2017 HCCA Clinical Practice Compliance Conference
Sunday, October 15, 2017 (12:30-2PM)
Session P3

The Art of Information Security Risk Assessments; you don’t have to be Classically Trained to be an Expert. The Basics of Risk Assessments and Strategies for Keeping your Assessment Current

BAPTIST HEALTH CARE

Jim Donaldson, M.S., MPA, CHC, CIPP/US, CISSP

Chief Compliance, Privacy and Information Security Officer
Baptist Health Care Corporation
Pensacola, Florida

BAPTIST HEALTH CARE

Baptist Health Care Corporation

Not-For-Profit, Locally Owned,
Integrated Delivery System
Headquartered in Pensacola, Florida

6800 Employees

3 Florida Hospitals
Hospital Based Inpatient Behavioral Health Facility
Surgery Centers, Rehab Offices, Commercial Pharmacies, Walk-In Care, Occupational Health

230+ Employed Providers
Andrews Institute Ortho and Sports Med
Athletic Trainers Assigned to Public Schools

BAPTIST HEALTH CARE

Lakeview Center Inc.

Fully Owned Subsidiary of BHC

Outpatient and Residential Behavioral Health

And……

Child Adoption Program
Children Services Center
FamiliesFirst Network (DCF)
Global Connections to Employment – Non-Healthcare Federal Contracts at Locations in 14 states and D.C.
2 DQ Grill & Chill Restaurants in the Tampa Area
DUI Program
Methadone Program

BAPTIST HEALTH CARE

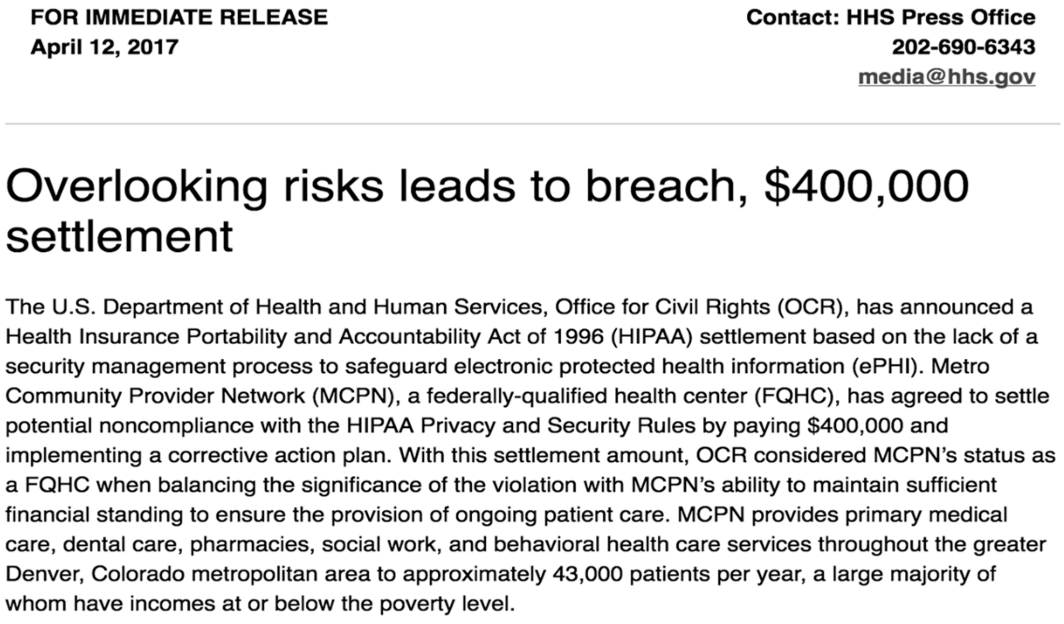
House Keeping and Other Items:

- The format is informal so ask questions along the way
- Your presenter does not know everything so audience participation is critical to the success of the session
- Surveys – Please complete one after each session
- After the conference is over, feel free to contact me anytime I may be of assistance in helping you have a successful compliance career.

BAPTIST HEALTH CARE

Session Goals

- Why the lack of a comprehensive information security risk assessment is singled out in almost every OCR HIPAA settlement agreement.
- Risk assessment basics and free references to help your organization through the process
- Walkthrough of a basic assessment

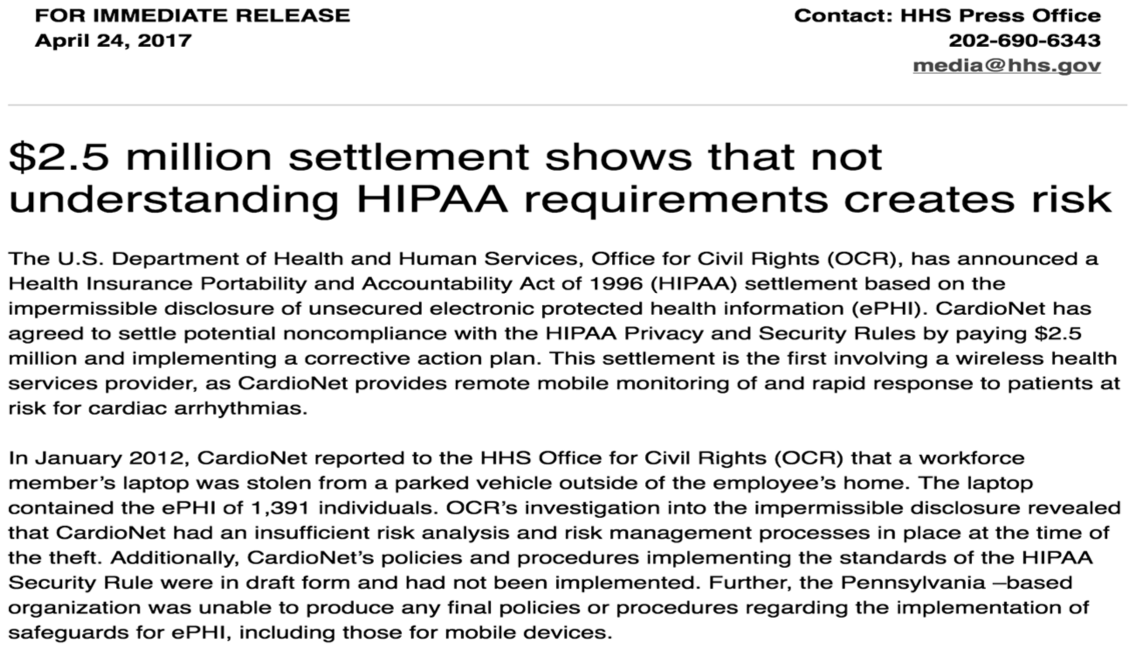


FOR IMMEDIATE RELEASE
April 12, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Overlooking risks leads to breach, $400,000 settlement

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the lack of a security management process to safeguard electronic protected health information (ePHI). Metro Community Provider Network (MCPN), a federally-qualified health center (FQHC), has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $400,000 and implementing a corrective action plan. With this settlement amount, OCR considered MCPN's status as a FQHC when balancing the significance of the violation with MCPN's ability to maintain sufficient financial standing to ensure the provision of ongoing patient care. MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.



FOR IMMEDIATE RELEASE
April 24, 2017

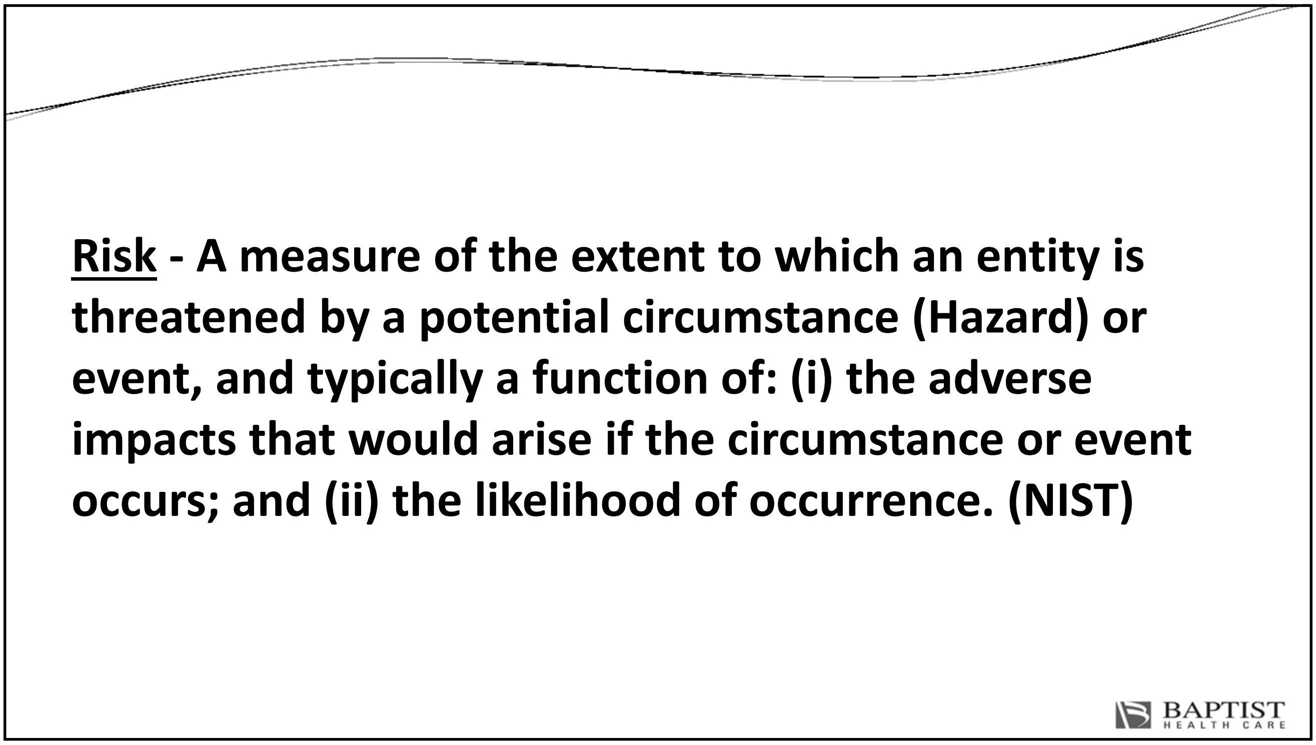
Contact: HHS Press Office
202-690-6343
media@hhs.gov

$2.5 million settlement shows that not understanding HIPAA requirements creates risk

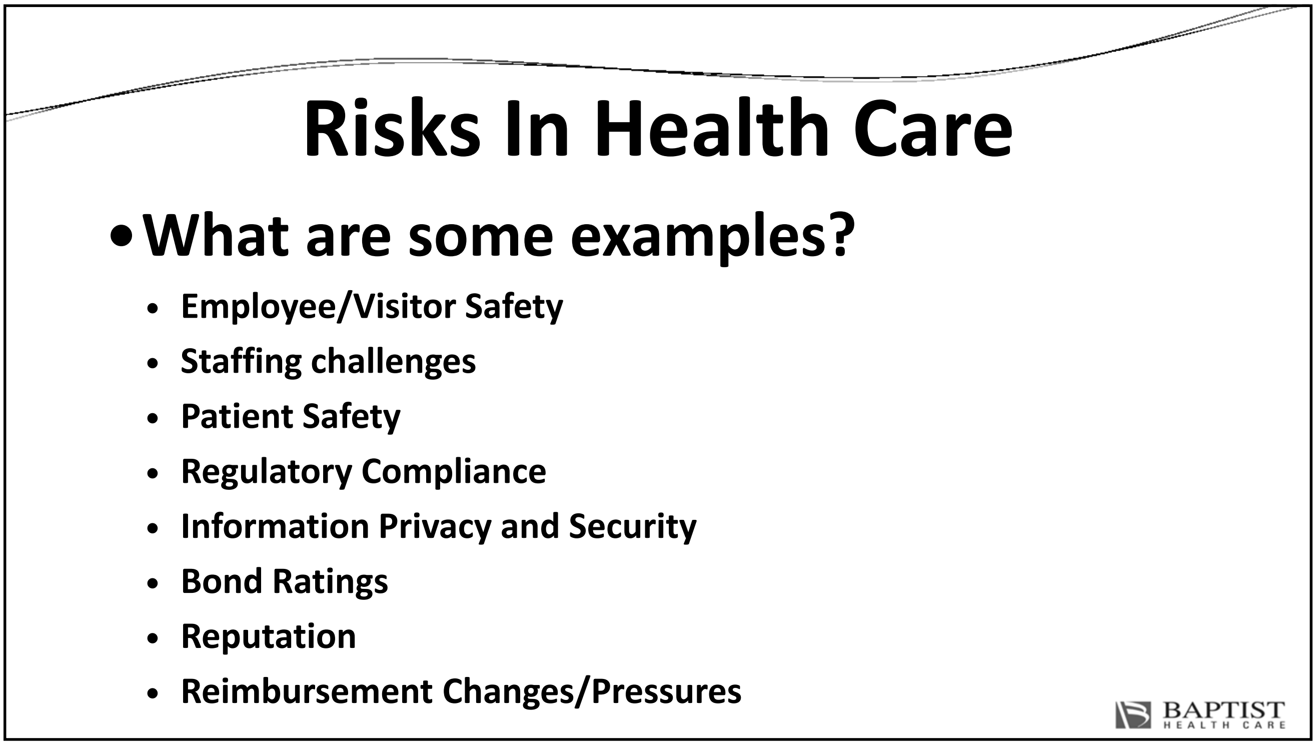
The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI). CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania –based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

Risk – The possibility that something bad or unpleasant (such as an injury or loss) will happen (Merriam-Webster)

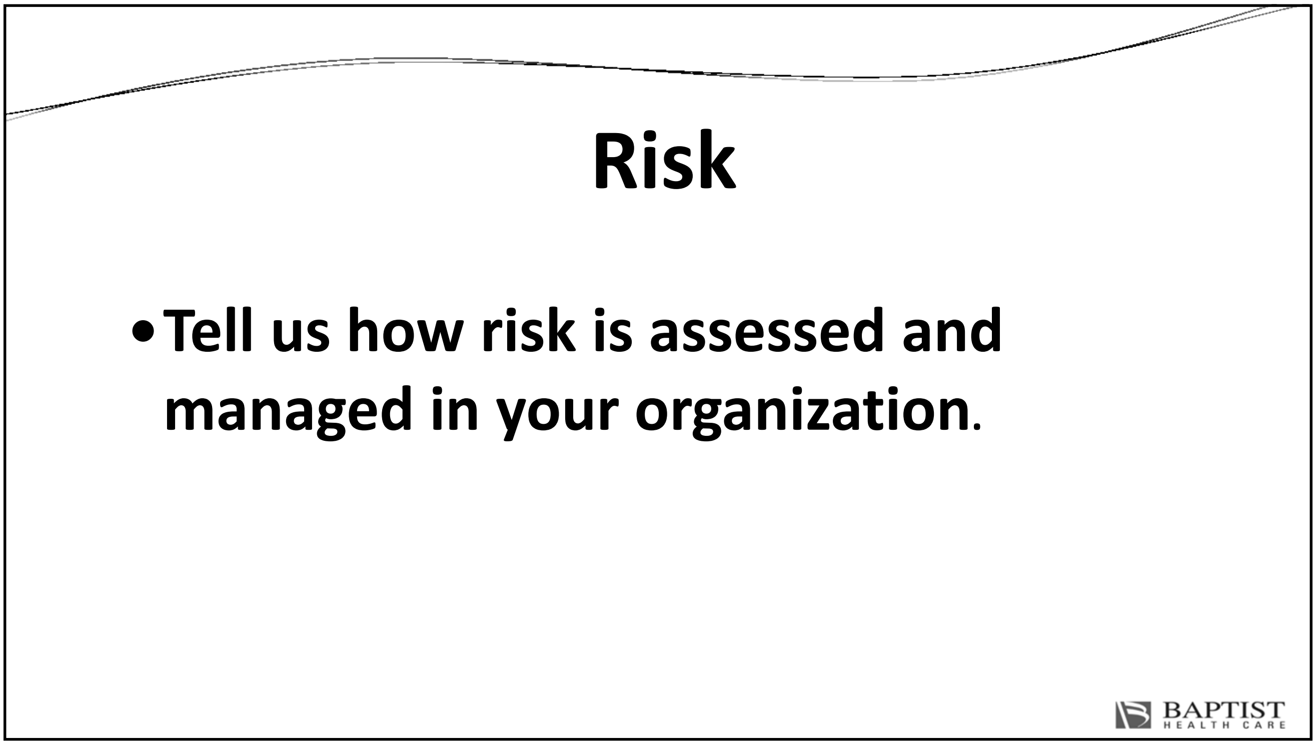


Risk - A measure of the extent to which an entity is threatened by a potential circumstance (Hazard) or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NIST)



