A Sensible Approach to HIPAA Security

Steve Taylor
IT Director, Valley Mental Health

The Halo Group

Larry C. Eighmy, CISSP, CISM, PMP
President, The Halo Group, Inc.

Susan A. Miller, JD
HIPAA Health Care

Agenda

1. **Introduction** – Susan Miller

2. **Challenge** – Steve Taylor

3. **Approach** – Susan Miller

4. **Assessment** – Larry Eighmy

5. **Questions**

1. Introduction – Susan Miller

2. Challenge – Steve Taylor

3. Approach – Susan Miller

4. Assessment – Larry Eighmy

5. Questions

Valley Mental Health

2008 provided Mental Health and Substance Abuse services to 18,278 consumers in 3 counties

- 65% adult consumers
  - 18 adult treatment programs
  - 10 housing/residential programs
- 26% child/youth consumers
  - 28 child/youth treatment programs
  - 9 residential programs
- 9% served by Medicaid subcontractors

Adult Programs

- Outpatient (7)
  - All serve dual diagnosed, substance abuse and mental health
  - 4 Specialize in Outpatient Substance Abuse
- Partial Day Treatment/Club House (4)
- Forensic (2)
- Specialized Assessment
  - PASRR
- Utilization Review
  - PEHP
  - CVR
- Homeless Outpatient
- Community Computer Education (multiple sites)
- Residential (13)
  - Independent Living (6)
  - Residential Support (5)
  - Residential Treatment (2)
    - ➢mental health
    - ➢substance abuse

Child/Youth Programs

- Outpatient (7)
  - Mental Health (3)
  - Substance Abuse (2)
  - Sex Abuse (1)
- Autism Center
- School Based (8)
- After School
- Day Treatment

- Residential (6)
  - Observation and Evaluation (2)
  - Sex Abuse Treatment
  - Substance Abuse (3)
- Therapeutic Foster Homes (25)

RELIEF • RECOVERY
REDISCOVERY
Valley Mental Health

VMH Security

- Privatized in 1987
- Dispersed Network
- Centralized Network
- Small amount of built in security
- HIPAA

Dispersed Network

- Designed a personal computer network
- VMH financially assisted employees buying computers
- Increased access for employees
- Not enough IT personnel to handle problems
- Small amount of built in security
- Threat level for security was small

Centralized Network

- IT able to handle problems without increased staff
- More security inherent with Citrix
- Security threat increased, but network industry as a whole ignored the increase in threats leaving Network Administrators with no way to combat the threat

Small Amount of Built in Security

- VMH decisions actually aided in keeping good security in some places while weakening in others
  - Keeping the Client Database on the AS/400 increased security (AS/400 is hard to compromise by the design of the system)
  - Moving to a Citrix environment increased security
  - VMH Chose to use off brand venders increasing security
  - Threat levels were increasing, however industry still ignored the warnings
  - VMH chose easier access for employees decreasing security

HIPAA…

- Threat levels increased to the point that medical records and personal information was being compromised across the globe
- Industry started to take notice and began to combat attacks
- Government stepped in to attempt to control an out of control situation
- Vague rules were created to try and cover all healthcare businesses regardless of size or budget
- Due diligence became the key words to avoiding
- VMH formed a committee
- VMH named a Privacy Officer
- VMH assigned a security role

Corrective Actions…

- VMH increased the security for external infrastructure

- Added firewalls and DMZ to separate internet access from intranet access

- Continued to use off brands and added multiple routers/firewalls to block internet access into the intranet

- Added encrypted email systems

- Added vulnerability scanners to constantly test servers and routers for areas in need of upgrades or security updates

Corrective Actions (continued) …

- Added intrusion detection systems to alert Administrators of unapproved access into the system
- Added a spam filter system to aid in deterring malware from getting to the employees
- Added a content filter system to keep employees from going to unauthorized or inappropriate websites
- Added a logging system to report unauthorized access of client records
- Submitted 30+ new policies for approval
    - Policies were combined into 2 which though approved never were printed or published

1. Introduction – Susan Miller

2. Challenge – Steve Taylor

3. Approach – Susan Miller

4. Assessment – Larry Eighmy

5. Questions

Goals…

- Reduce Costs
  - Travel (conduct portions of the project remotely)
  - Compressed time line
    - Solid Methodology
    - Automated Tools
    - Experience Staff
- Provide simplified written report with tangible action items.
- Leave behind an easy to use tool to track and report progress after the fact.

Three Tasks…

- On-Site Visits and Interviews
- Project Manager Training
- HIPAA Security Assessment

Why Did This Approach Work?

- Very Strong Senior Management Support
- Excellent Security Staff
- Everyone Primed for On-Site Visit and Phone Interview

Staff Interviewed…

- Privacy Officer
- Comptroller
- Corporate Compliance Officer
- Medical Records
- Human Resources

On-Site Issues and Solutions…

Fourteen (14) Sites Visited

- Locked doors
- Paper + paperless
- Fax machines + mail boxes+ shred boxes + printers
- Courier service
- Releases
- Cleaning staff
- Other

Interviews Discovered…

- HIPAA privacy is ubiquitous at Valley Mental Health
- Staff understands the confidentiality of client medical records
- Staff understands the HIPAA issues at their unit
- Staff wants to fix the HIPAA issues at their unit

Interviews Discovered (continued) . . .

- Good HIPAA privacy and security culture
- But cannot prove it
- Need to
- Complete documentation
- More training
- Contingency plan role playing/training
- Build compliance office

1. Introduction – Susan Miller

2. Challenge – Steve Taylor

3. Approach – Susan Miller

4. **Assessment – Larry Eighmy**

5. Questions

Accelerated Success Criteria…

Our experience has been that the following aspects impact the project schedule the most:

- ✓ Clearly defined and documented Methodology, Roles and Responsibilities
- ✓ Experienced HIPAA Security and Privacy resources
- ✓ Easy to use Collection Tool
- ✓ Completed pre-onsite information package
- ✓ Availability of staff members
- ✓ Availability of application/ePHI inventories
- ✓ Availability of infrastructure topologies
- ✓ Completed department questionnaires
- ✓ Onsite central coordinator
- - No central meeting facility for department interviews
- - Multiple missed or re-scheduled department interviews

Risk / Gap Hybrid Strategy…

Not a full Qualitative Risk Analysis, however, included many risk components that will easily contribute to this effort.

