability of sensitive information if this threat were to exploit this vulnerability given the predisposing conditions, controls given above and other significant controls in place for this media/asset?
Impact
Return to Risk Questionnaire List
Go to the next Threat/Vulnerability for this Media


Administrative Safeguards
Assessment > Administrative Safeguards
Security Management Process - § 164.308(a)(1)
Risk Analysis
Risk Management
Sanction Policy
Information System Activity Review
Assigned Security Responsibility - § 164.308(a)(2)
Workforce Security § 164.308(a)(3)
Information Access Management § 164.308(a)(4)
Security Awareness and Training § 164.308(a)(5)
Security Incident Procedures § 164.308(a)(6)
Contingency Plan § 164.308(a)(7)
Evaluation § 164.308(a)(8)
Business Associate Contracts and Other Arrangements -§ 164.308(b)(1)
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. (Reference: HHS / OCR Risk Analysis Final Guidance.)
Tell Me More
Add A Note (16)
Upload Document
Question 1. Does the organization have written policies and procedures or other appropriate documentation that demonstrates compliance with the implementation specification described above?
Yes
In Progress
No
N/A
Question 2. Is the organization abiding by / enforcing / practicing that which is documented in policies and procedures or other documentation?
Yes
In Progress
No
N/A
Question 3. Do the organization's practices and/or enforcement of same, whether documented or not, represent reasonable and appropriate safeguards to comply with the implementation specification described above?
Yes
In Progress
No
N/A
Save Answers and Continue
Cancel