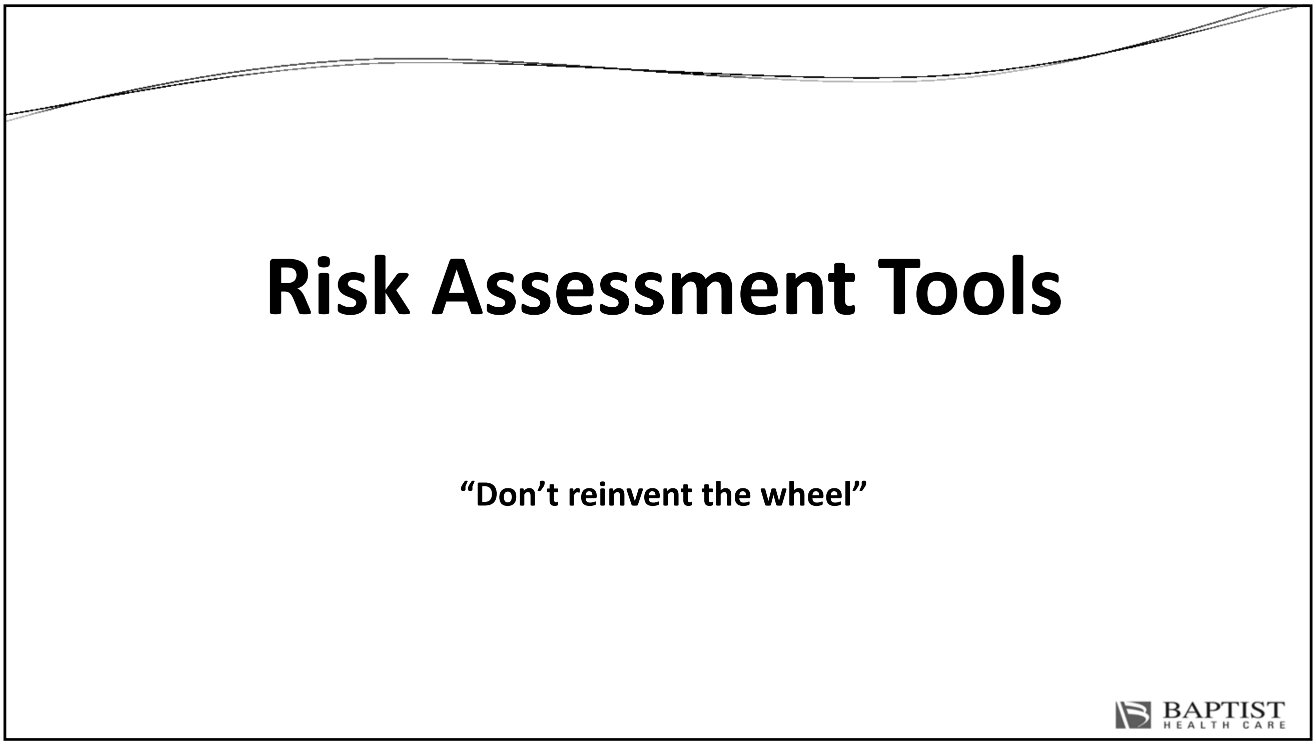
Risks In Health Care

- What are some examples?
  - Employee/Visitor Safety
  - Staffing challenges
  - Patient Safety
  - Regulatory Compliance
  - Information Privacy and Security
  - Bond Ratings
  - Reputation
  - Reimbursement Changes/Pressures



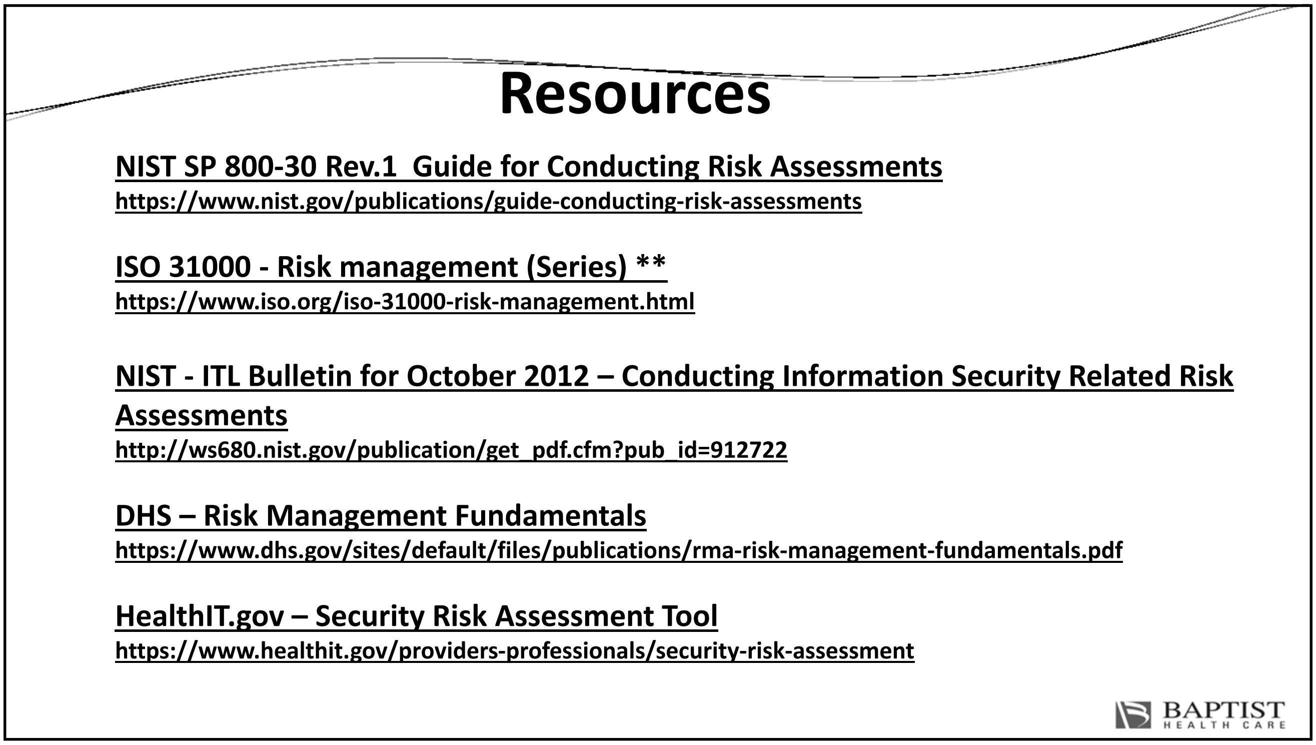
Risk

- Tell us how risk is assessed and managed in your organization.



Risk Assessment Tools

“Don’t reinvent the wheel”



Resources

NIST SP 800-30 Rev.1 Guide for Conducting Risk Assessments
https://www.nist.gov/publications/guide-conducting-risk-assessments

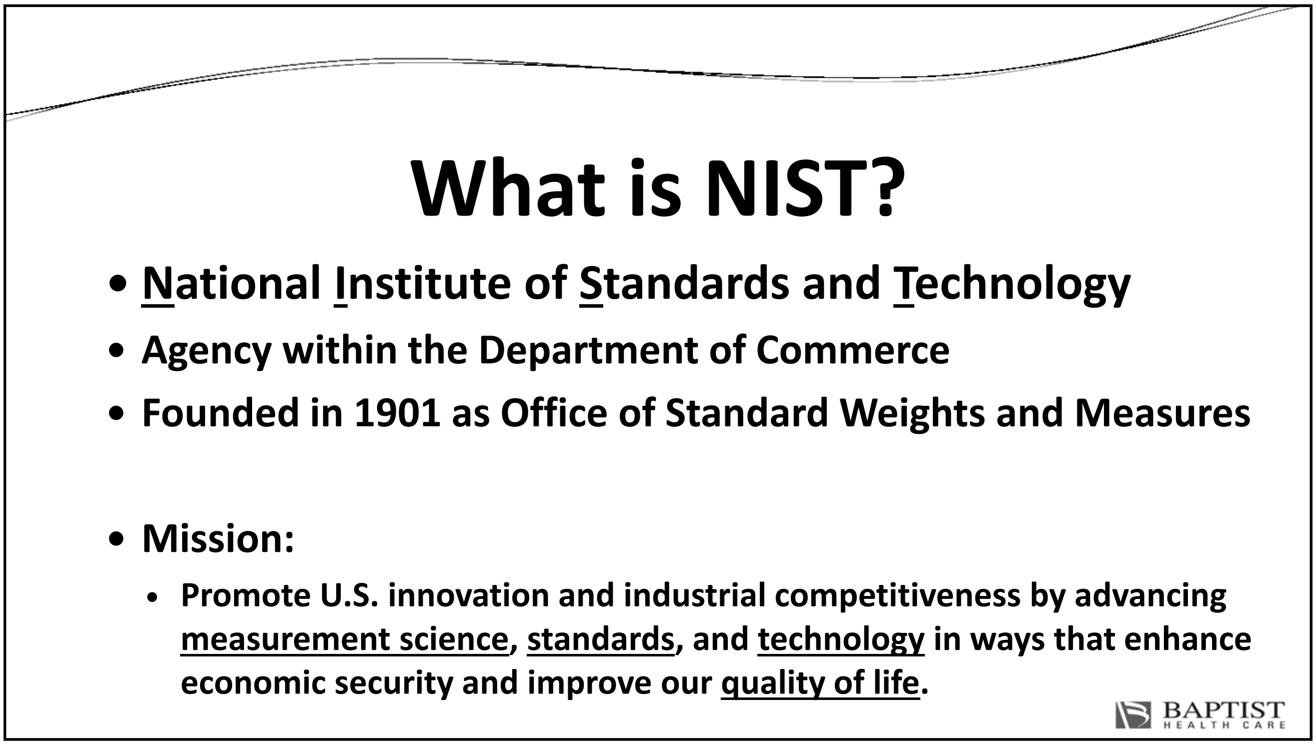
ISO 31000 - Risk management (Series) **
https://www.iso.org/iso-31000-risk-management.html

NIST - ITL Bulletin for October 2012 – Conducting Information Security Related Risk Assessments
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=912722

DHS – Risk Management Fundamentals
https://www.dhs.gov/sites/default/files/publications/rma-risk-management-fundamentals.pdf

HealthIT.gov – Security Risk Assessment Tool
https://www.healthit.gov/providers-professionals/security-risk-assessment

BAPTIST HEALTH CARE



What is NIST?

- **National Institute of Standards and Technology**
- **Agency within the Department of Commerce**
- **Founded in 1901 as Office of Standard Weights and Measures**

- **Mission:**
  - **Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.**

BAPTIST HEALTH CARE

The NIST 800 Series

- Special Publications in the 800 series (established in 1990) are of general interest to the computer security community. This series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

The NIST 800 Series (examples)

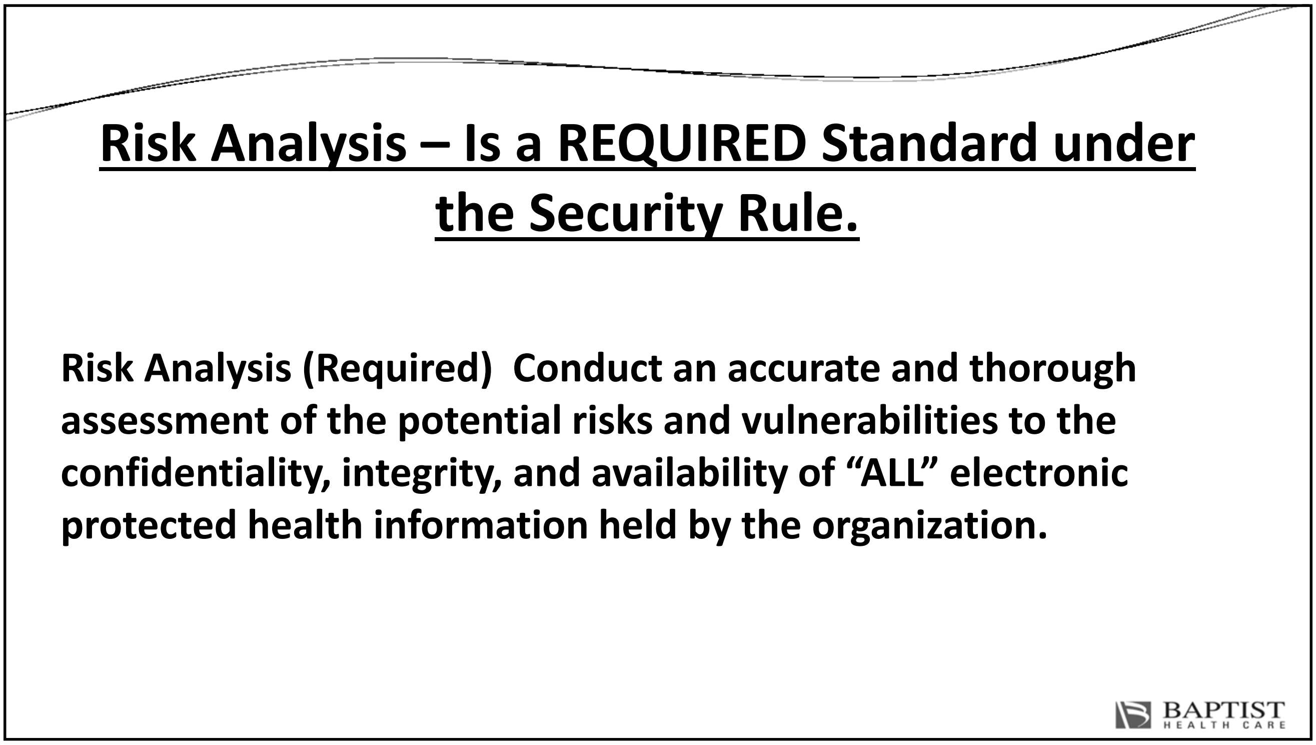
- 800-163 Vetting the Security of Mobile Applications
- 800-153 Guidelines for Security Wireless Local Area Networks
- 800-145 The NIST Definition of Cloud Computing
- 800-121 Guide to Bluetooth Security
- 800-88 Guidelines for Media Sanitization
- 800- Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach

