Presented by:
Vienna Morrill

IT SECURITY RISK ASSESSMENT

CASE STUDY FROM UNC CHARLOTTE

BerryDunn

VIENNA MORRILL, MSA, CISA

Manager
BerryDunn
Management and IT
Consulting Group

AGENDA

1. What is risk?
2. Why do an IT Security Risk Assessment?
3. What does the IT Security Risk Assessment process entail?
4. What elements of this approach should you apply in your organization?

F12
Risk
Enter

STACKING UP THE RISKS

Winning PowerBall Grand Prize (1 in 175.2M)

Attacked and killed by shark (1 in 3.7M)

Getting a hole in one (1 in 12,750)

Getting struck by lightening (1 in 12,000)

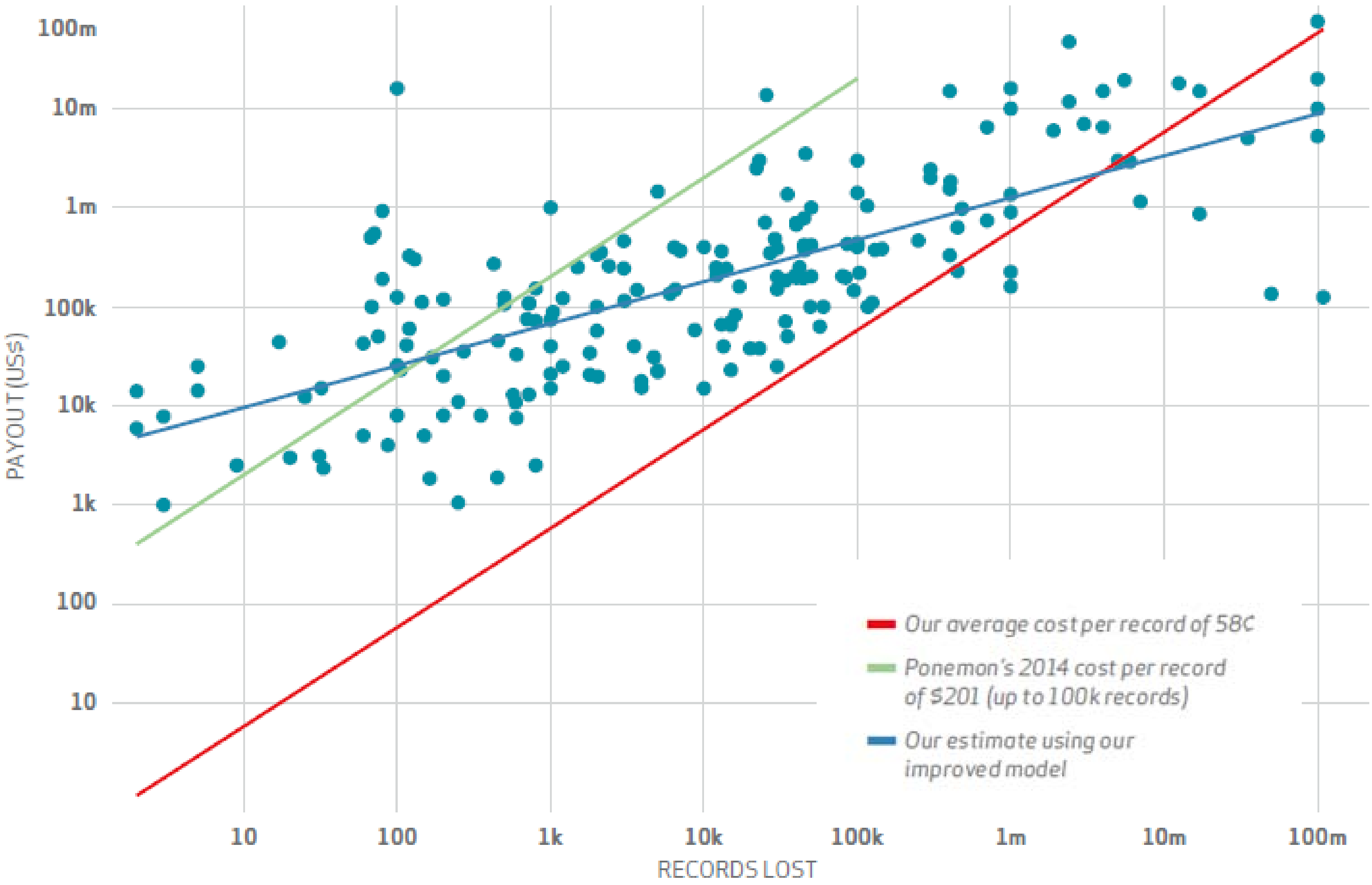
Being audited by the IRS (1 in 175)