Enablers:

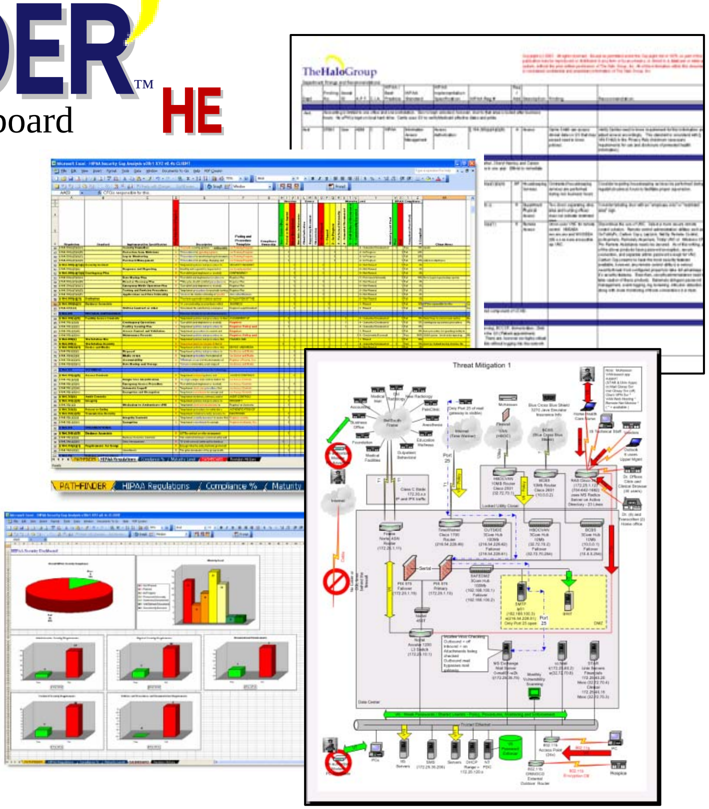
- ✓ Leveraged VMH’s internal security group. They were very knowledgeable, trained and experienced. VMH had many industry standard controls in place that addressed several standards at once.
- ✓ VMH’s Security team could easily articulate their configurations and topologies.
- ✓ VMH’s Security team already completed System Characterization, Threat and Vulnerability Identification, Control Analysis and Impact Ratings.
- ✓ VMH runs periodic vulnerability scans and performs Ethical Hacking (Pen Tests) on systems.
- ✓ Team was very open and eager to participate.
- ✓ Steve provided excellent coordination and sharing between the groups.