NIST Special Publication 800-30 Revision 1

Guide for Conducting Risk Assessments

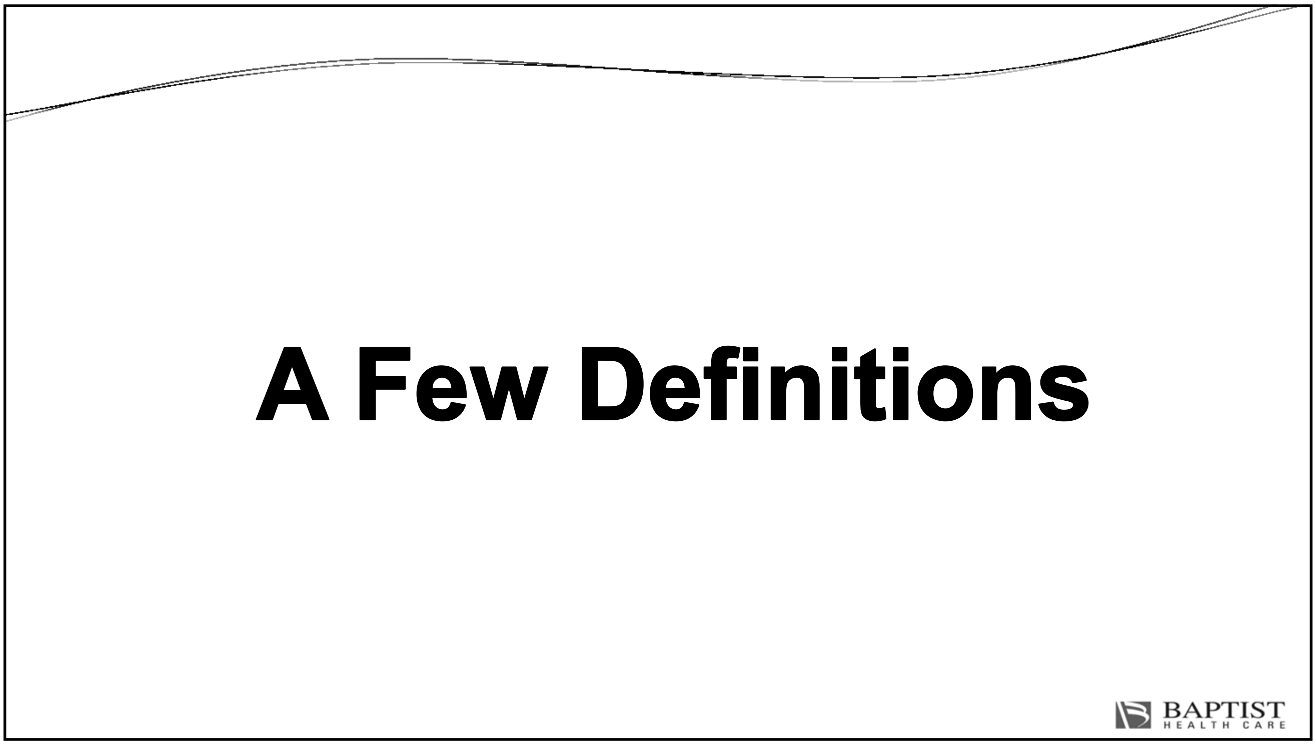
Disclaimers

- **There are many U.S. and international resources to assist you and your organization with risk assessment and management. This session is not intended to make you an expert but it is intended to provide you with a basic understanding of the risk assessment process laid out in NIST 800-30.**
- **NIST 800-30 was written primarily to address cyber security related risks. HOWEVER – the framework and processes are solid and will work for assessing any risk areas. We will hitch a ride on 800-30.**
- **The vast majority of this presentation is attributable to the work published by NIST.**



Risk Analysis – Is a REQUIRED Standard under the Security Rule.

Risk Analysis (Required) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of "ALL" electronic protected health information held by the organization.



A Few Definitions

Threat/Hazard – Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals or other organizations

Threat Source:

- **The intent and method (Vector) targeted at exploiting a vulnerability**
- **A situation and method that may accidentally exploit a vulnerability**

Risk Assessment - The process of identifying, estimating and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals and other organizations. (NIST)

Risk Assessment - A process to identify potential hazards and analyze what could happen if a hazard occurs. (Ready.Gov)

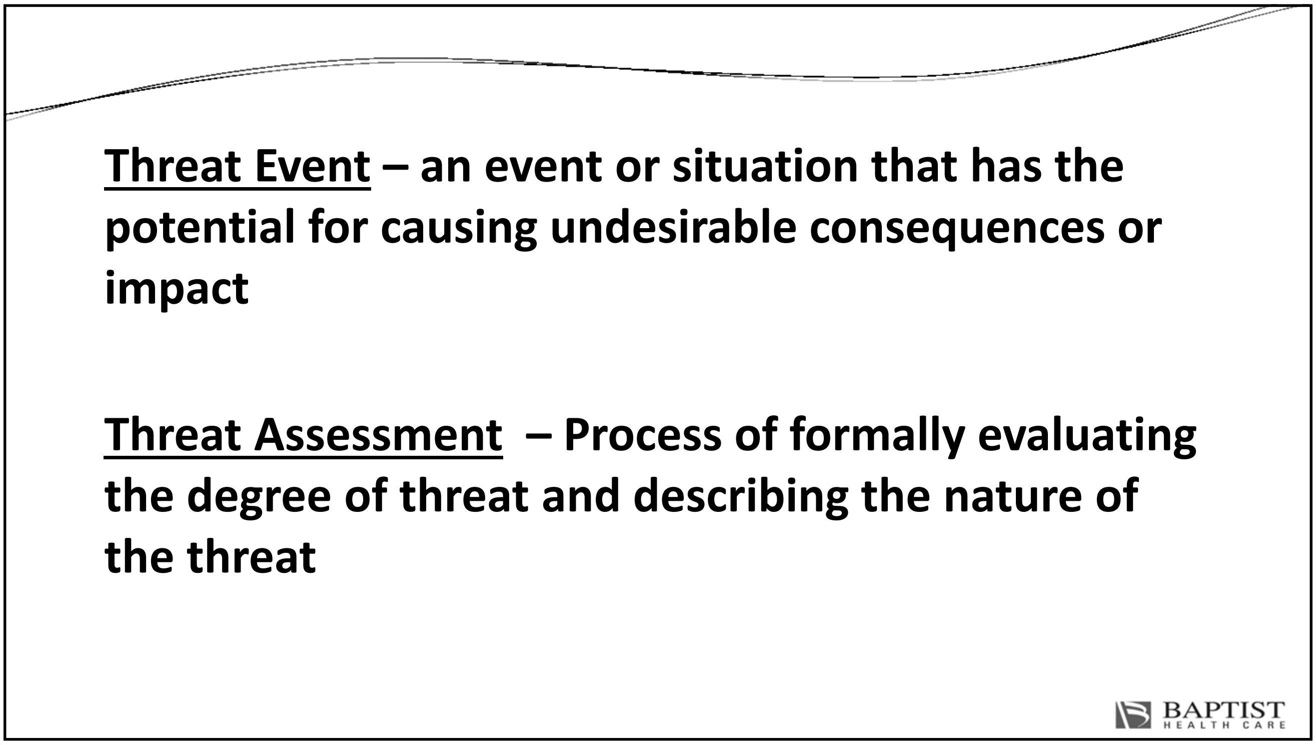
<u>Risk Assessment</u> – The process to identify the potential hazards arising from a work activity and the likelihood of harm from those hazards, then putting the two together to estimate the risk involved in the activity. (NERC)

BAPTIST HEALTH CARE

<u>Vulnerability</u> – the inability to withstand hostile environment and/or action from a threat source

<u>Vulnerability Assessment</u> – The process of identifying, quantifying and prioritizing vulnerabilities

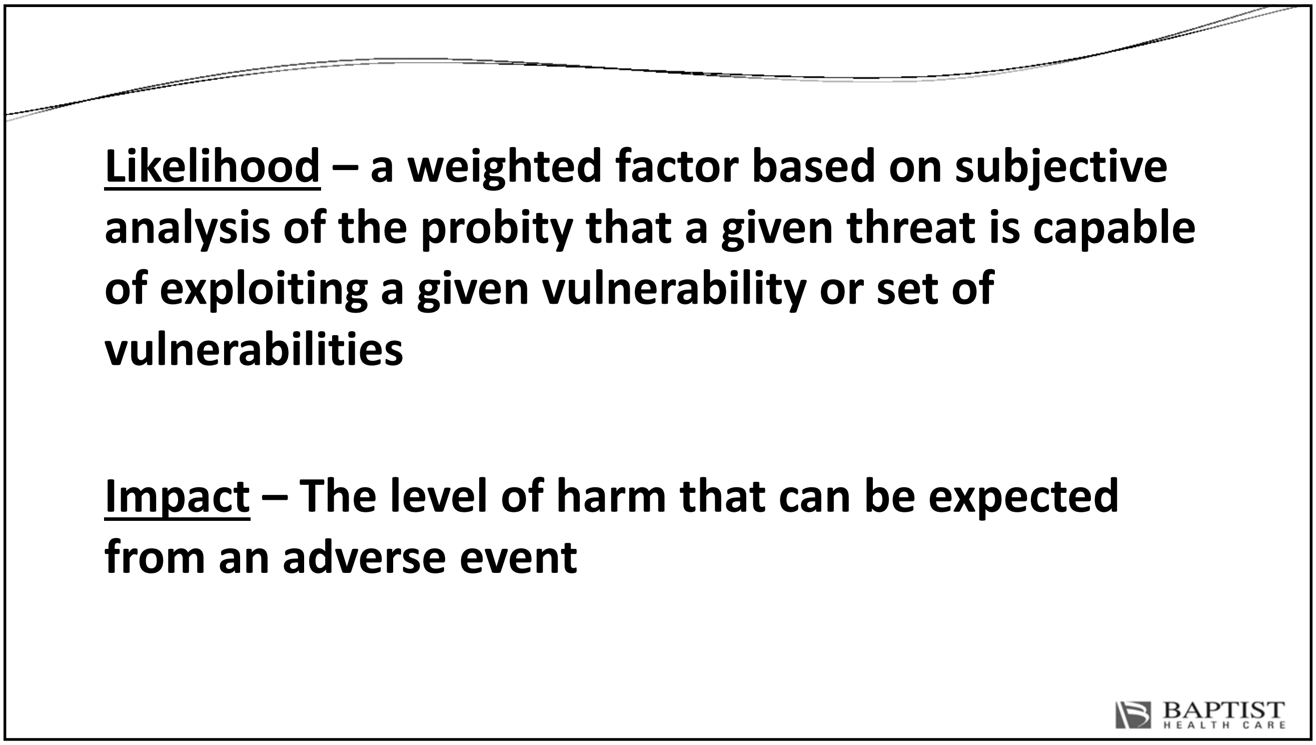
BAPTIST HEALTH CARE



Threat Event – an event or situation that has the potential for causing undesirable consequences or impact

Threat Assessment – Process of formally evaluating the degree of threat and describing the nature of the threat

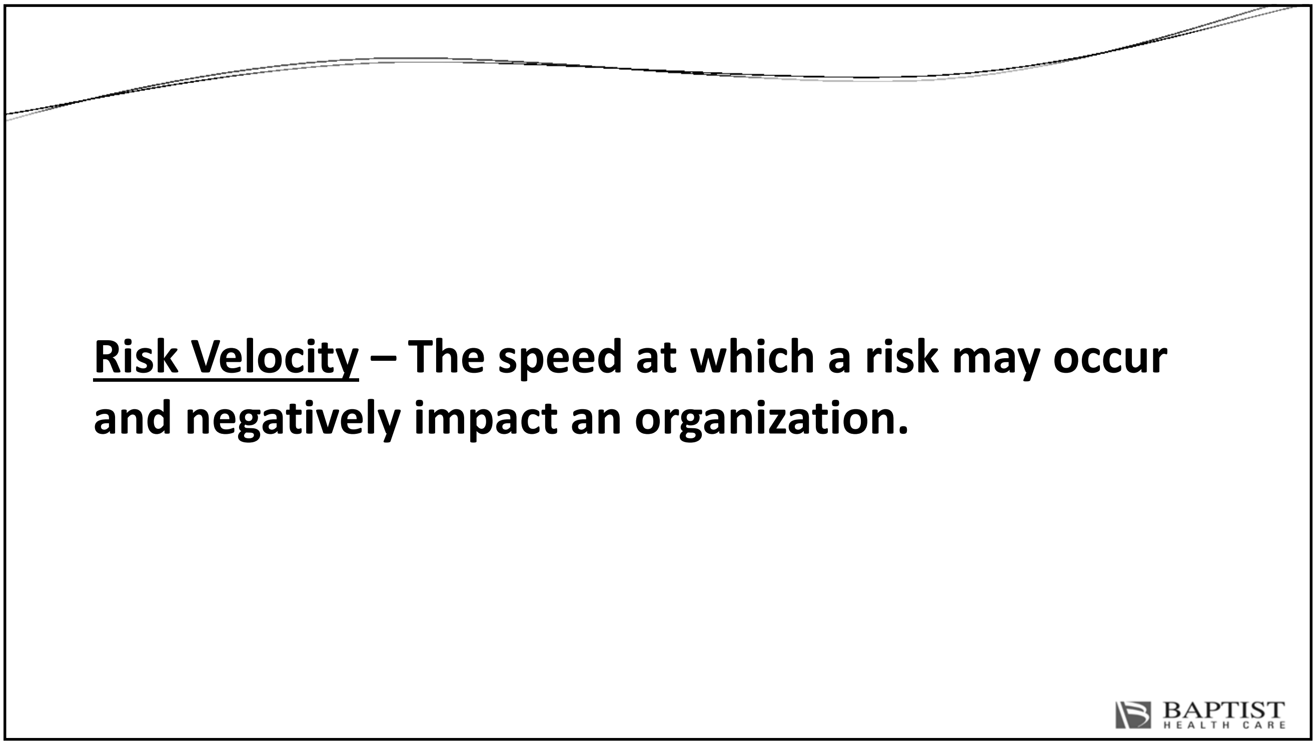
BAPTIST HEALTH CARE



Likelihood – a weighted factor based on subjective analysis of the probity that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities

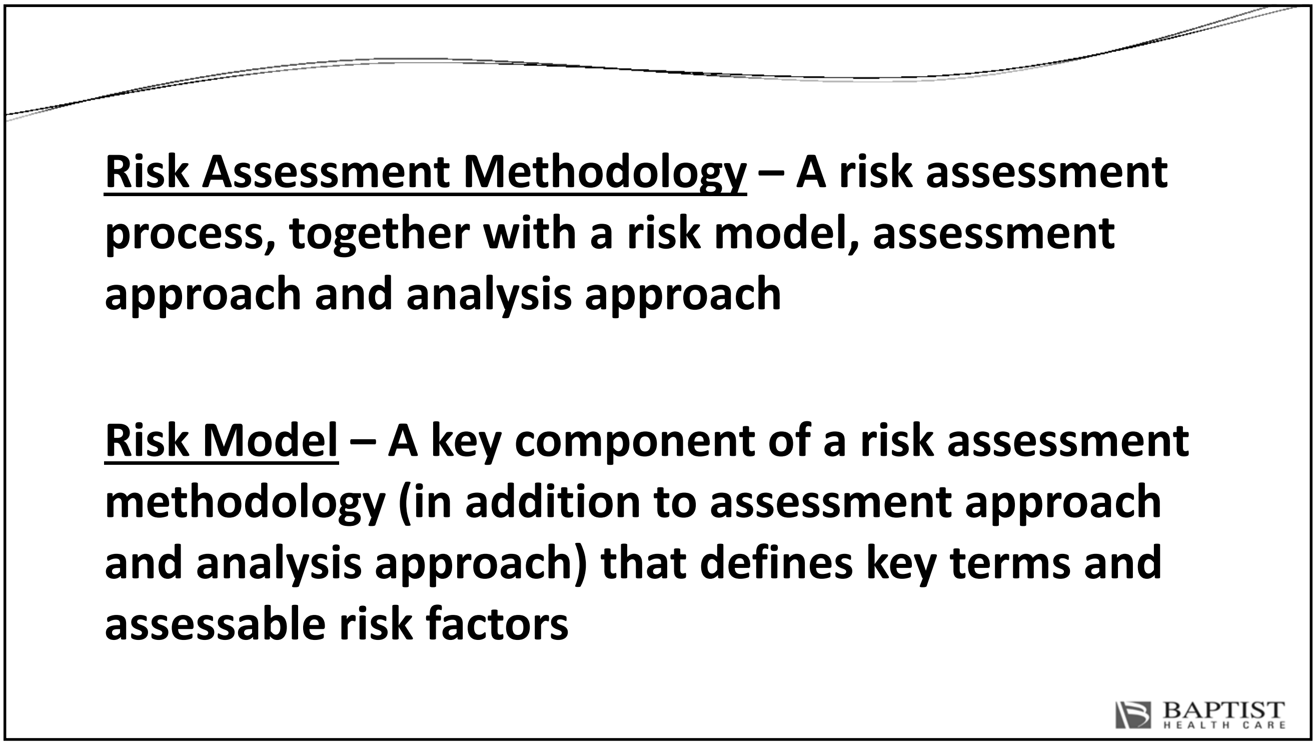
Impact – The level of harm that can be expected from an adverse event

BAPTIST HEALTH CARE



<u>Risk Velocity</u> – The speed at which a risk may occur and negatively impact an organization.