Having a security breach at your organization
in the next two years (1 in 5)

COST OF A DATA BREACH

Estimates range from $0.58/record (Verizon Data Breach Investigations Report) to $201/record (Ponemon Institute Report).

COST OF A DATA BREACH



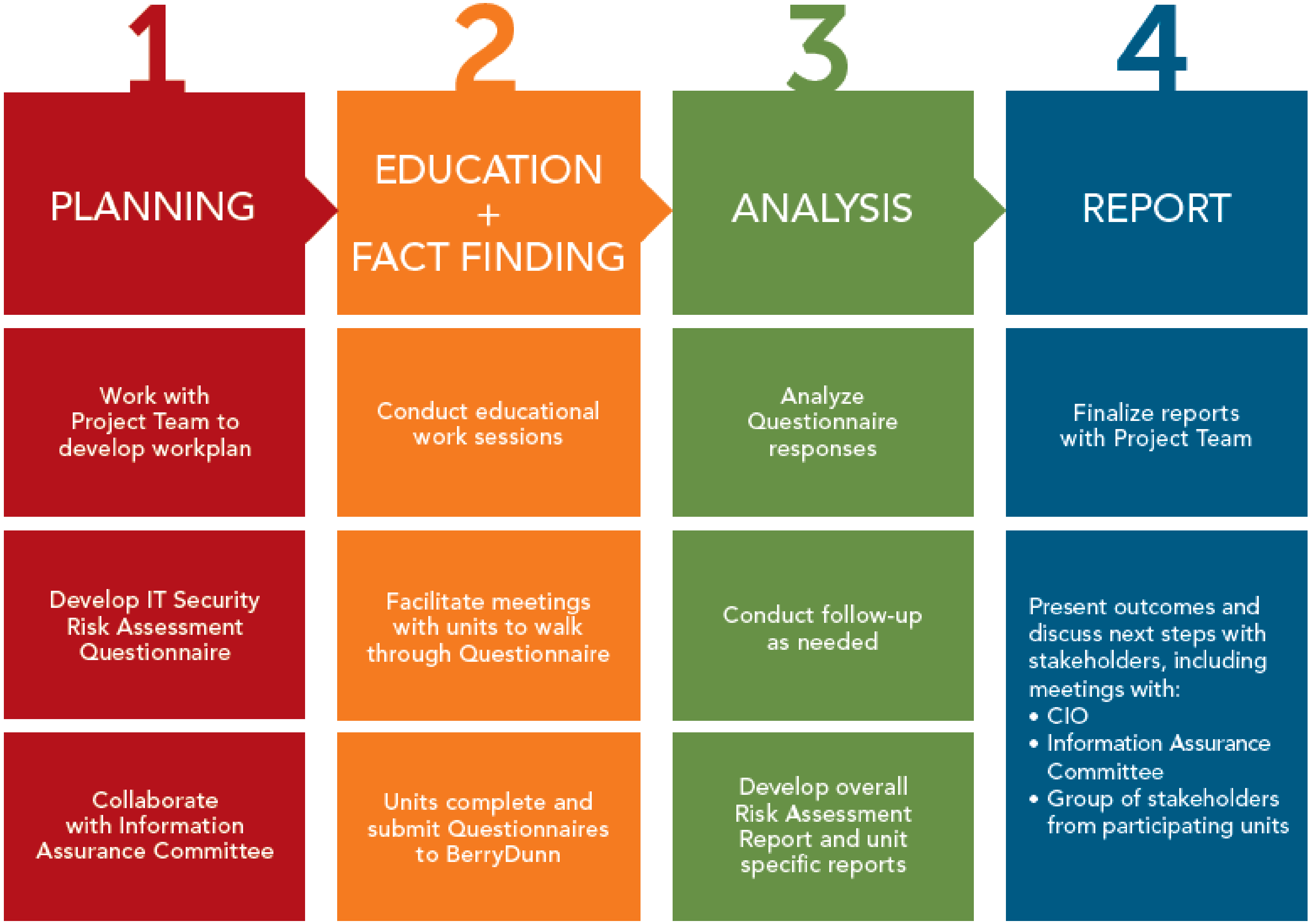
Source: Verizon 2015 Data Breach Investigations Report