Tools…

PATHFINDER™ HE

Security Compliance Dashboard

HIPAA Edition



RISKFINDER™ HE

IT Risk Analysis Tool

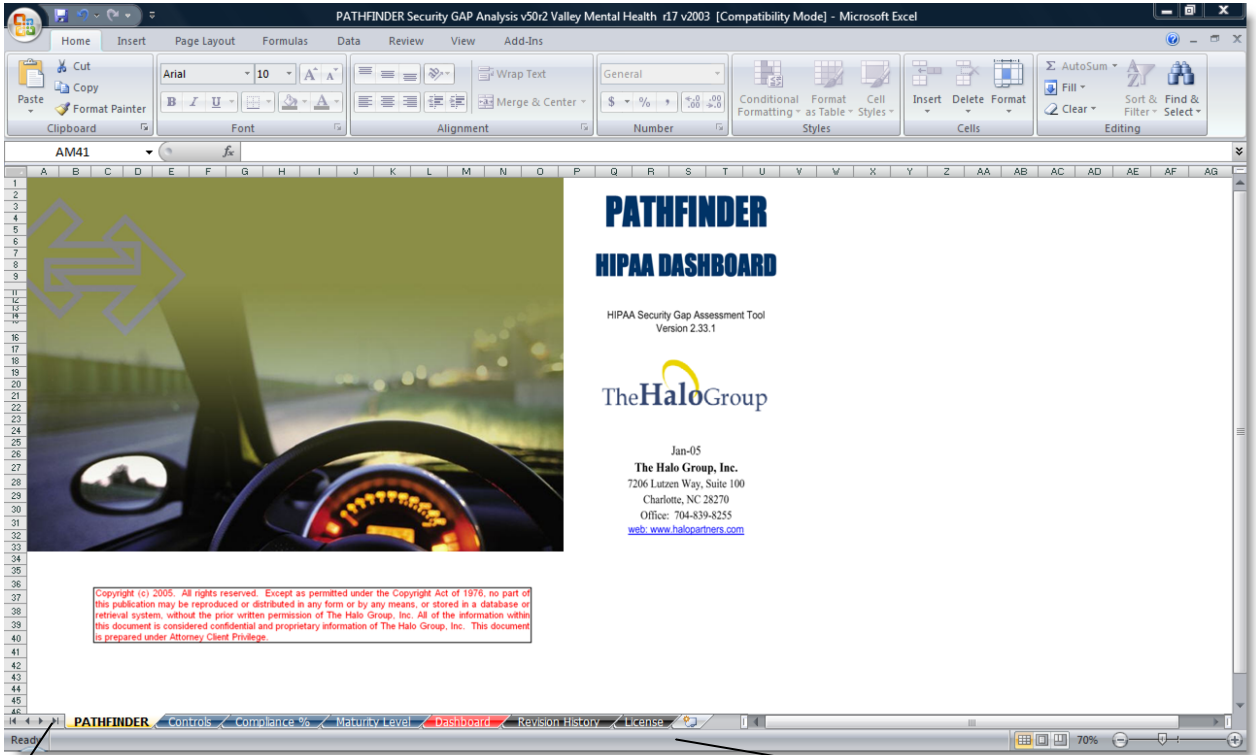
HIPAA Edition

Assessment Tool…

PATHFINDER™ HE

Security Compliance Dashboard

HIPAA Edition



PATHFINDER

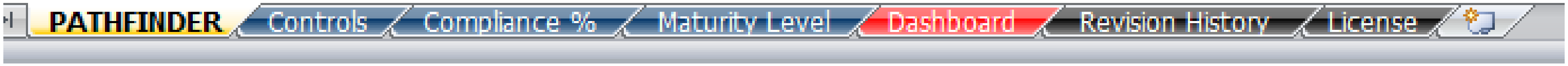
HIPAA DASHBOARD

HIPAA Security Gap Assessment Tool
Version 2.33.1

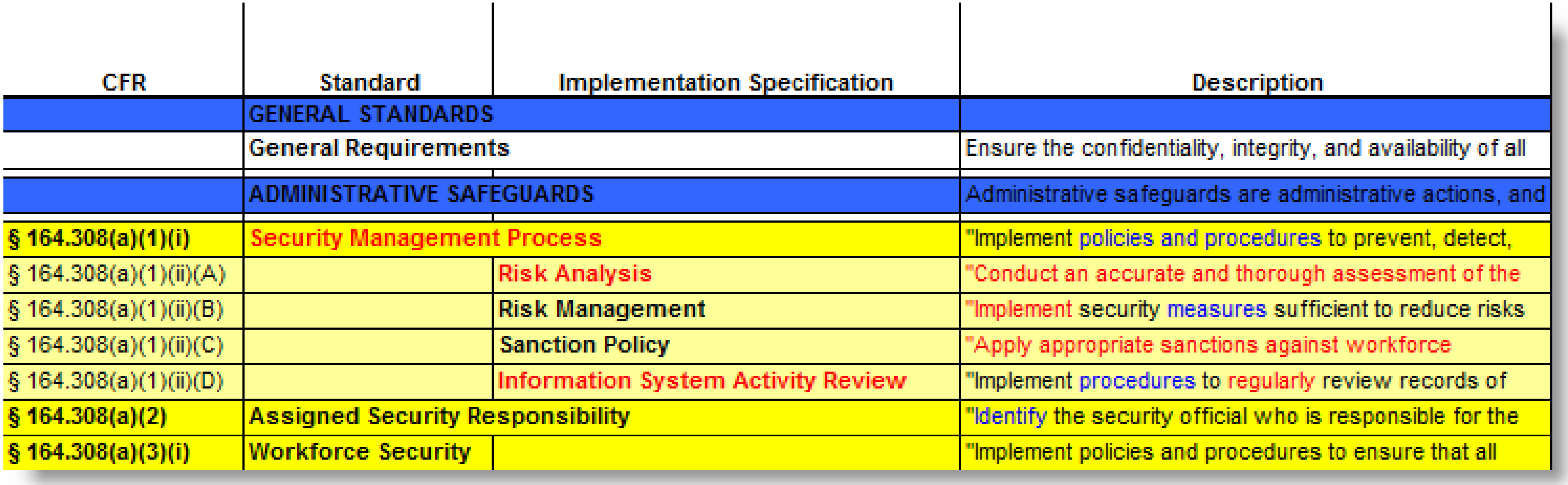
TheHaloGroup

Jan-05
The Halo Group, Inc.
7206 Lutzen Way, Suite 100
Charlotte, NC 28270
Office: 704-839-8255
web: www.halopartners.com

Copyright (c) 2005. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of The Halo Group, Inc. All of the information within this document is considered confidential and proprietary information of The Halo Group, Inc. This document is prepared under Attorney Client Privilege.