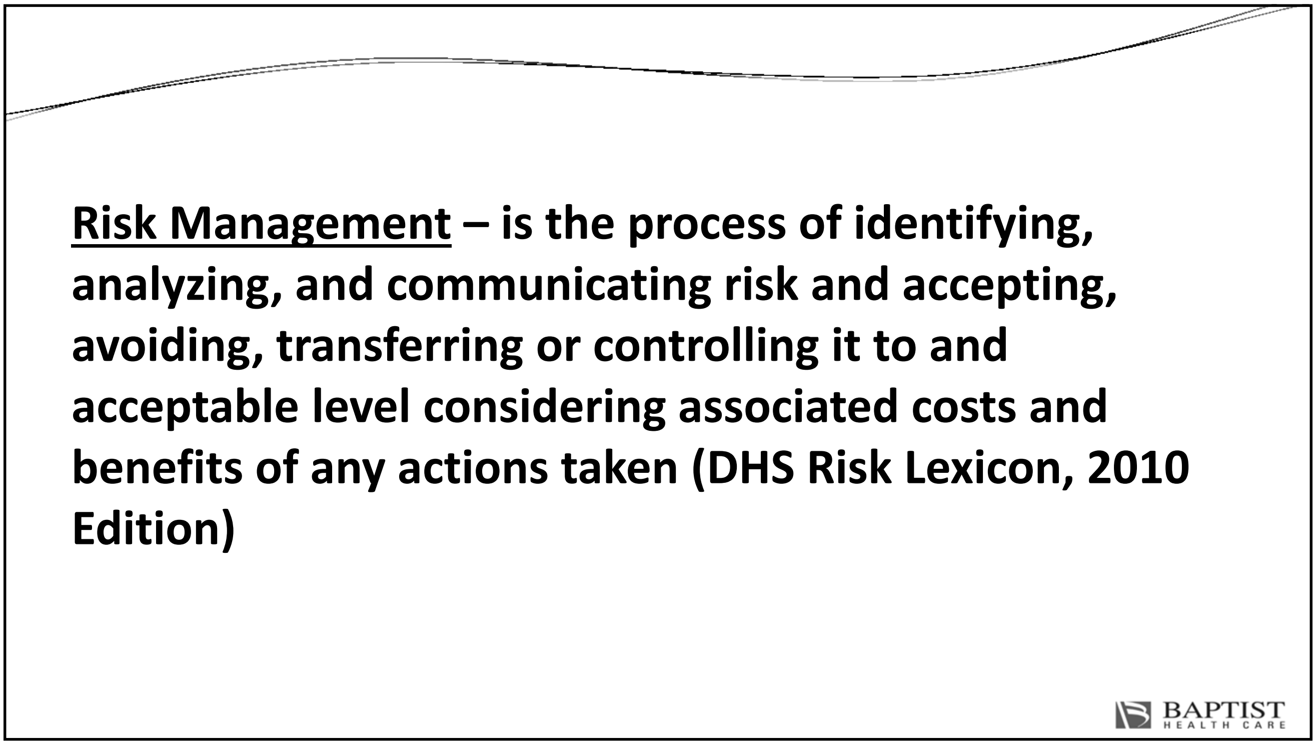
BAPTIST HEALTH CARE



<u>Risk Assessment Methodology</u> – A risk assessment process, together with a risk model, assessment approach and analysis approach

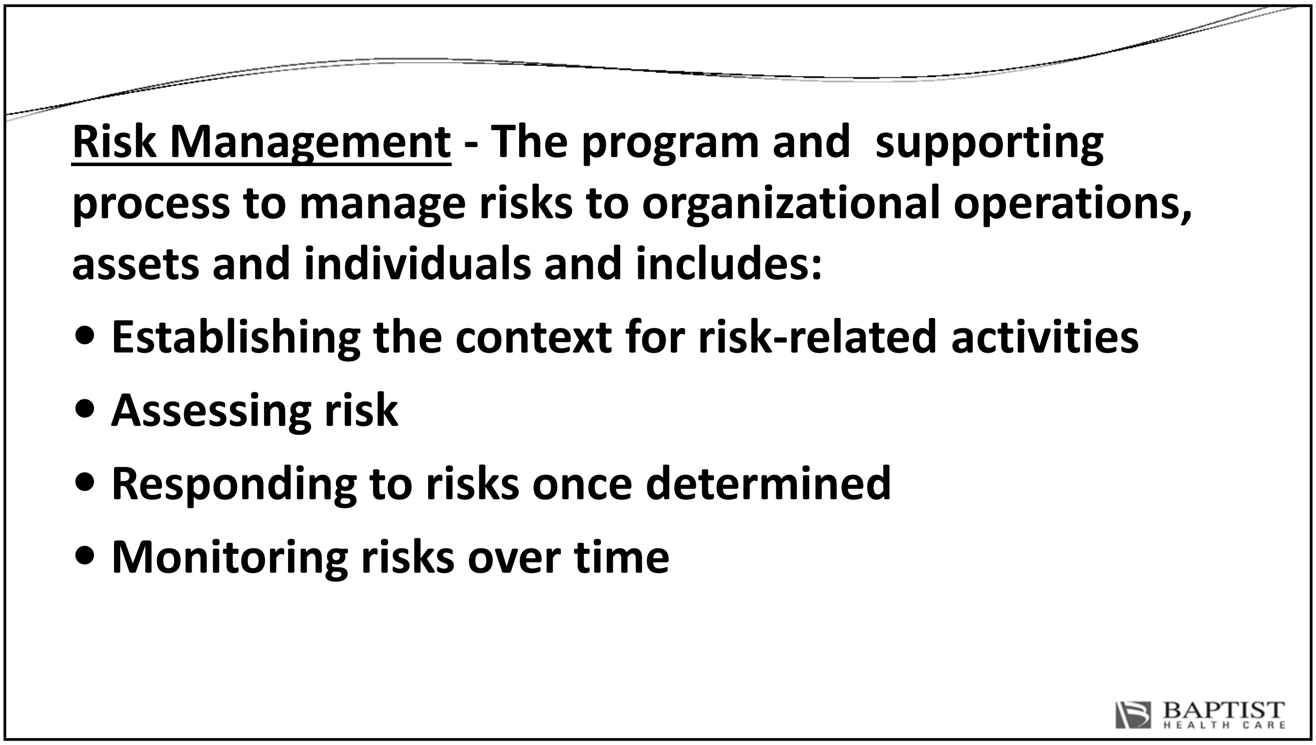
<u>Risk Model</u> – A key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors

BAPTIST HEALTH CARE



<u>Risk Management</u> – is the process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to and acceptable level considering associated costs and benefits of any actions taken (DHS Risk Lexicon, 2010 Edition)

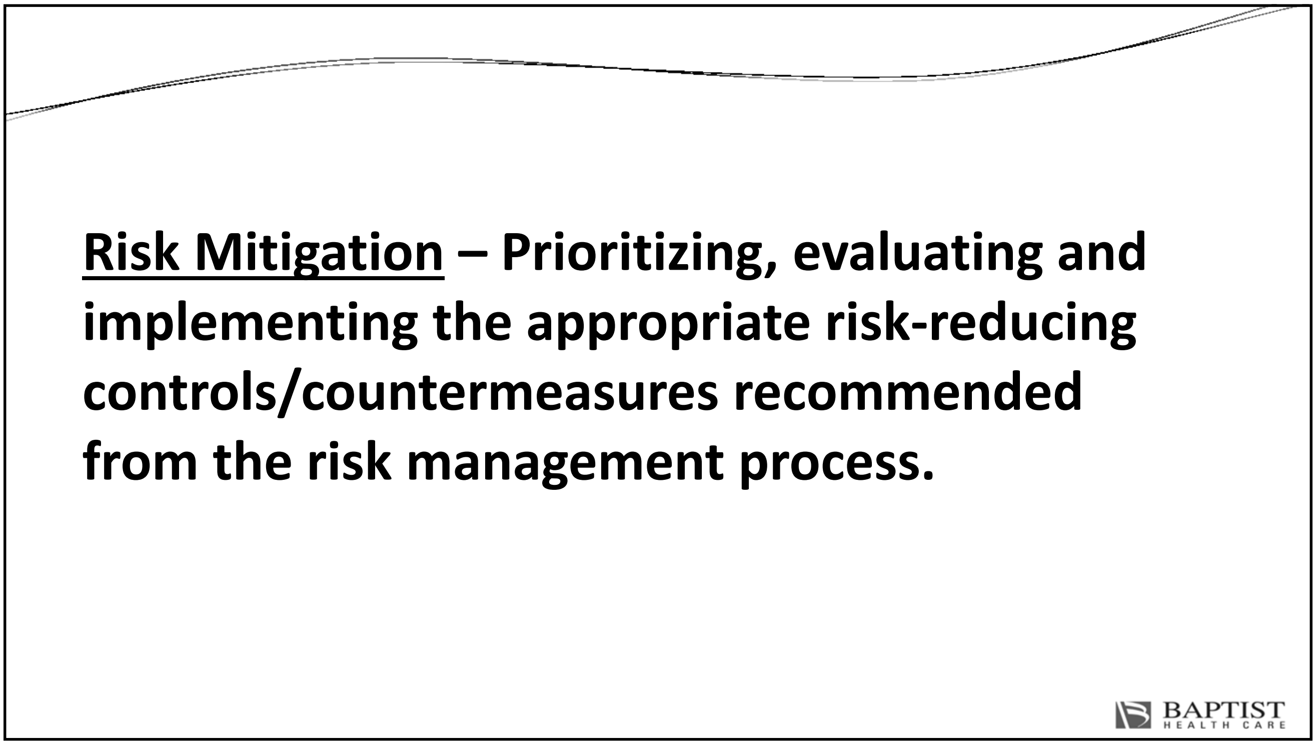
BAPTIST HEALTH CARE



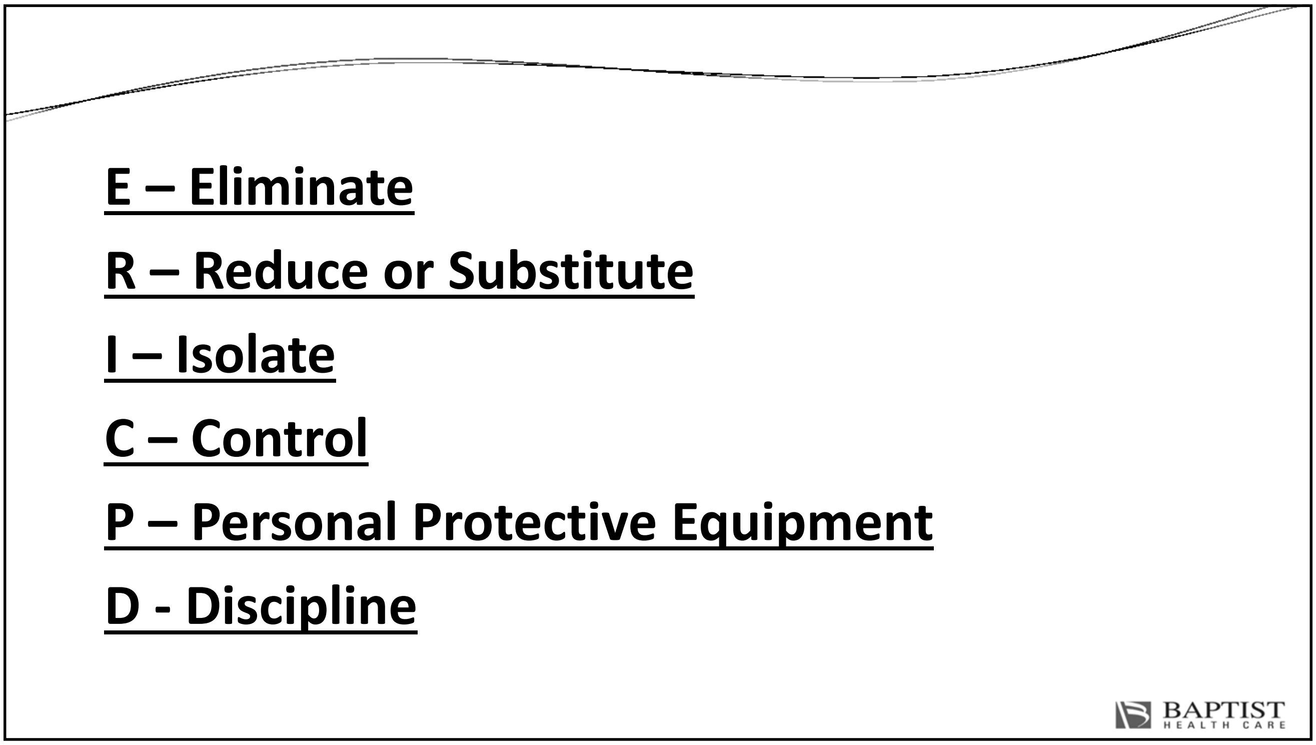
<u>Risk Management</u> - The program and supporting process to manage risks to organizational operations, assets and individuals and includes:

- Establishing the context for risk-related activities
- Assessing risk
- Responding to risks once determined
- Monitoring risks over time

BAPTIST HEALTH CARE



<u>Risk Mitigation</u> – Prioritizing, evaluating and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.