CASE STUDY

UNC CHARLOTTE

Information Technology
Security Risk Assessment

THE RISK ASSESSMENT PROCESS



1 PLANNING	2 EDUCATION + FACT FINDING	3 ANALYSIS	4 REPORT
Work with Project Team to develop workplan	Conduct educational work sessions	Analyze Questionnaire responses	Finalize reports with Project Team
Develop IT Security Risk Assessment Questionnaire	Facilitate meetings with units to walk through Questionnaire	Conduct follow-up as needed	Present outcomes and discuss next steps with stakeholders, including meetings with: • CIO • Information Assurance Committee • Group of stakeholders from participating units
Collaborate with Information Assurance Committee	Units complete and submit Questionnaires to BerryDunn	Develop overall Risk Assessment Report and unit specific reports	

1

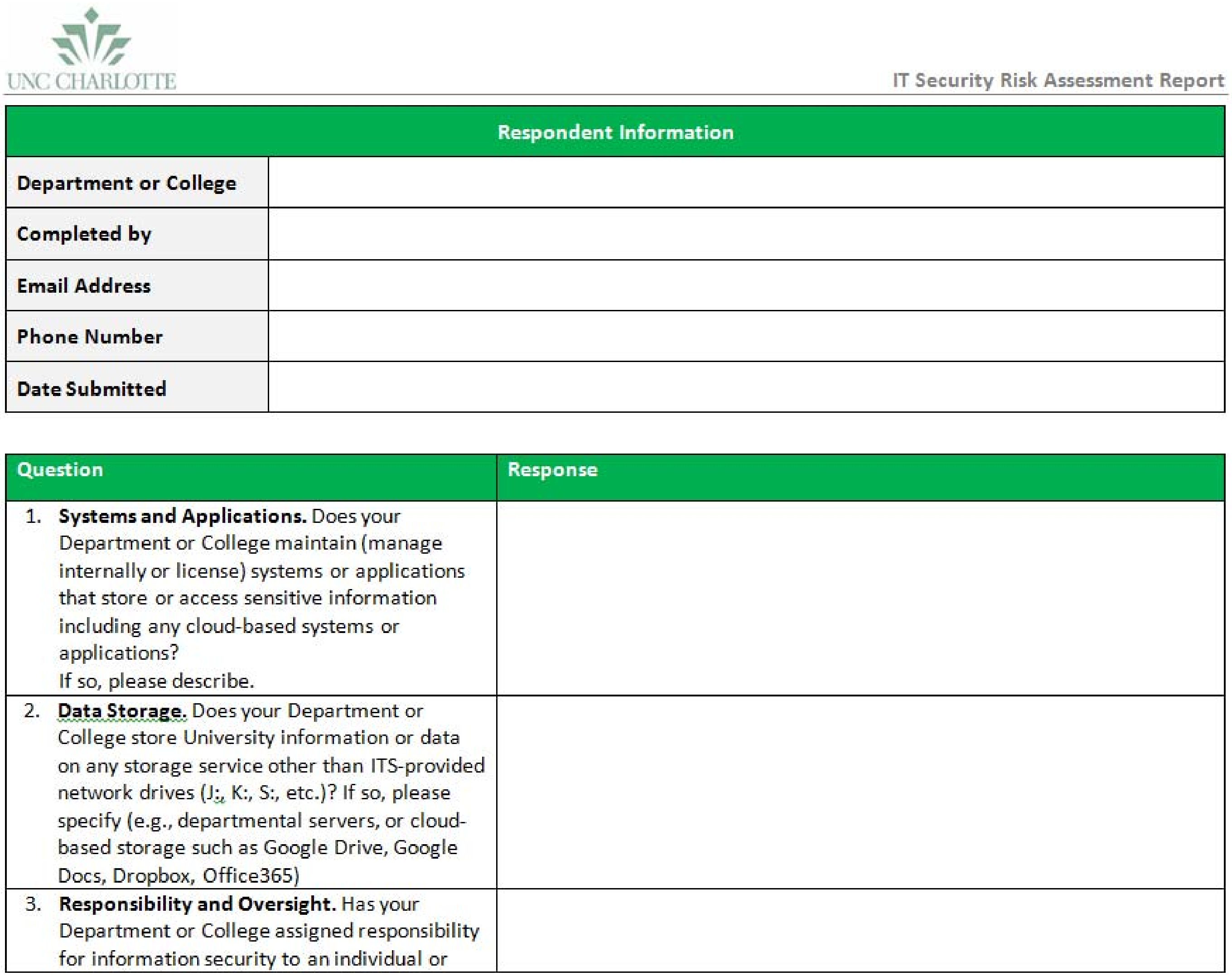
PLANNING

Work with Project Team to develop workplan

Develop IT Security Risk Assessment Questionnaire

Collaborate with Information Assurance Committee

THE QUESTIONNAIRE



UNC CHARLOTTE

IT Security Risk Assessment Report

Respondent Information	
Department or College	
Completed by	
Email Address	
Phone Number	
Date Submitted	

Question	Response
1. **Systems and Applications.** Does your Department or College maintain (manage internally or license) systems or applications that store or access sensitive information including any cloud-based systems or applications? If so, please describe.	
2. **Data Storage.** Does your Department or College store University information or data on any storage service other than ITS-provided network drives (J:, K:, S:, etc.)? If so, please specify (e.g., departmental servers, or cloud-based storage such as Google Drive, Google Docs, Dropbox, Office365)	
3. **Responsibility and Oversight.** Has your Department or College assigned responsibility for information security to an individual or	

Included 21 Risk Areas:

1. Systems and Applications
2. Data Storage
3. Responsibility and Oversight
4. Information Security Training and Awareness
5. IT Security Incident Response
6. Access Controls
7. Audit Logs
8. Remote Access
9. Change Management
10. Incident Management
11. Physical Security
12. Data Transmission
13. Service Provider/ Vendor Due Diligence
14. Disaster Recovery Planning
15. Data Backups
16. Copiers and Multi-Function Devices
17. Hardware Disposal
18. Mobile Devices
19. Compliance
20. Data Protection
21. Credit Cards/Payment Information