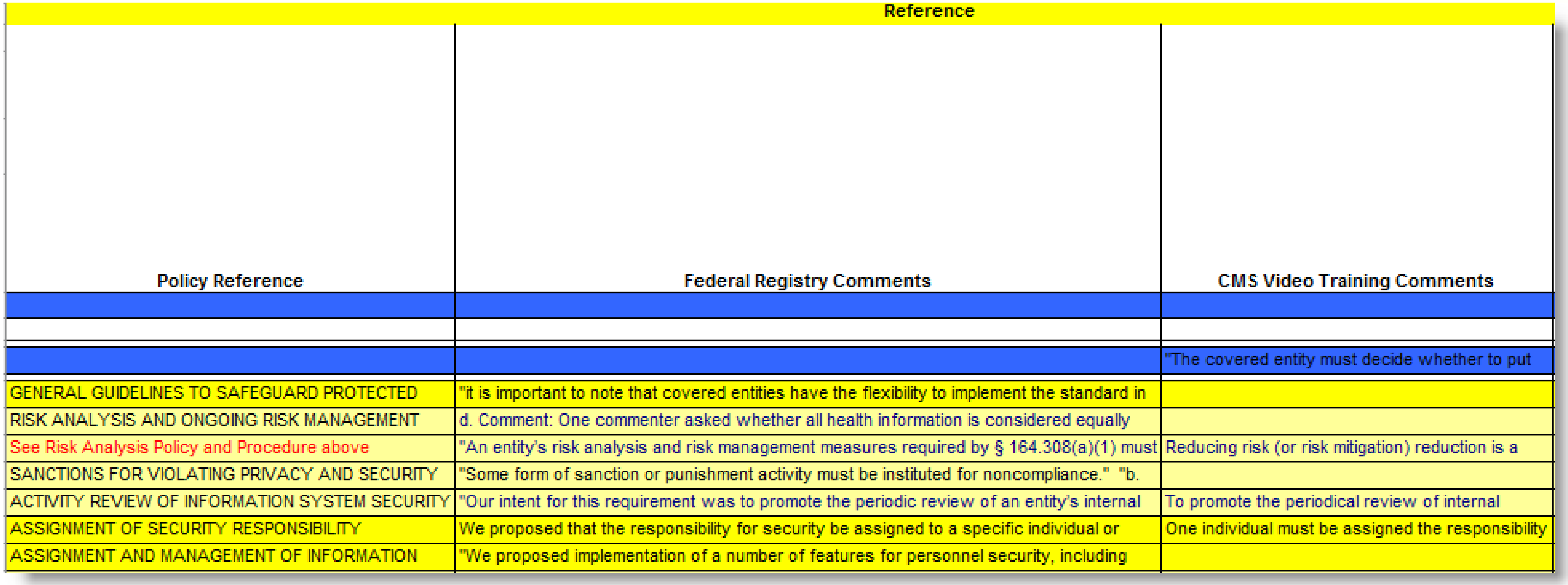


Control Descriptions…

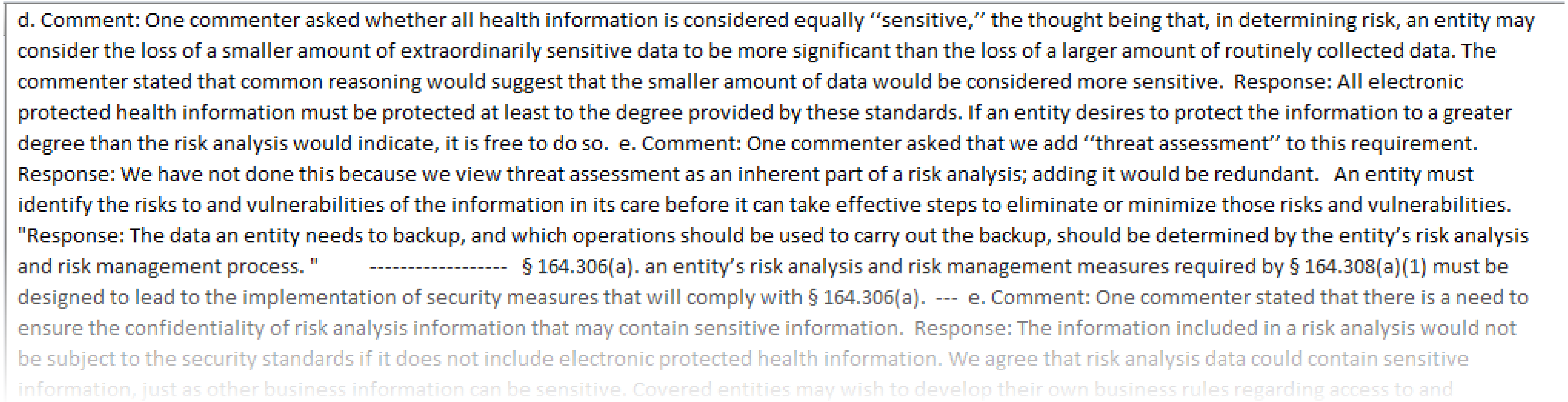


CFR	Standard	Implementation Specification	Description
	GENERAL STANDARDS		
	General Requirements		Ensure the confidentiality, integrity, and availability of all
	ADMINISTRATIVE SAFEGUARDS		Administrative safeguards are administrative actions, and
§ 164.308(a)(1)(i)	Security Management Process		"Implement policies and procedures to prevent, detect,
§ 164.308(a)(1)(ii)(A)		Risk Analysis	"Conduct an accurate and thorough assessment of the
§ 164.308(a)(1)(ii)(B)		Risk Management	"Implement security measures sufficient to reduce risks
§ 164.308(a)(1)(ii)(C)		Sanction Policy	"Apply appropriate sanctions against workforce
§ 164.308(a)(1)(ii)(D)		Information System Activity Review	"Implement procedures to regularly review records of
§ 164.308(a)(2)	Assigned Security Responsibility		"Identify the security official who is responsible for the
§ 164.308(a)(3)(i)	Workforce Security		"Implement policies and procedures to ensure that all

References…

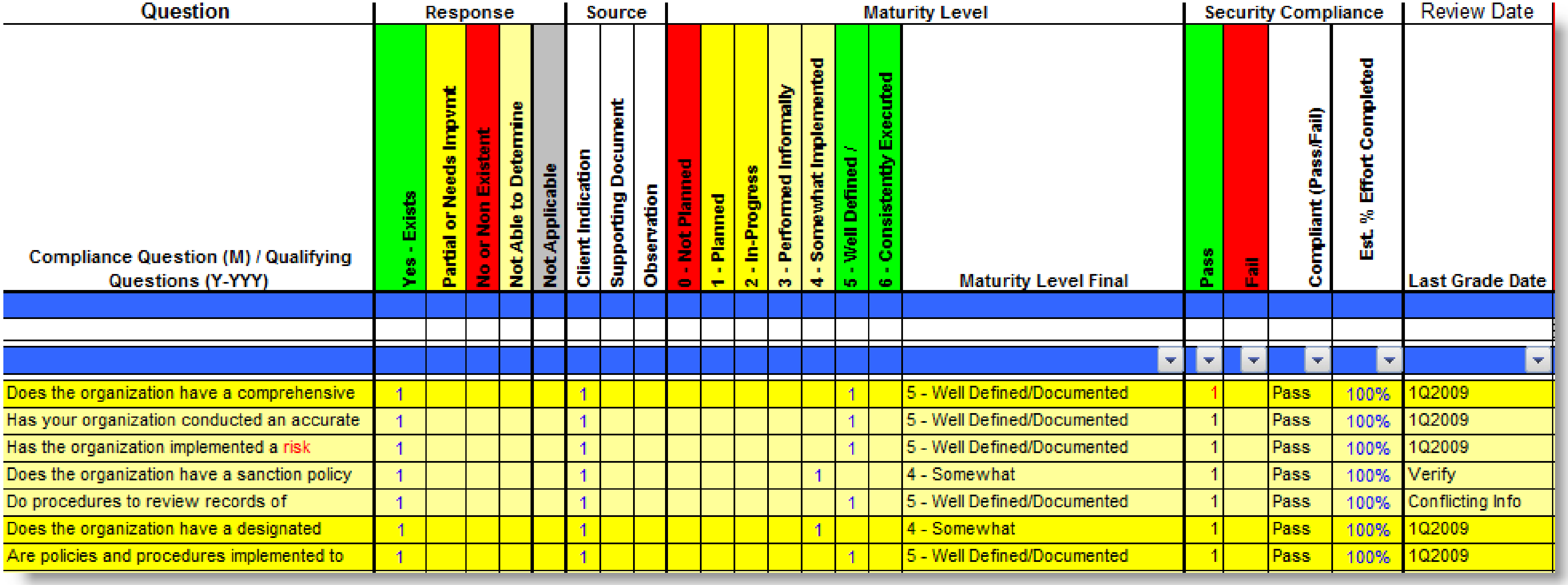


Reference		
Policy Reference	Federal Registry Comments	CMS Video Training Comments
		"The covered entity must decide whether to put
GENERAL GUIDELINES TO SAFEGUARD PROTECTED	"it is important to note that covered entities have the flexibility to implement the standard in	
RISK ANALYSIS AND ONGOING RISK MANAGEMENT	d. Comment: One commenter asked whether all health information is considered equally	
See Risk Analysis Policy and Procedure above	"An entity's risk analysis and risk management measures required by § 164.308(a)(1) must	Reducing risk (or risk mitigation) reduction is a
SANCTIONS FOR VIOLATING PRIVACY AND SECURITY	"Some form of sanction or punishment activity must be instituted for noncompliance." "b.	
ACTIVITY REVIEW OF INFORMATION SYSTEM SECURITY	"Our intent for this requirement was to promote the periodic review of an entity's internal	To promote the periodical review of internal
ASSIGNMENT OF SECURITY RESPONSIBILITY	We proposed that the responsibility for security be assigned to a specific individual or	One individual must be assigned the responsibility
ASSIGNMENT AND MANAGEMENT OF INFORMATION	"We proposed implementation of a number of features for personnel security, including	