<u>E – Eliminate</u>

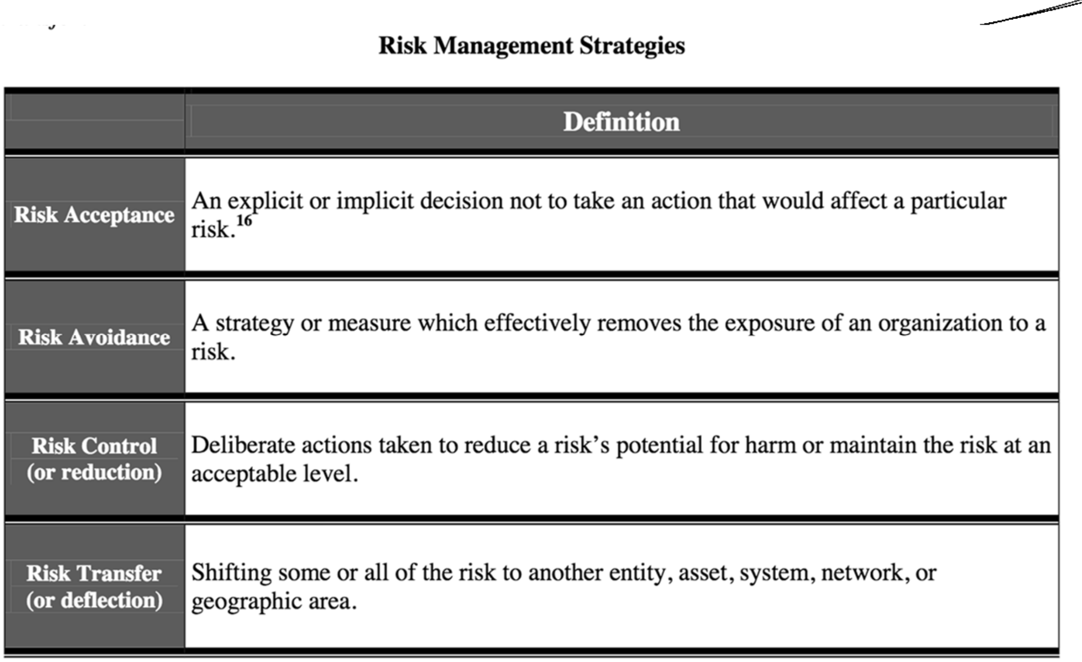
<u>R – Reduce or Substitute</u>

<u>I – Isolate</u>

<u>C – Control</u>

<u>P – Personal Protective Equipment</u>

<u>D - Discipline</u>



Risk Management Strategies

	Definition
Risk Acceptance	An explicit or implicit decision not to take an action that would affect a particular risk.[16]
Risk Avoidance	A strategy or measure which effectively removes the exposure of an organization to a risk.
Risk Control (or reduction)	Deliberate actions taken to reduce a risk's potential for harm or maintain the risk at an acceptable level.
Risk Transfer (or deflection)	Shifting some or all of the risk to another entity, asset, system, network, or geographic area.

Assessment Types

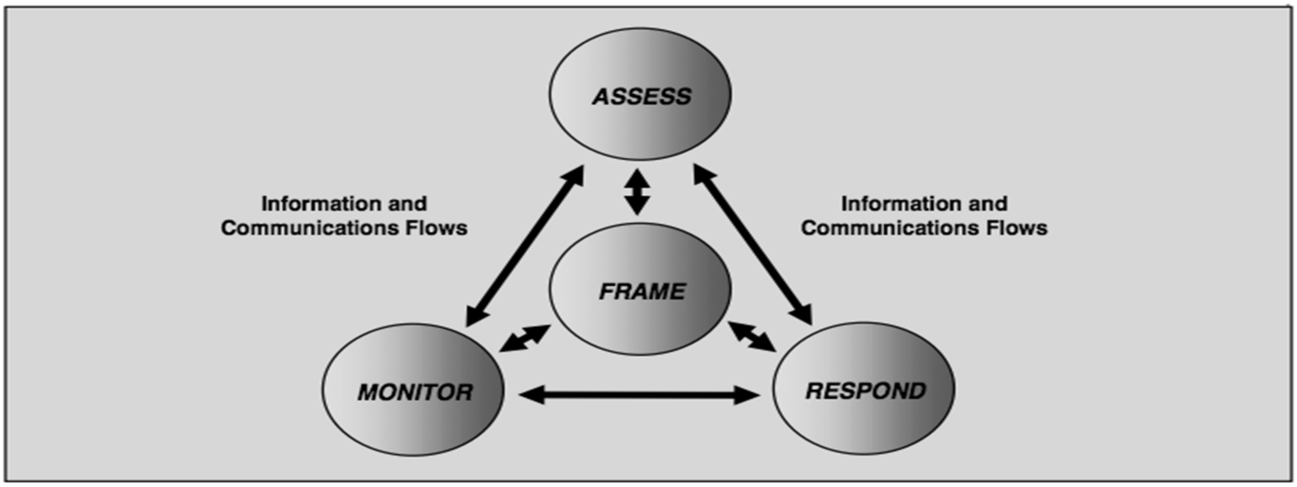
<u>Quantitative</u>– Based on numbers (0 – 100)

<u>Qualitative</u> – Based on nonnumeric categories or levels (very low, low, medium, high, very high,

<u>Simi-quantitative</u> – Uses bin, scales or representative numbers to communicate risk

(0-10, 11-20, 21-30, etc.)

Risk Management Process


ASSESS
FRAME
MONITOR
RESPOND
Information and Communications Flows
Information and Communications Flows

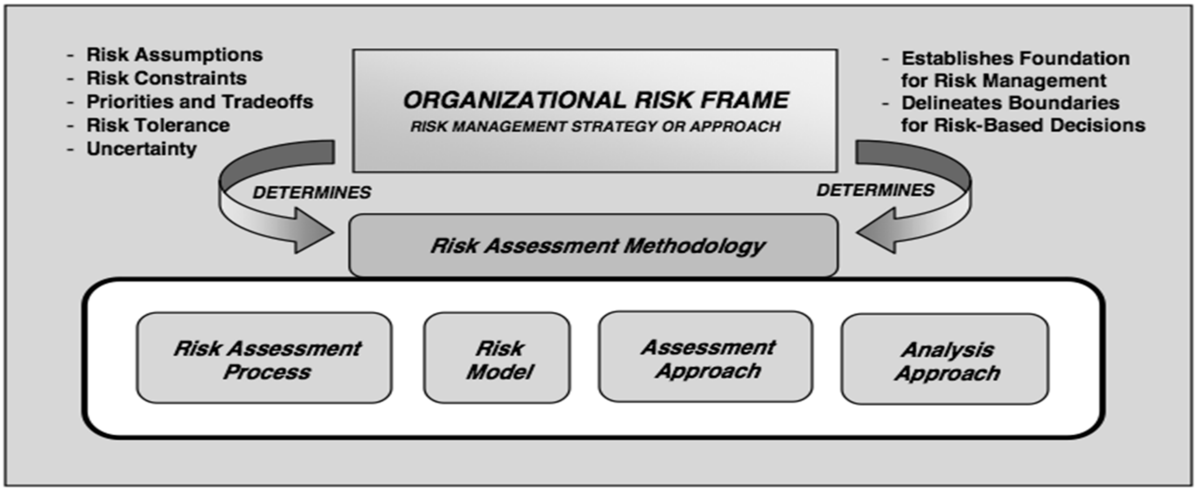
#1 - <u>Risk Management Framework</u> – Describes the environment in which risk-based decisions are made. Assess/Respond/Monitor - The organization's Risk Policy

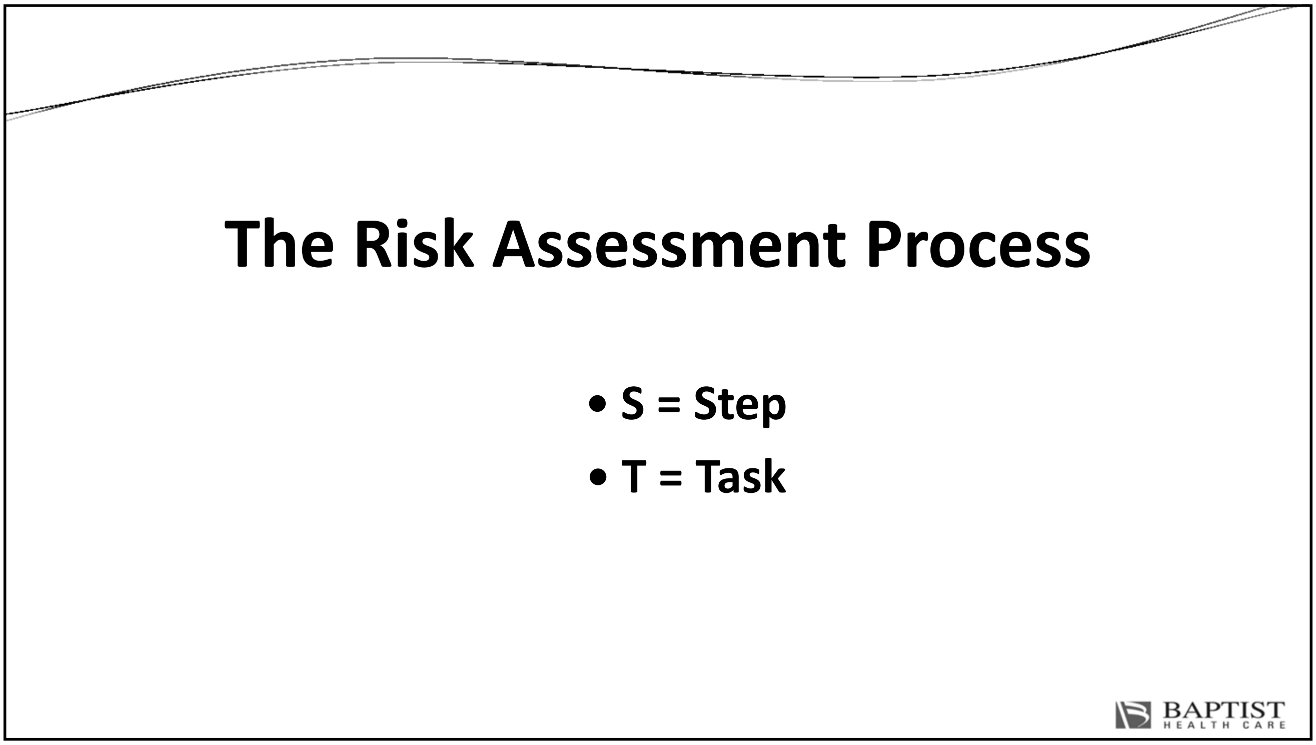
<u>#2 The Risk Assessment Process</u> – The process for assessing risk – How is it done within the organization’s Risk Framework?

#3 – Risk Response– Describes how the organization responds to risks once they have been identified in step #2.

#4 Monitoring Risk – Describes how the organization monitors risks over time and to determine effectiveness of risk mitigation. Helps determine if the risk framework is working as it should and provides feedback for 'tweaking' the framework.