Less Effort – Workflows and Automation

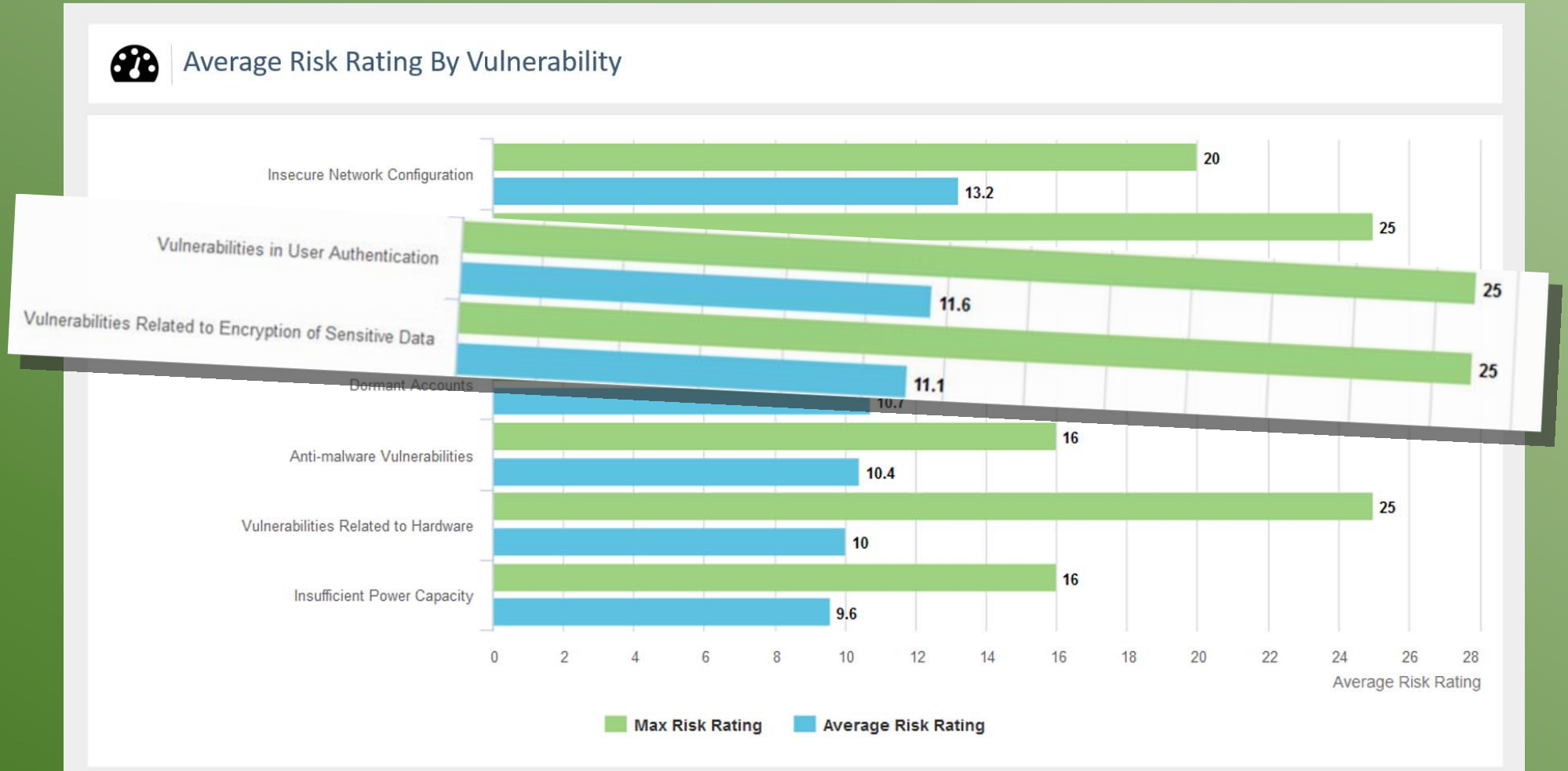

Risk Questionnaire List
Risk Determination › Risk Questionnaire List
o view threats, vulnerabilities, controls and answer the risk analysis questions.
46.0%
54.3%
38.1%
42.8%
60.9%
63.0%
40.4%
Media/Label
Information Assets
Total Sensi Recor
Server / Corporate Data Center
Electronic Health Record System
Laptop / Administrative
Financial System
Electronic Medical Device
Automated Medication Cabinet