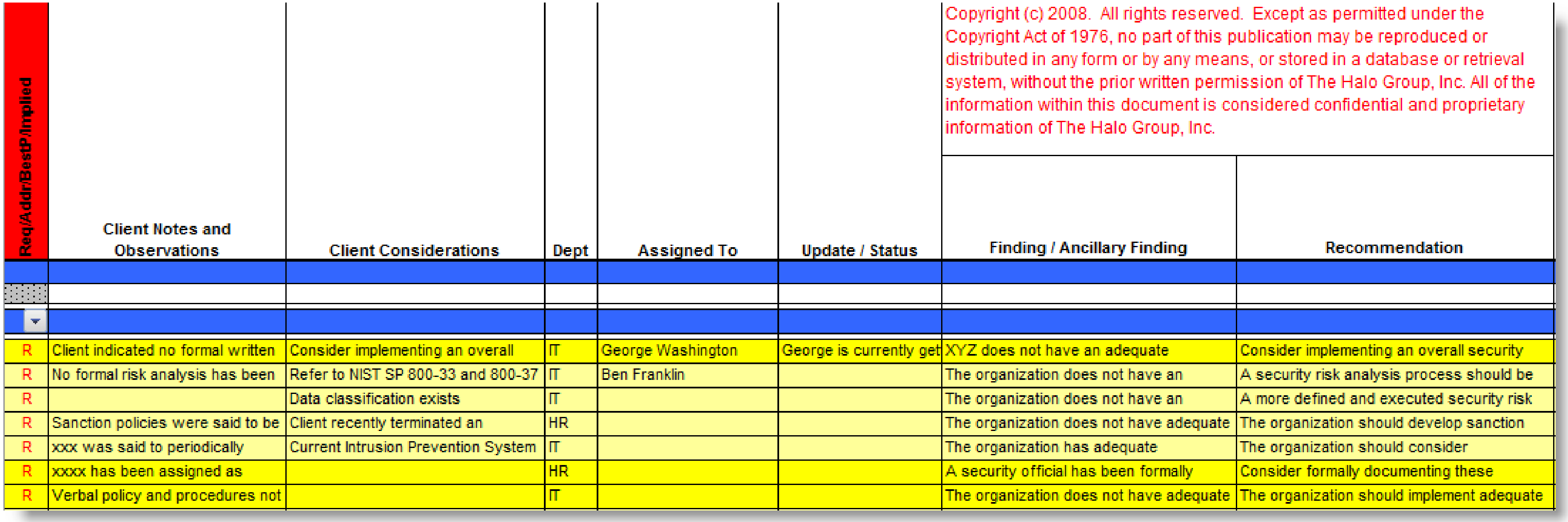
d. Comment: One commenter asked whether all health information is considered equally ''sensitive,'' the thought being that, in determining risk, an entity may consider the loss of a smaller amount of extraordinarily sensitive data to be more significant than the loss of a larger amount of routinely collected data. The commenter stated that common reasoning would suggest that the smaller amount of data would be considered more sensitive. Response: All electronic protected health information must be protected at least to the degree provided by these standards. If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so. e. Comment: One commenter asked that we add ''threat assessment'' to this requirement. Response: We have not done this because we view threat assessment as an inherent part of a risk analysis; adding it would be redundant. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities. "Response: The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. " ------------------ § 164.306(a). an entity's risk analysis and risk management measures required by § 164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with § 164.306(a). --- e. Comment: One commenter stated that there is a need to ensure the confidentiality of risk analysis information that may contain sensitive information. Response: The information included in a risk analysis would not be subject to the security standards if it does not include electronic protected health information. We agree that risk analysis data could contain sensitive information, just as other business information can be sensitive. Covered entities may wish to develop their own business rules regarding access to and