Risk Framework Concept

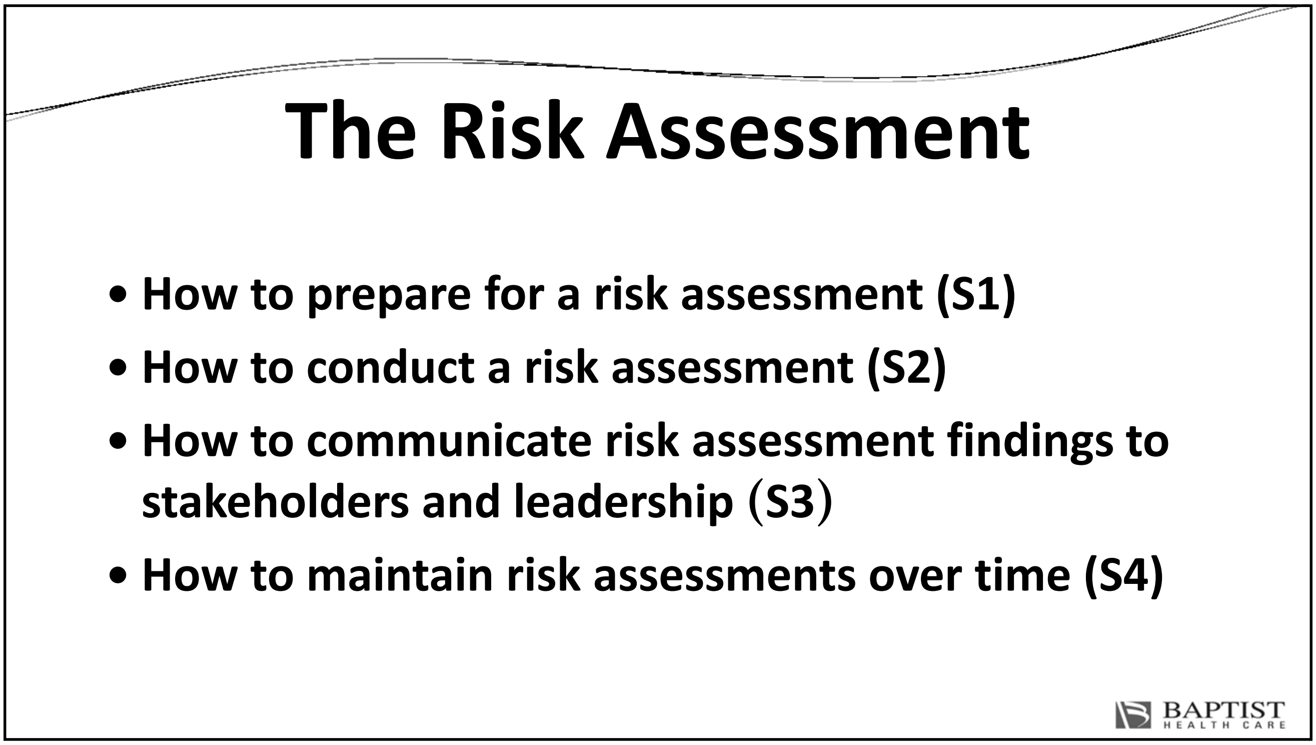

- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach



The Risk Assessment Process

- S = Step
- T = Task

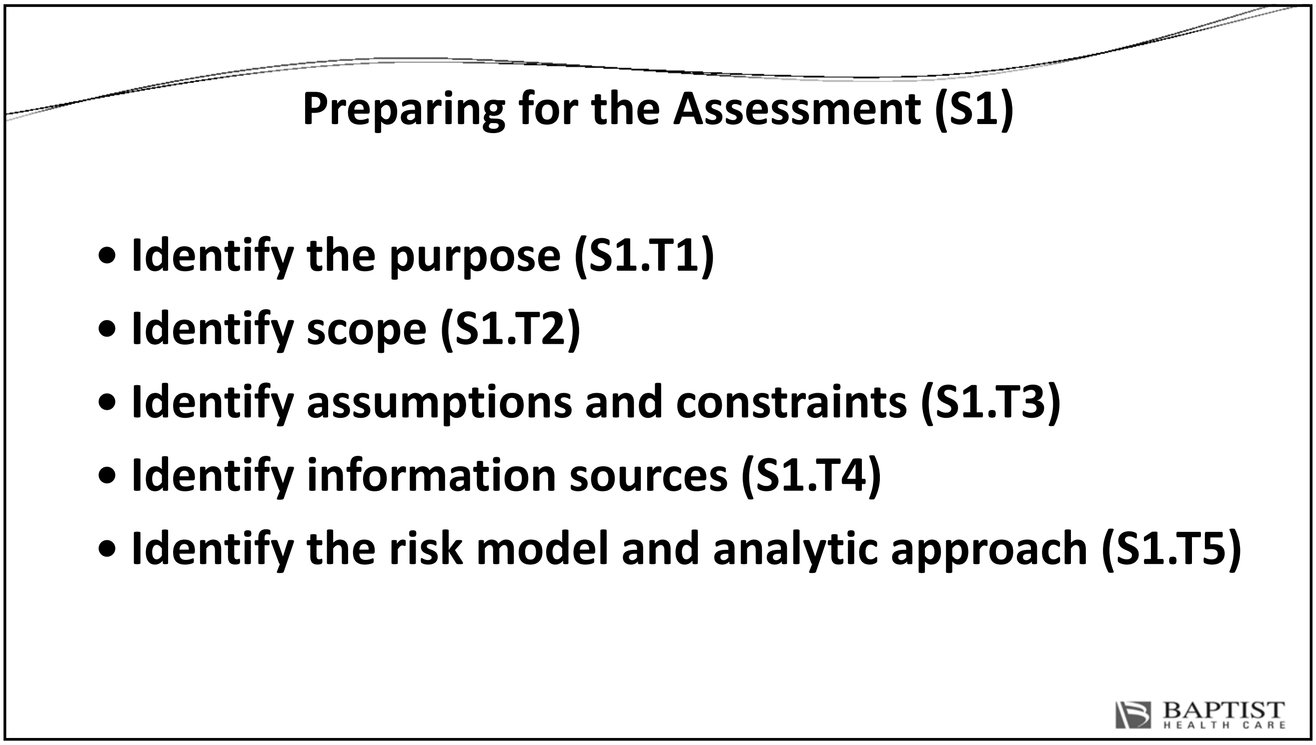
BAPTIST HEALTH CARE



The Risk Assessment

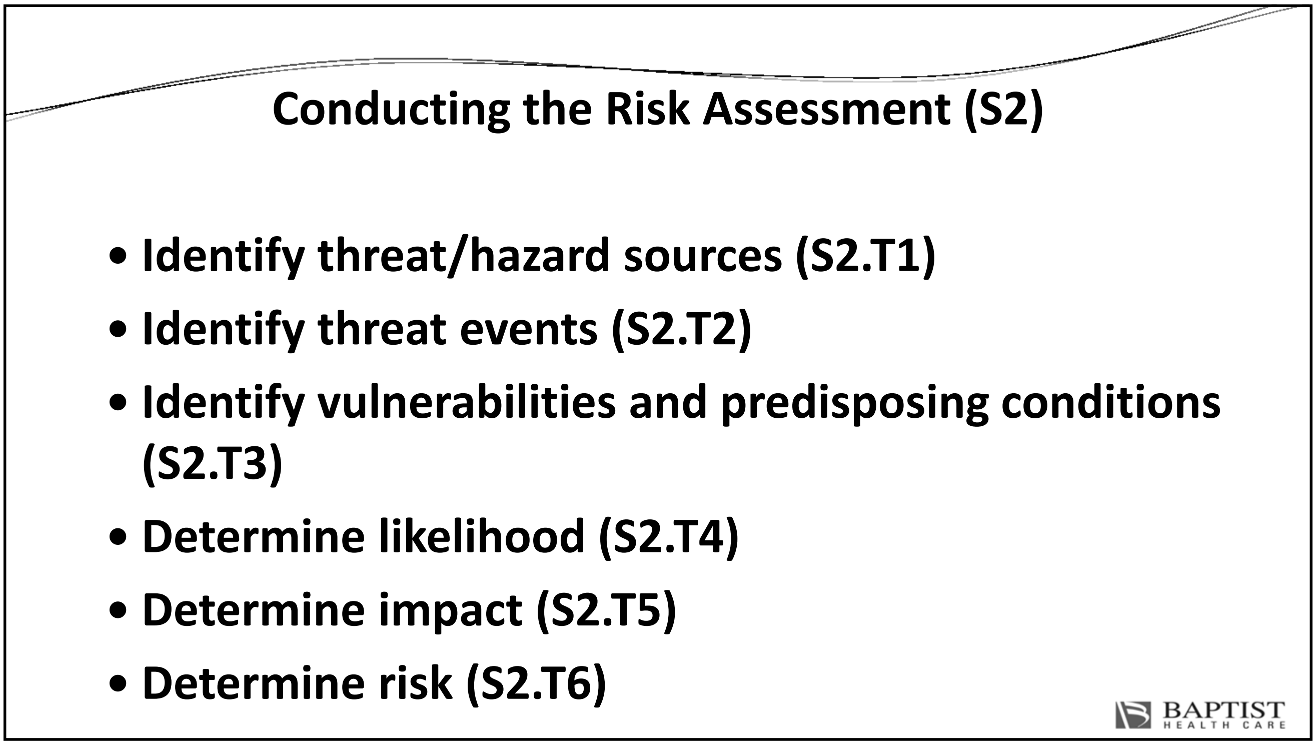
- How to prepare for a risk assessment (S1)
- How to conduct a risk assessment (S2)
- How to communicate risk assessment findings to stakeholders and leadership (S3)
- How to maintain risk assessments over time (S4)

BAPTIST HEALTH CARE



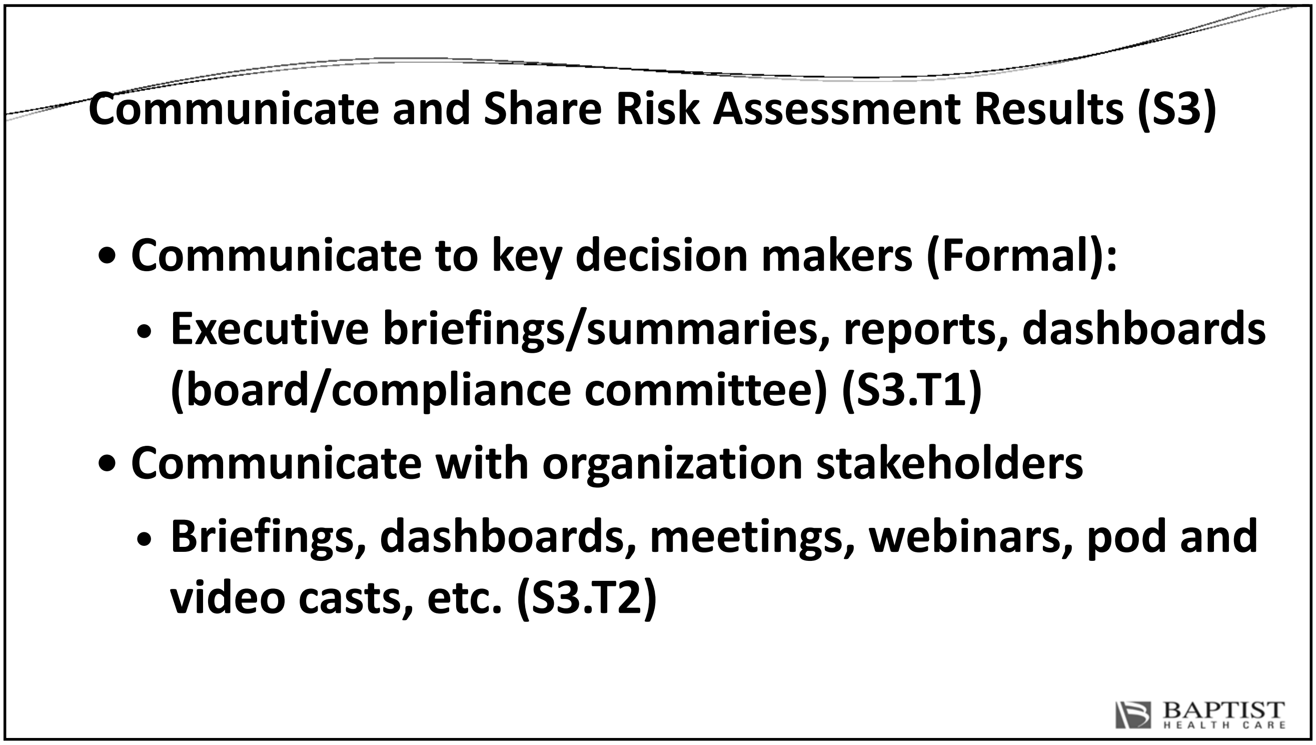
Preparing for the Assessment (S1)

- Identify the purpose (S1.T1)
- Identify scope (S1.T2)
- Identify assumptions and constraints (S1.T3)
- Identify information sources (S1.T4)
- Identify the risk model and analytic approach (S1.T5)



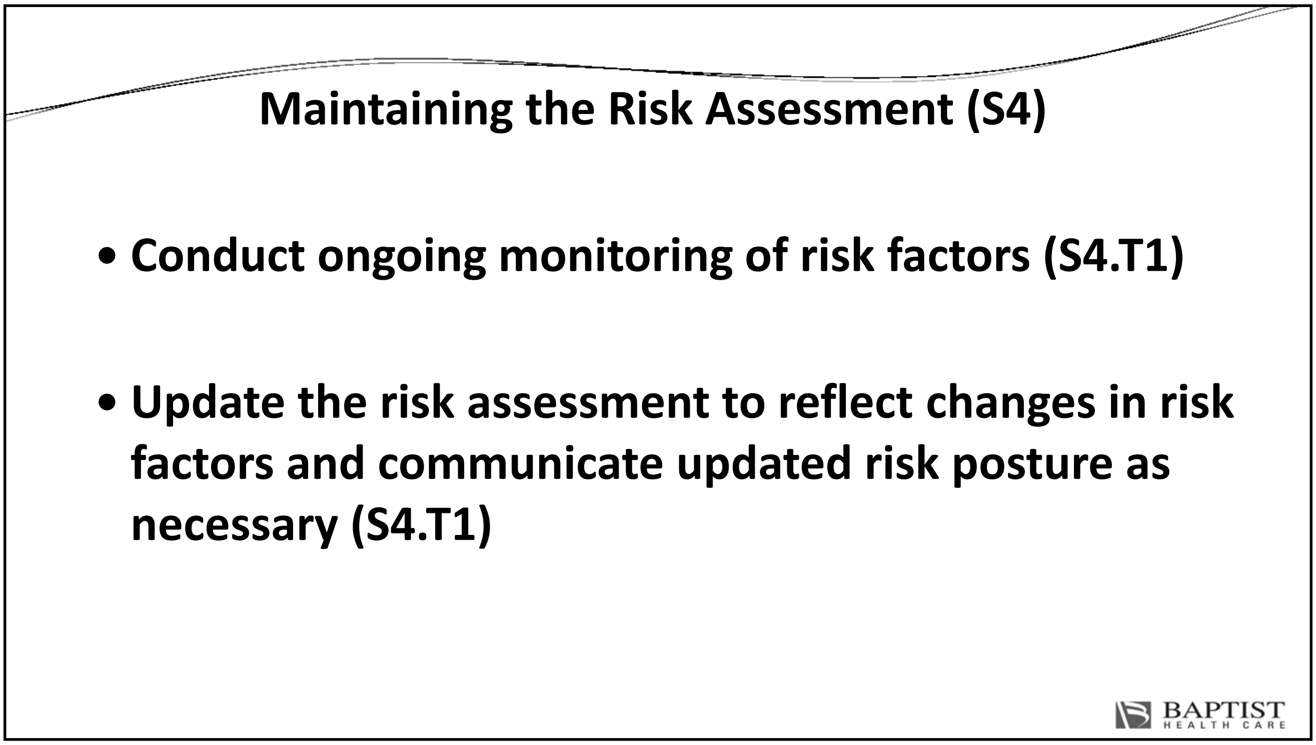
Conducting the Risk Assessment (S2)

- Identify threat/hazard sources (S2.T1)
- Identify threat events (S2.T2)
- Identify vulnerabilities and predisposing conditions (S2.T3)
- Determine likelihood (S2.T4)
- Determine impact (S2.T5)
- Determine risk (S2.T6)



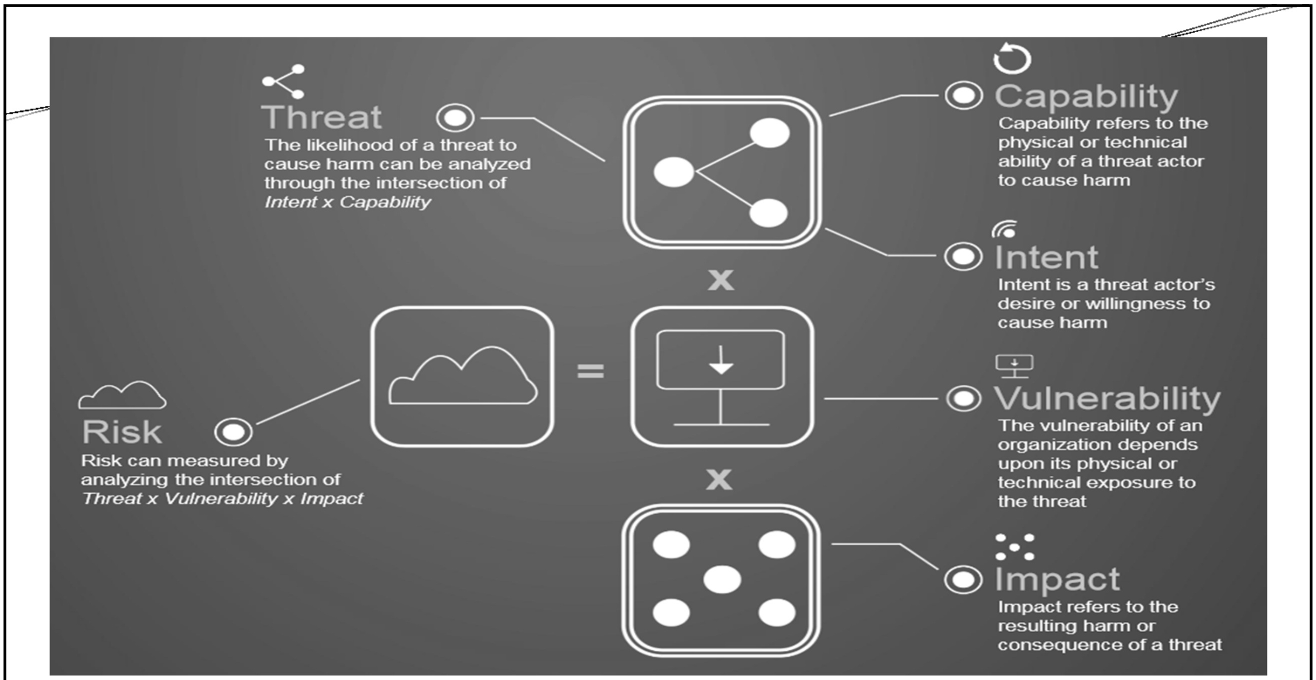
Communicate and Share Risk Assessment Results (S3)

- Communicate to key decision makers (Formal):
  - Executive briefings/summaries, reports, dashboards (board/compliance committee) (S3.T1)
- Communicate with organization stakeholders
  - Briefings, dashboards, meetings, webinars, pod and video casts, etc. (S3.T2)



Maintaining the Risk Assessment (S4)

- Conduct ongoing monitoring of risk factors (S4.T1)
- Update the risk assessment to reflect changes in risk factors and communicate updated risk posture as necessary (S4.T1)



Threat
The likelihood of a threat to cause harm can be analyzed through the intersection of *Intent x Capability*

Capability
Capability refers to the physical or technical ability of a threat actor to cause harm