Desktop / Administrative
LIS
SAN / Corporate Data Center
Electronic Health Record System
Smartphone / BYOD
Email
Server / Internet Facing Systems
Electronic Health Record System
Risk Analyst
Due Date
Action
Raul Andres S
10/29/2016
Continue
Lori Hessey
06/24/2016
Continue
Lori Massey
10/22/2016
Continue
Jon Stone
11/25/2016
Continue
Lori Massey
06/24/2016
Continue
Jon Stone
10/28/2016
Continue

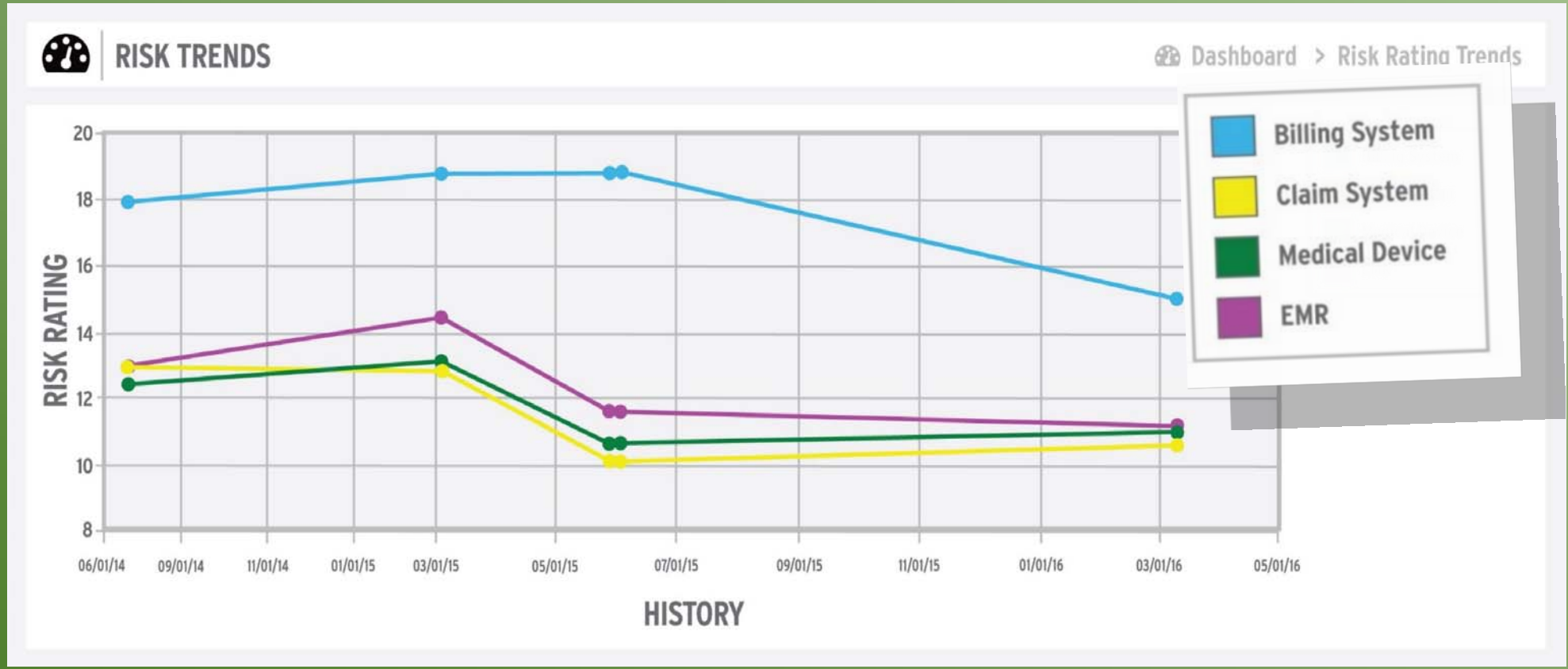
Understand Exposures
Extensive Dashboards and Reports