2

EDUCATION + FACT FINDING

Conduct educational work sessions

Facilitate meetings with units to walk through Questionnaire

Units complete and submit Questionnaires to BerryDunn

3

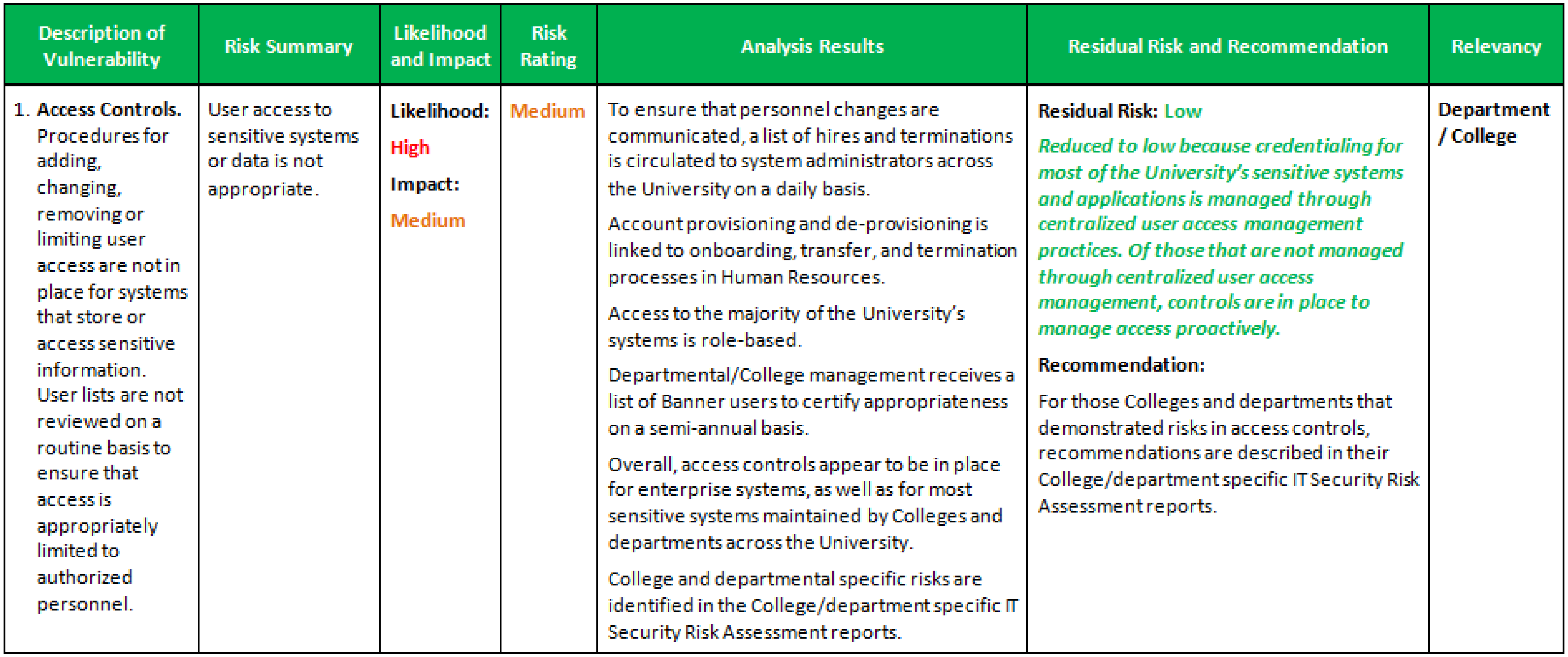
ANALYSIS

Analyze Questionnaire responses

Conduct follow-up as needed

Develop overall Risk Assessment Report and unit specific reports

THE IT SECURITY RISK ASSESSMENT MATRIX



Description of Vulnerability	Risk Summary	Likelihood and Impact	Risk Rating	Analysis Results	Residual Risk and Recommendation	Relevancy
1. **Access Controls.** Procedures for adding, changing, removing or limiting user access are not in place for systems that store or access sensitive information. User lists are not reviewed on a routine basis to ensure that access is appropriately limited to authorized personnel.	User access to sensitive systems or data is not appropriate.	**Likelihood:** High **Impact:** Medium	Medium	To ensure that personnel changes are communicated, a list of hires and terminations is circulated to system administrators across the University on a daily basis. Account provisioning and de-provisioning is linked to onboarding, transfer, and termination processes in Human Resources. Access to the majority of the University's systems is role-based. Departmental/College management receives a list of Banner users to certify appropriateness on a semi-annual basis. Overall, access controls appear to be in place for enterprise systems, as well as for most sensitive systems maintained by Colleges and departments across the University. College and departmental specific risks are identified in the College/department specific IT Security Risk Assessment reports.	**Residual Risk:** Low ***Reduced to low because credentialing for most of the University's sensitive systems and applications is managed through centralized user access management practices. Of those that are not managed through centralized user access management, controls are in place to manage access proactively.*** **Recommendation:** For those Colleges and departments that demonstrated risks in access controls, recommendations are described in their College/department specific IT Security Risk Assessment reports.	**Department / College**