Intent
Intent is a threat actor's desire or willingness to cause harm

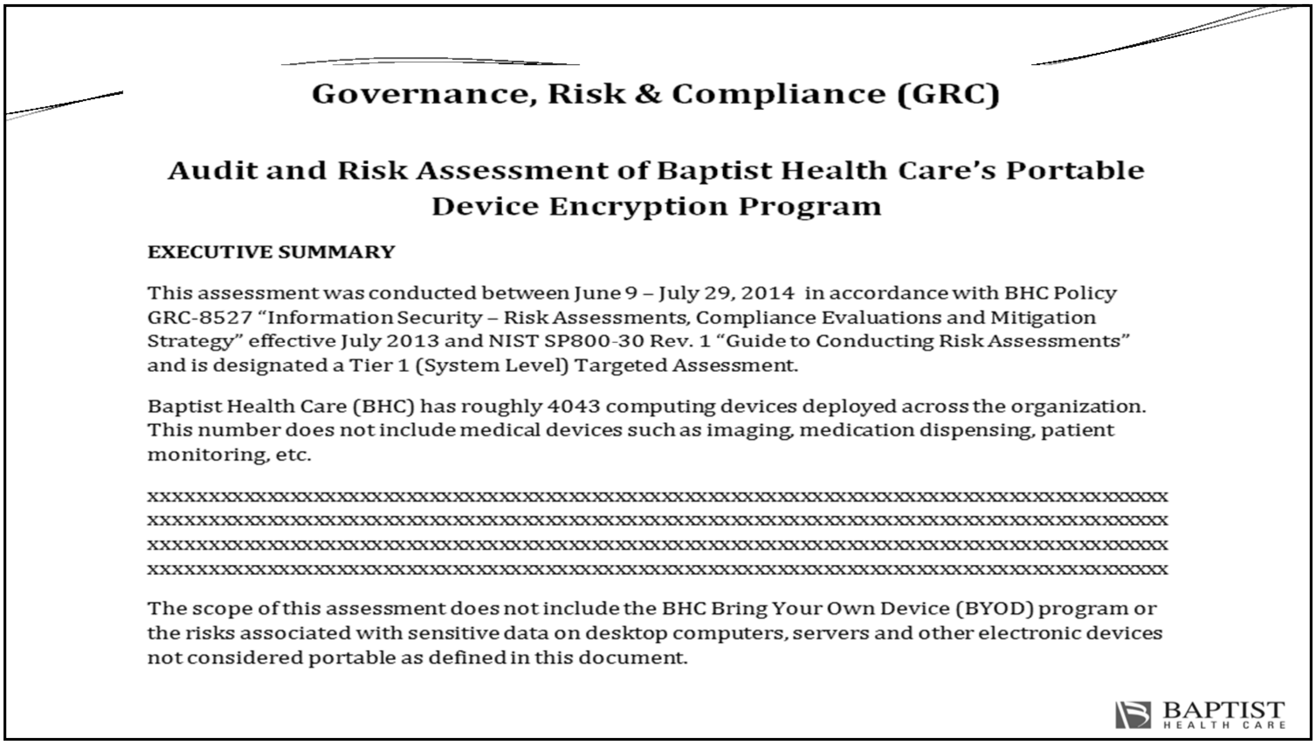
Risk
Risk can measured by analyzing the intersection of *Threat x Vulnerability x Impact*

Vulnerability
The vulnerability of an organization depends upon its physical or technical exposure to the threat

Impact
Impact refers to the resulting harm or consequence of a threat

Source: U.S. Department of State - OSAC

Example Assessment



Governance, Risk & Compliance (GRC)

Audit and Risk Assessment of Baptist Health Care's Portable Device Encryption Program

EXECUTIVE SUMMARY

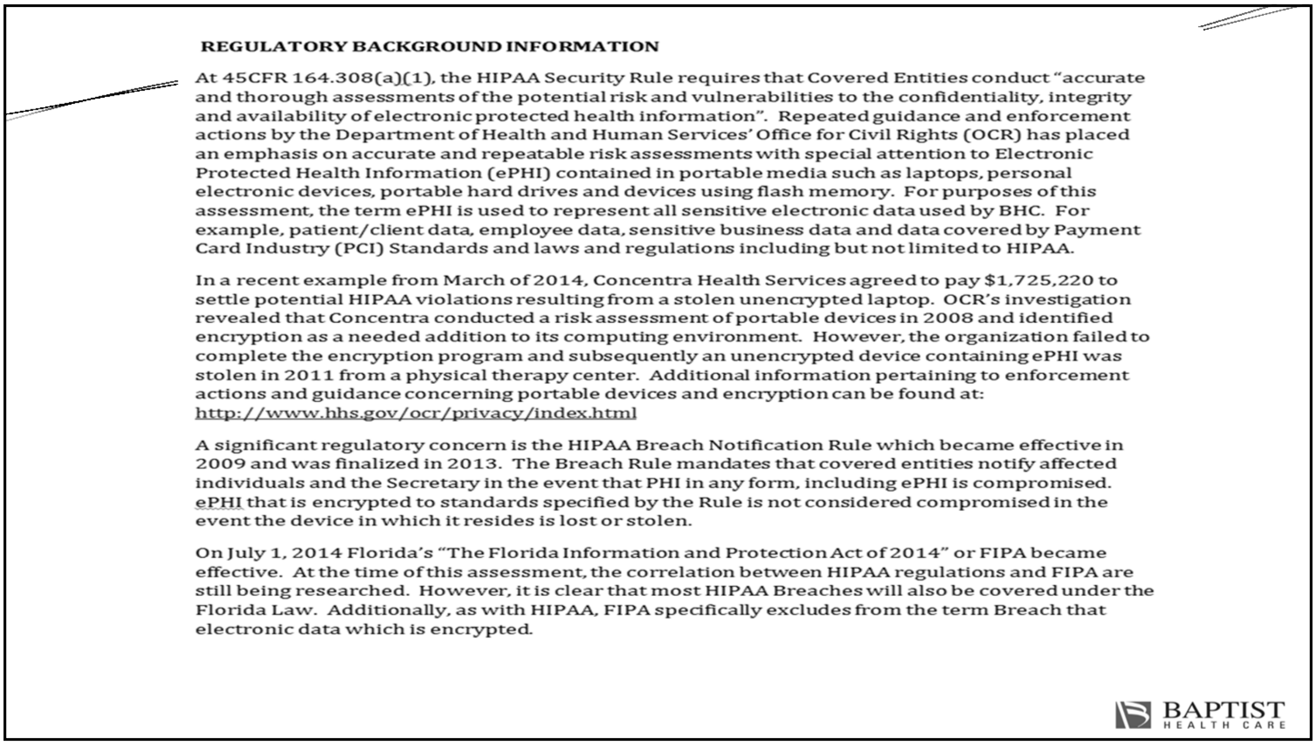
This assessment was conducted between June 9 – July 29, 2014 in accordance with BHC Policy GRC-8527 "Information Security – Risk Assessments, Compliance Evaluations and Mitigation Strategy" effective July 2013 and NIST SP800-30 Rev. 1 "Guide to Conducting Risk Assessments" and is designated a Tier 1 (System Level) Targeted Assessment.

Baptist Health Care (BHC) has roughly 4043 computing devices deployed across the organization. This number does not include medical devices such as imaging, medication dispensing, patient monitoring, etc.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

The scope of this assessment does not include the BHC Bring Your Own Device (BYOD) program or the risks associated with sensitive data on desktop computers, servers and other electronic devices not considered portable as defined in this document.

BAPTIST HEALTH CARE



REGULATORY BACKGROUND INFORMATION

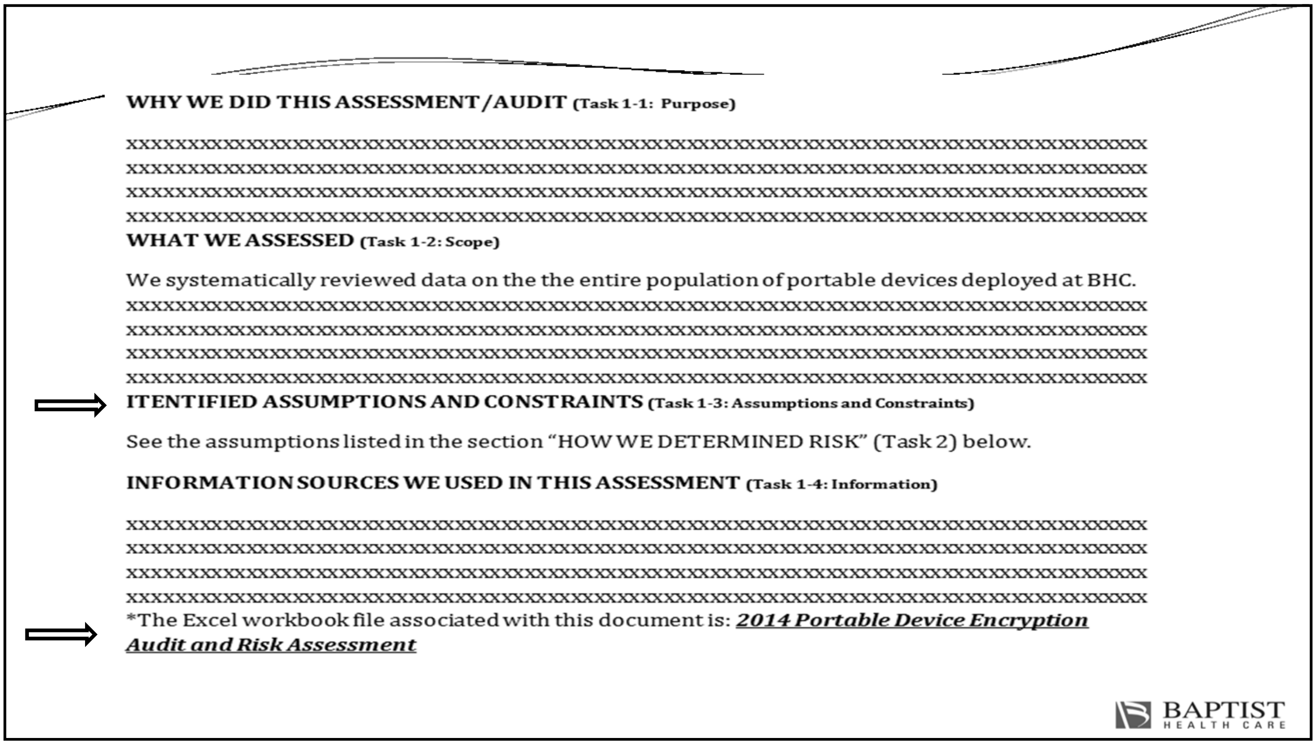
At 45CFR 164.308(a)(1), the HIPAA Security Rule requires that Covered Entities conduct "accurate and thorough assessments of the potential risk and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information". Repeated guidance and enforcement actions by the Department of Health and Human Services' Office for Civil Rights (OCR) has placed an emphasis on accurate and repeatable risk assessments with special attention to Electronic Protected Health Information (ePHI) contained in portable media such as laptops, personal electronic devices, portable hard drives and devices using flash memory. For purposes of this assessment, the term ePHI is used to represent all sensitive electronic data used by BHC. For example, patient/client data, employee data, sensitive business data and data covered by Payment Card Industry (PCI) Standards and laws and regulations including but not limited to HIPAA.

In a recent example from March of 2014, Concentra Health Services agreed to pay $1,725,220 to settle potential HIPAA violations resulting from a stolen unencrypted laptop. OCR's investigation revealed that Concentra conducted a risk assessment of portable devices in 2008 and identified encryption as a needed addition to its computing environment. However, the organization failed to complete the encryption program and subsequently an unencrypted device containing ePHI was stolen in 2011 from a physical therapy center. Additional information pertaining to enforcement actions and guidance concerning portable devices and encryption can be found at: http://www.hhs.gov/ocr/privacy/index.html

A significant regulatory concern is the HIPAA Breach Notification Rule which became effective in 2009 and was finalized in 2013. The Breach Rule mandates that covered entities notify affected individuals and the Secretary in the event that PHI in any form, including ePHI is compromised. ePHI that is encrypted to standards specified by the Rule is not considered compromised in the event the device in which it resides is lost or stolen.

On July 1, 2014 Florida's "The Florida Information and Protection Act of 2014" or FIPA became effective. At the time of this assessment, the correlation between HIPAA regulations and FIPA are still being researched. However, it is clear that most HIPAA Breaches will also be covered under the Florida Law. Additionally, as with HIPAA, FIPA specifically excludes from the term Breach that electronic data which is encrypted.

BAPTIST HEALTH CARE



WHY WE DID THIS ASSESSMENT/AUDIT (Task 1-1: Purpose)

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

WHAT WE ASSESSED (Task 1-2: Scope)

We systematically reviewed data on the the entire population of portable devices deployed at BHC.
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

⇒ **ITENTIFIED ASSUMPTIONS AND CONSTRAINTS (Task 1-3: Assumptions and Constraints)**

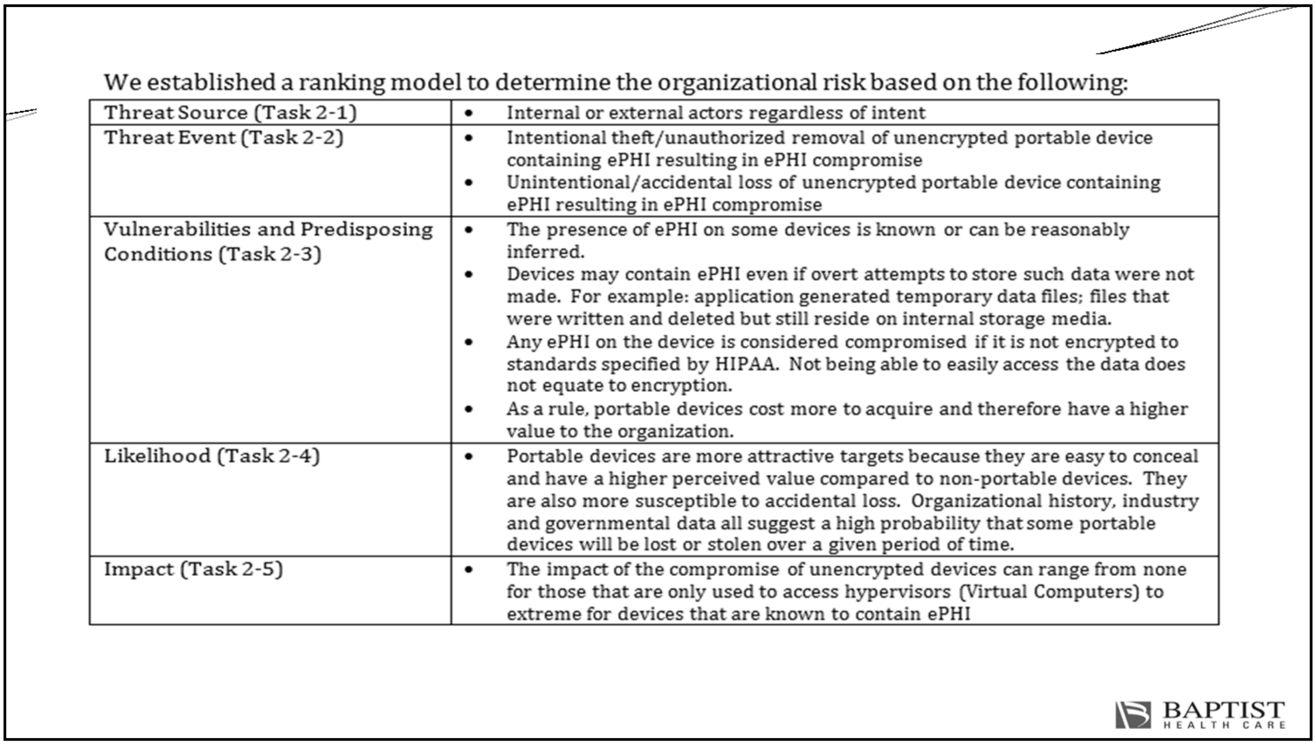
See the assumptions listed in the section “HOW WE DETERMINED RISK” (Task 2) below.