Risk Rating Report

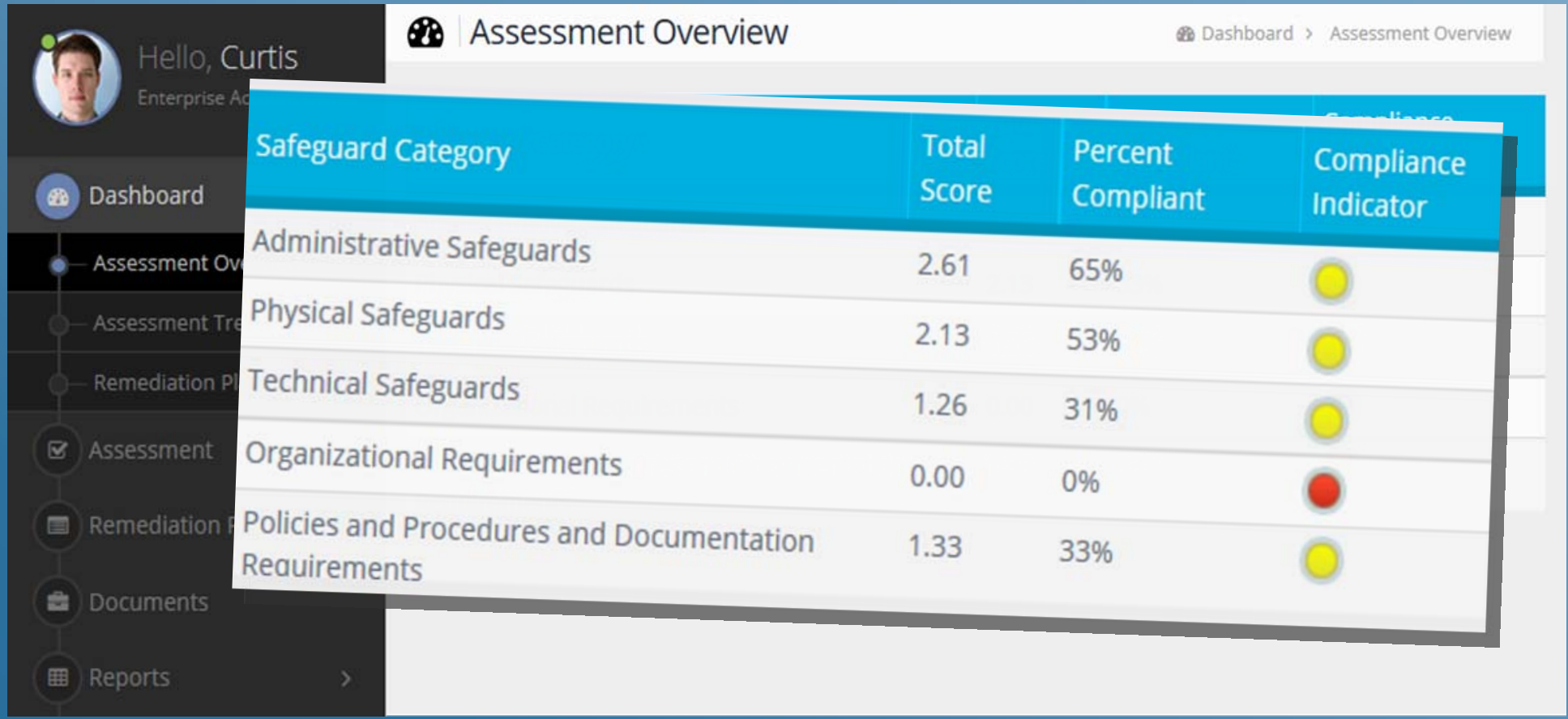
Media And Storage Devices/Label	Asset Name(s)	Threat Agent	Threat Action	Vulnerability
Laptop / Administrative	Financial System	Burglar, Thief or Anyone Who Finds a Lost Device	Access to Sensitive Data Once in Possession of the Device	Vulnerabilities to Encryption Sensitive Data
Electronic Medical Device	Automated Medication Cabinet	Careless IT Personnel	Insecure User Management	Vulnerabilities Password Crea Distribution
Desktop / Administrative	LIS	System Cracker	Theft of Sensitive Data	Anti-malware Vulnerabilities
Server / Corporate Data Center	Electronic Health Record System	Careless User	Weak Passwords	Weak Password
Smartphone / BYOD	Email	Burglar, Thief or Anyone Who Finds a Lost Device	Access to Sensitive Data Once in Possession of the Device	Vulnerabilities i Authentication
Server / Internet Facing Systems	Electronic Health Record System	Malware	Theft of Sensitive Data	Anti-malware Vulnerabilities