HEAT MAPS

Exhibit A: Risk Profile Map

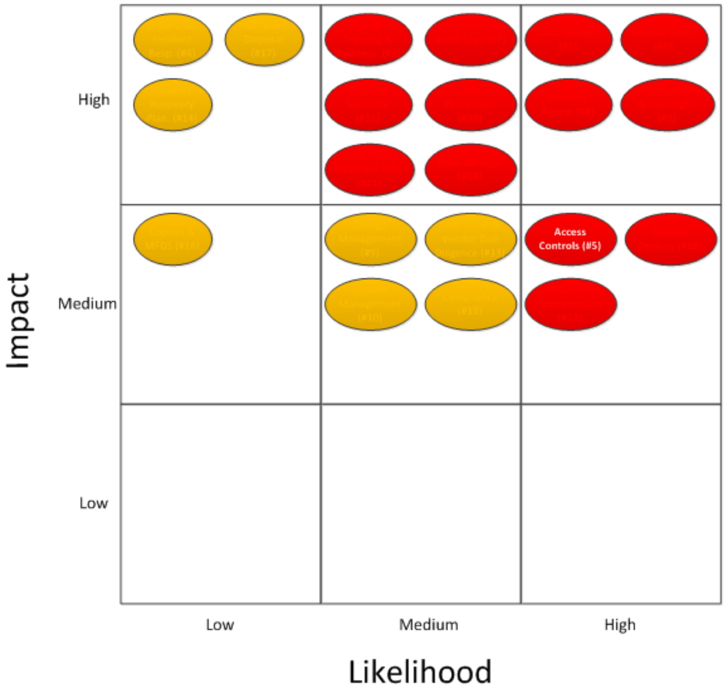
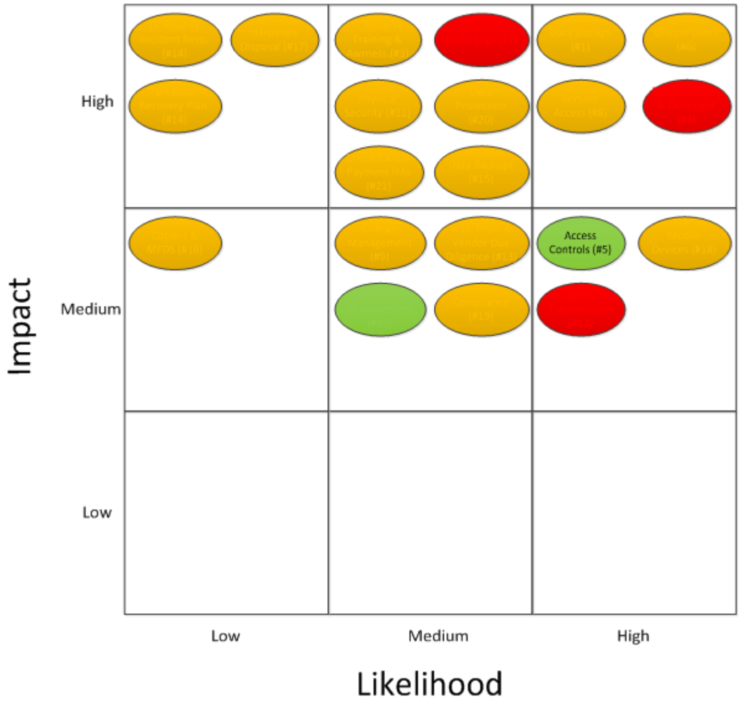


Exhibit B: Residual Risk Map



4

REPORT

Finalize reports with Project Team

Present outcomes and discuss next steps with stakeholders, including meetings with:

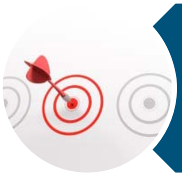
- CIO
- Information Assurance Committee
- Group of stakeholders from participating units

OUTCOMES FOR UNC CHARLOTTE

Fostered Collaboration

Developed a Sustainable Approach

Increased Awareness for IT Security Risk



Established Priorities for Addressing Gaps

TAKEAWAYS

It’s a risky world and security breaches are expensive.

Engagement of stakeholders and executive level support are critical.

An IT security risk assessment is not an audit.

Conducting an Information Security Risk Assessment doesn’t have to be complicated.

QUESTIONS

INTERESTED IN MORE?

We are always available for your questions

vmorrill@berrydunn.com