Input…



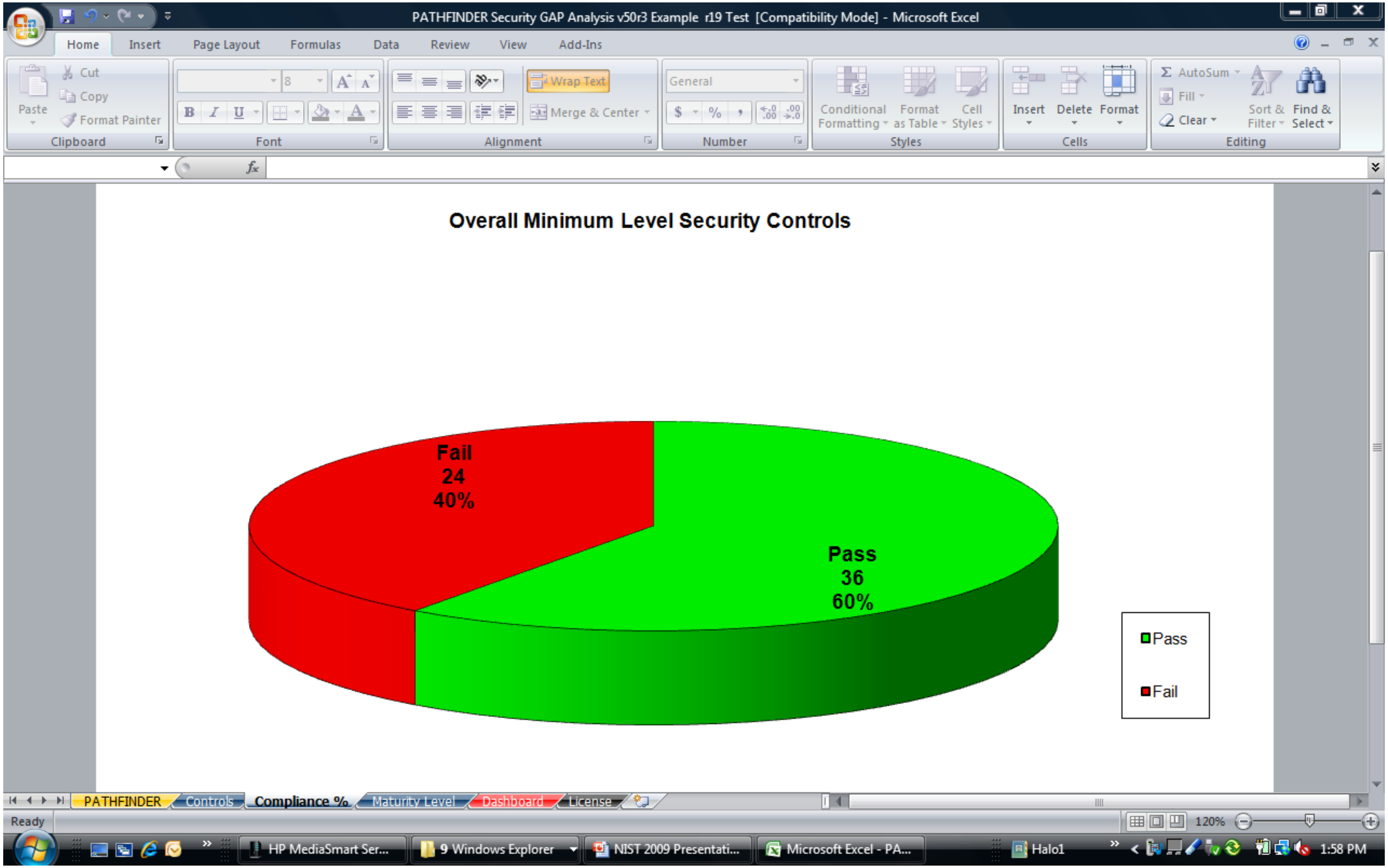
Question	Response					Source			Maturity Level								Security Compliance				Review Date
Compliance Question (M) / Qualifying Questions (Y-YYY)	Yes - Exists	Partial or Needs Impvmt	No or Non Existent	Not Able to Determine	Not Applicable	Client Indication	Supporting Document	Observation	0 - Not Planned	1 - Planned	2 - In-Progress	3 - Performed Informally	4 - Somewhat Implemented	5 - Well Defined /	6 - Consistently Executed	Maturity Level Final	Pass	Fail	Compliant (Pass/Fail)	Est. % Effort Completed	Last Grade Date
Does the organization have a comprehensive	1					1								1		5 - Well Defined/Documented	1		Pass	100%	1Q2009
Has your organization conducted an accurate	1					1								1		5 - Well Defined/Documented	1		Pass	100%	1Q2009
Has the organization implemented a risk	1					1								1		5 - Well Defined/Documented	1		Pass	100%	1Q2009
Does the organization have a sanction policy	1					1							1			4 - Somewhat	1		Pass	100%	Verify
Do procedures to review records of	1					1								1		5 - Well Defined/Documented	1		Pass	100%	Conflicting Info
Does the organization have a designated	1					1							1			4 - Somewhat	1		Pass	100%	1Q2009
Are policies and procedures implemented to	1					1								1		5 - Well Defined/Documented	1		Pass	100%	1Q2009

Findings and Suggestions…



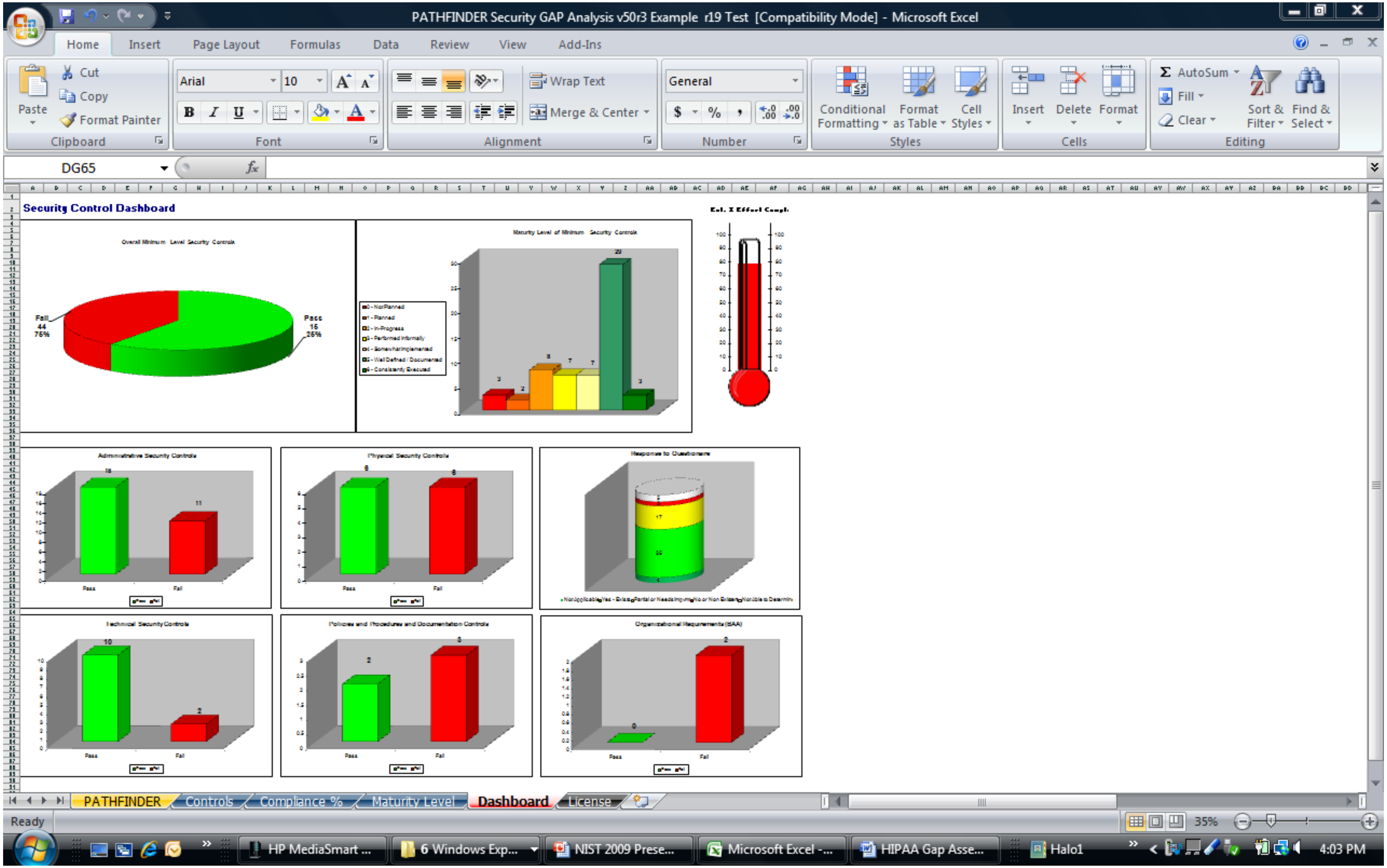
Req/Addr/BestP/Implied	Client Notes and Observations	Client Considerations	Dept	Assigned To	Update / Status	Finding / Ancillary Finding	Recommendation
▾							
R	Client indicated no formal written	Consider implementing an overall	IT	George Washington	George is currently get	XYZ does not have an adequate	Consider implementing an overall security
R	No formal risk analysis has been	Refer to NIST SP 800-33 and 800-37	IT	Ben Franklin		The organization does not have an	A security risk analysis process should be
R		Data classification exists	IT			The organization does not have an	A more defined and executed security risk
R	Sanction policies were said to be	Client recently terminated an	HR			The organization does not have adequate	The organization should develop sanction
R	xxx was said to periodically	Current Intrusion Prevention System	IT			The organization has adequate	The organization should consider
R	xxxx has been assigned as		HR			A security official has been formally	Consider formally documenting these
R	Verbal policy and procedures not		IT			The organization does not have adequate	The organization should implement adequate