Risk Likelihood	Risk Impact	Risk Rating	Risk Rating
5	5	25	Critical
4	3	12	Medium
4	4	16	High
4	2	8	Medium
4	5	20	High
5	5	25	Critical

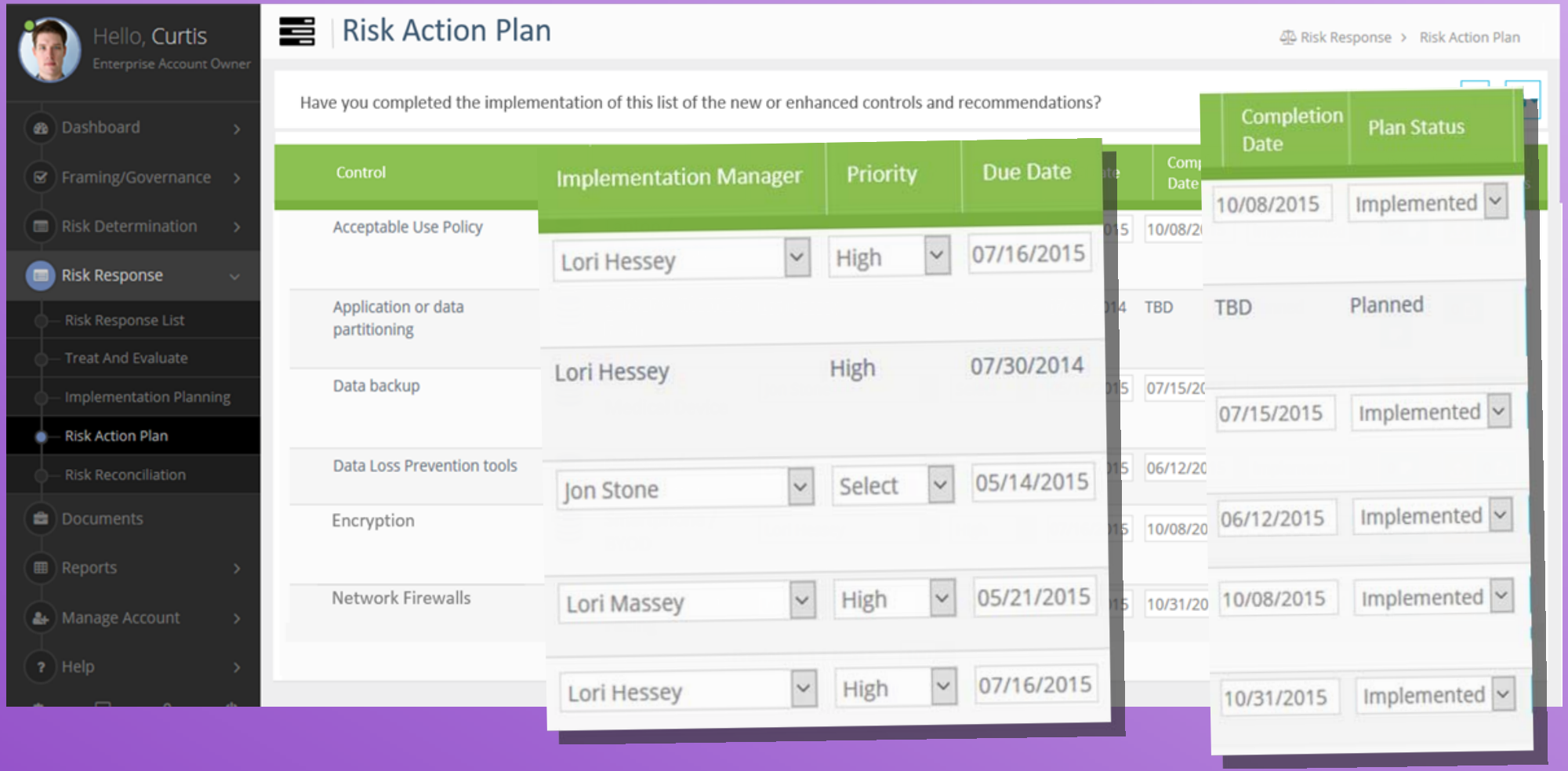

Average Risk Rating By Vulnerability
Insecure Network Configuration
20
13.2
Vulnerabilities in User Authentication
25
11.6
Vulnerabilities Related to Encryption of Sensitive Data
25
11.1
Dormant Accounts
10.7
Anti-malware Vulnerabilities
16
10.4
Vulnerabilities Related to Hardware
25
10
Insufficient Power Capacity
16
9.6
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28
Average Risk Rating
Max Risk Rating
Average Risk Rating


RISK TRENDS
Dashboard > Risk Rating Trends
RISK RATING
20
18
16
14
12
10
8
06/01/14
09/01/14
11/01/14
01/01/15
03/01/15
05/01/15
07/01/15
09/01/15
11/01/15
01/01/16
03/01/16
05/01/16
HISTORY
Billing System
Claim System
Medical Device
EMR

Be Confident
By the Book Approach


Hello, Curtis
Dashboard
Assessment Ov
Assessment Tre
Remediation Pl
Assessment
Remediation P
Documents
Reports
Assessment Overview
Dashboard › Assessment Overview
Safeguard Category
Total Score
Percent Compliant
Compliance Indicator
Administrative Safeguards
2.61
65%
Physical Safeguards
2.13
53%
Technical Safeguards
1.26
31%
Organizational Requirements
0.00
0%
Policies and Procedures and Documentation Requirements
1.33
33%

Reduce Cybersecurity Risk - Protect ePHI


Hello, Curtis
Enterprise Account Owner
Dashboard
Framing/Governance
Risk Determination
Risk Response
Risk Response List
Treat And Evaluate
Implementation Planning
Risk Action Plan
Risk Reconciliation
Documents
Reports
Manage Account
Help
Risk Action Plan
Risk Response > Risk Action Plan
Have you completed the implementation of this list of the new or enhanced controls and recommendations?
Control
Implementation Manager
Priority
Due Date
Completion Date
Plan Status
Acceptable Use Policy
Lori Hessey
High
07/16/2015
10/08/2015
Implemented
Application or data partitioning
TBD
Planned
Data backup
Lori Hessey
High
07/30/2014
07/15/2015
Implemented
Data Loss Prevention tools
Jon Stone
Select
05/14/2015
06/12/2015
Implemented
Encryption
Network Firewalls
Lori Massey
High
05/21/2015
10/08/2015
Implemented
Lori Hessey
High
07/16/2015
10/31/2015
Implemented

Start Fast - Easy Implementation

Less Effort – Workflows and Automation

Remove Guesswork - Expert System

Understand Exposures – Extensive Dashboards and Reports

Be Confident – By the Book

Reduce Cybersecurity Risk - Protect ePHI

IRM | Pro

Safeguard Information

http://www.ClearwaterCompliance.com
Phone: 800-704-3394

CLEARWATER COMPLIANCE

Copyright Notice

Copyright Notice. All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

For reprint permission and information, please direct your inquiry to info@clearwatercompliance.com

Legal Disclaimer

Legal Disclaimer. This information does not constitute legal advice and is for educational purposes only. This information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Since this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource regarding the matters covered, and may not be tailored to your specific circumstance. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND ADVICE PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE. The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.