Compliance %…



PATHFINDER Security GAP Analysis v50r3 Example r19 Test [Compatibility Mode] - Microsoft Excel

Dashboard…



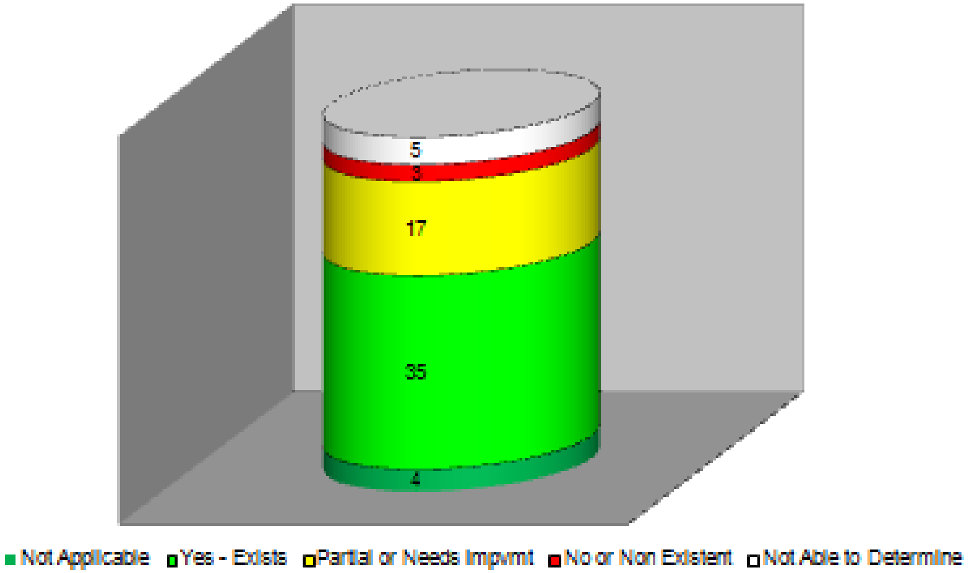
PATHFINDER Security GAP Analysis v50r3 Example r19 Test [Compatibility Mode] - Microsoft Excel

DG65

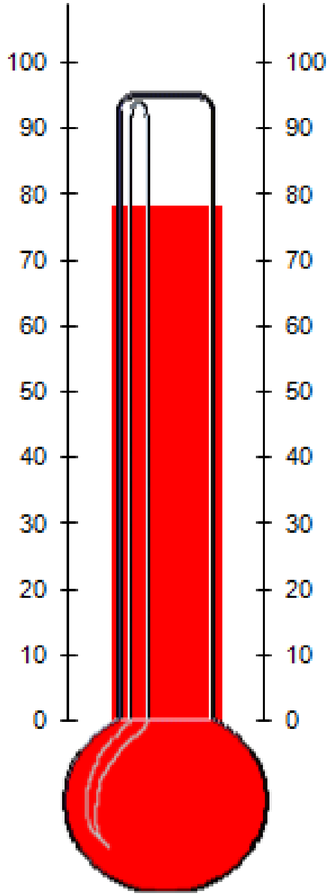
Security Control Dashboard

Dashboard…

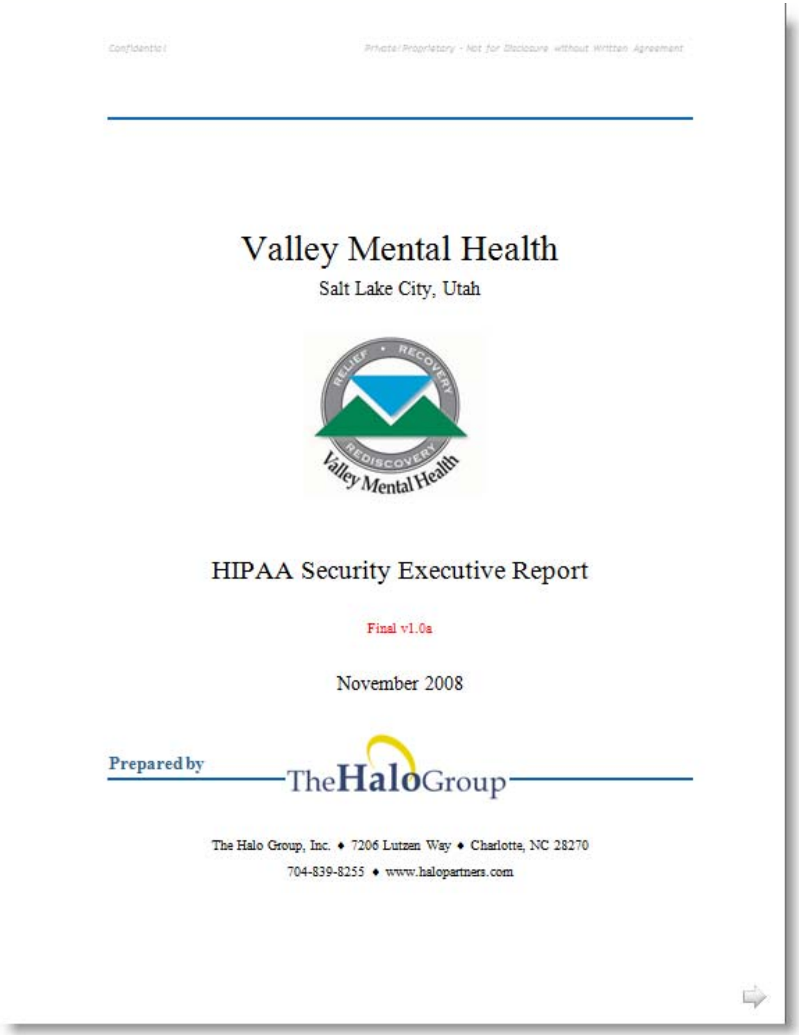
Response to Questionaire



Est. % Effort Completed



Executive Report…



Confidential   Private/Proprietary - Not for Disclosure without Written Agreement

Valley Mental Health

Salt Lake City, Utah

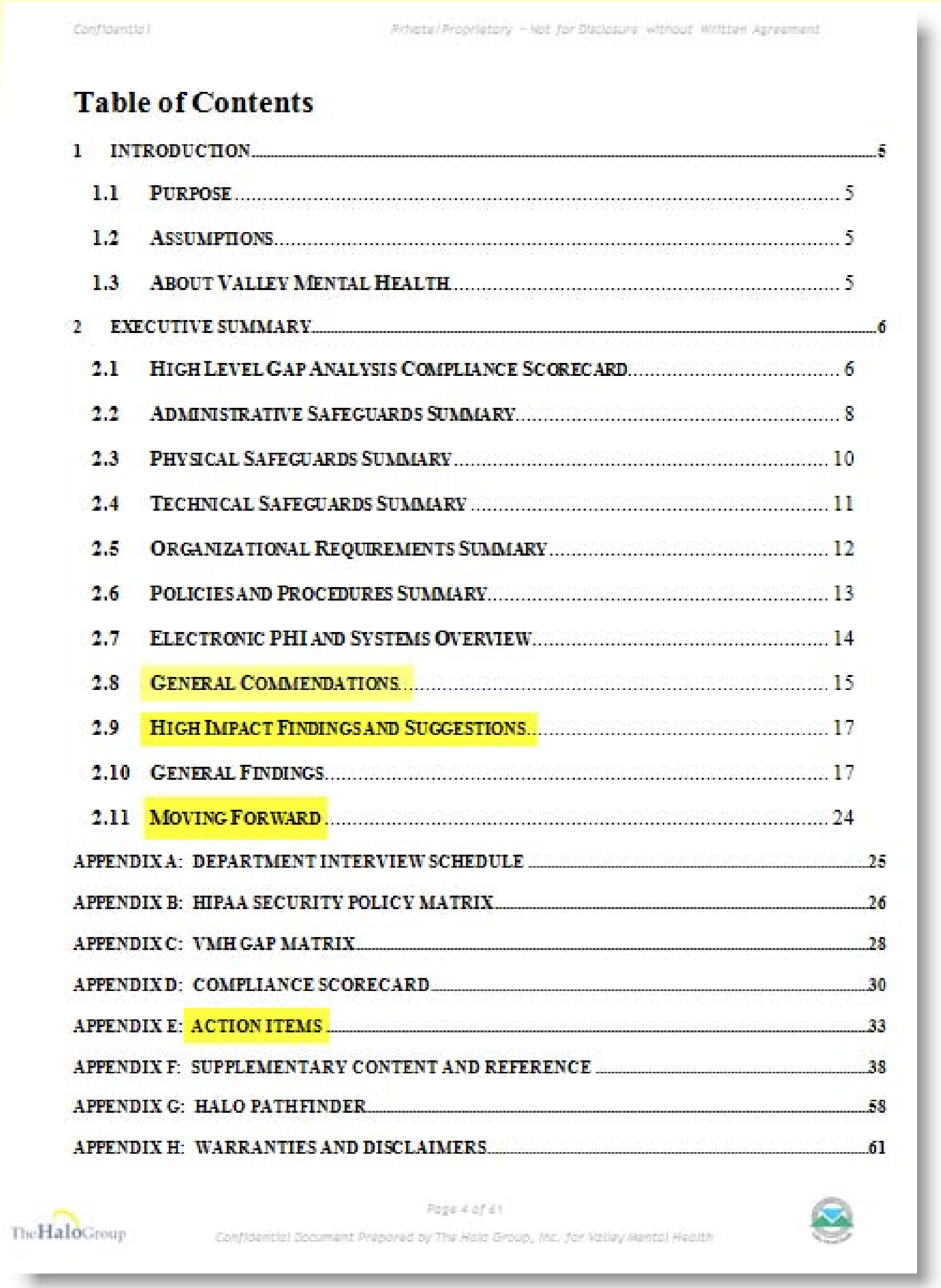
HIPAA Security Executive Report

Final v1.0a

November 2008

Prepared by The Halo Group

The Halo Group, Inc. ♦ 7206 Lutzen Way ♦ Charlotte, NC 28270
704-839-8255 ♦ www.halopartners.com



Confidential   Private/Proprietary - Not for Disclosure without Written Agreement

Table of Contents

The Halo Group   Page 4 of 61

Confidential Document Prepared by The Halo Group, Inc. for Valley Mental Health

Client Feedback…

- Executive Leadership Team appreciates dashboard view.
- Security Team favored details of the report and maturity model.
- Management Team liked the detailed Action Item list.
- Management liked the ability to show progress to Executives.
- Simplicity and portability of Microsoft Excel spreadsheet.
- Team liked the explanations of each Standard and Implementation Specification. Cross references to the Federal Registry Comments, CMS Video, and other sources. Cross references of required Policies and Procedures.

Questions…

Steve Taylor
SteveT@vmh.com
801-743-6159

Susan A. Miller, JD
TMSAM@aol.com
978-369-2092

Larry C. Eighmy
LarryEighmy@HaloPartners.com
704-839-8255