INFORMATION SOURCES WE USED IN THIS ASSESSMENT (Task 1-4: Information)

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

⇒ *The Excel workbook file associated with this document is: ***2014 Portable Device Encryption Audit and Risk Assessment***

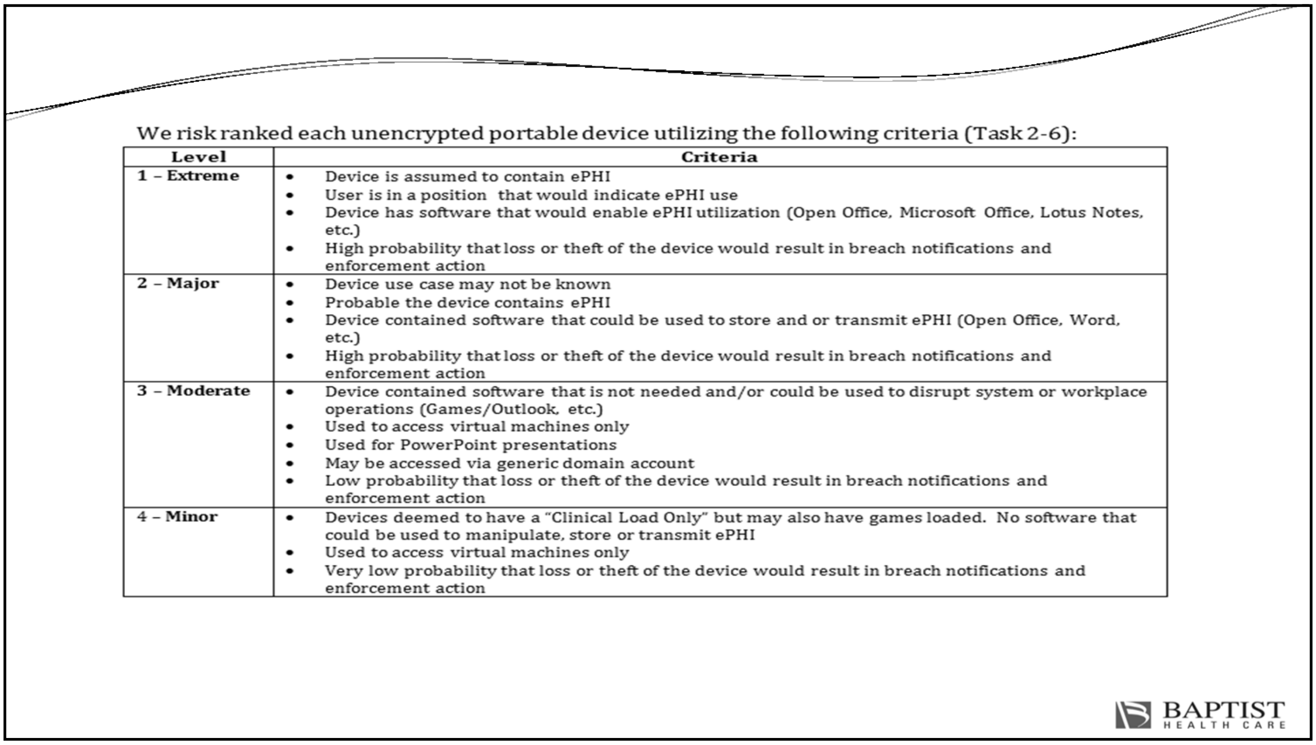
BAPTIST HEALTH CARE



We established a ranking model to determine the organizational risk based on the following:

Threat Source (Task 2-1)	• Internal or external actors regardless of intent
Threat Event (Task 2-2)	• Intentional theft/unauthorized removal of unencrypted portable device containing ePHI resulting in ePHI compromise • Unintentional/accidental loss of unencrypted portable device containing ePHI resulting in ePHI compromise
Vulnerabilities and Predisposing Conditions (Task 2-3)	• The presence of ePHI on some devices is known or can be reasonably inferred. • Devices may contain ePHI even if overt attempts to store such data were not made. For example: application generated temporary data files; files that were written and deleted but still reside on internal storage media. • Any ePHI on the device is considered compromised if it is not encrypted to standards specified by HIPAA. Not being able to easily access the data does not equate to encryption. • As a rule, portable devices cost more to acquire and therefore have a higher value to the organization.
Likelihood (Task 2-4)	• Portable devices are more attractive targets because they are easy to conceal and have a higher perceived value compared to non-portable devices. They are also more susceptible to accidental loss. Organizational history, industry and governmental data all suggest a high probability that some portable devices will be lost or stolen over a given period of time.
Impact (Task 2-5)	• The impact of the compromise of unencrypted devices can range from none for those that are only used to access hypervisors (Virtual Computers) to extreme for devices that are known to contain ePHI

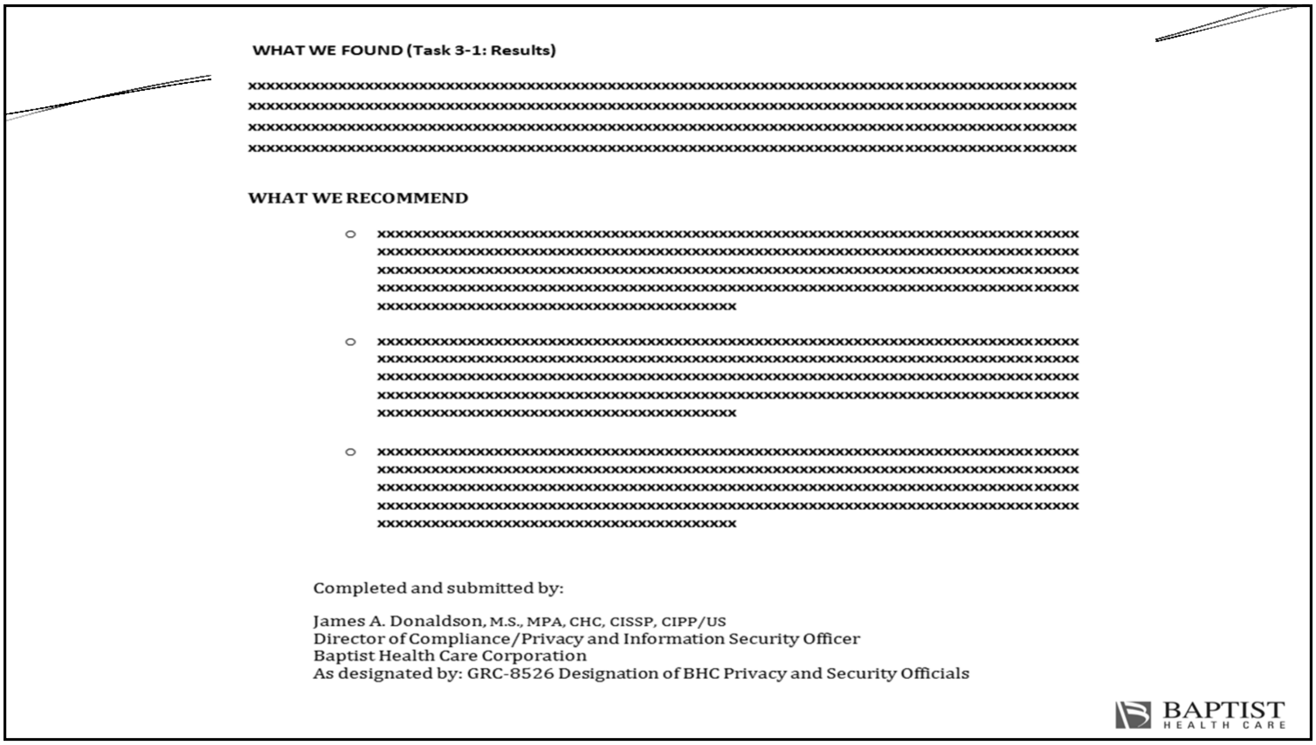
BAPTIST HEALTH CARE



We risk ranked each unencrypted portable device utilizing the following criteria (Task 2-6):

Level	Criteria
1 – Extreme	• Device is assumed to contain ePHI • User is in a position that would indicate ePHI use • Device has software that would enable ePHI utilization (Open Office, Microsoft Office, Lotus Notes, etc.) • High probability that loss or theft of the device would result in breach notifications and enforcement action
2 – Major	• Device use case may not be known • Probable the device contains ePHI • Device contained software that could be used to store and or transmit ePHI (Open Office, Word, etc.) • High probability that loss or theft of the device would result in breach notifications and enforcement action
3 – Moderate	• Device contained software that is not needed and/or could be used to disrupt system or workplace operations (Games/Outlook, etc.) • Used to access virtual machines only • Used for PowerPoint presentations • May be accessed via generic domain account • Low probability that loss or theft of the device would result in breach notifications and enforcement action
4 – Minor	• Devices deemed to have a "Clinical Load Only" but may also have games loaded. No software that could be used to manipulate, store or transmit ePHI • Used to access virtual machines only • Very low probability that loss or theft of the device would result in breach notifications and enforcement action

BAPTIST HEALTH CARE



WHAT WE FOUND (Task 3-1: Results)

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

WHAT WE RECOMMEND

○ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

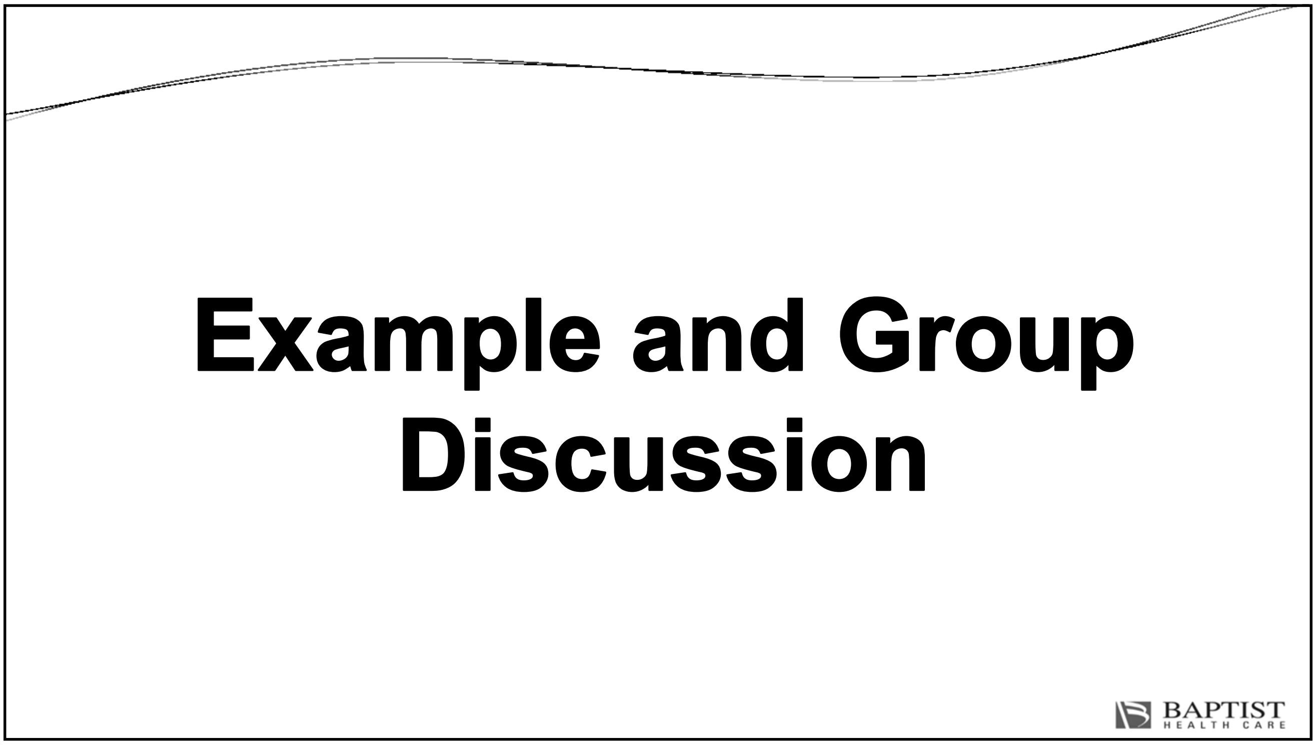
○ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

○ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

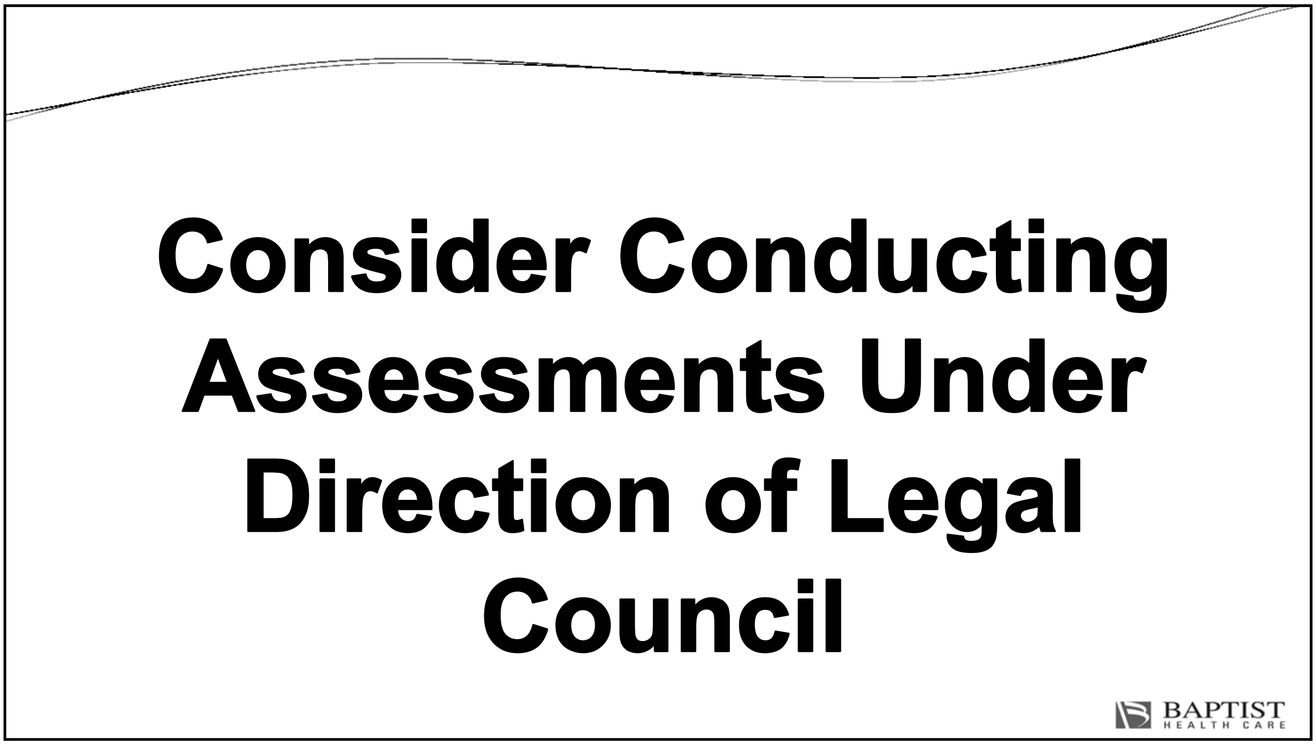
Completed and submitted by:

James A. Donaldson, M.S., MPA, CHC, CISSP, CIPP/US
Director of Compliance/Privacy and Information Security Officer
Baptist Health Care Corporation
As designated by: GRC-8526 Designation of BHC Privacy and Security Officials

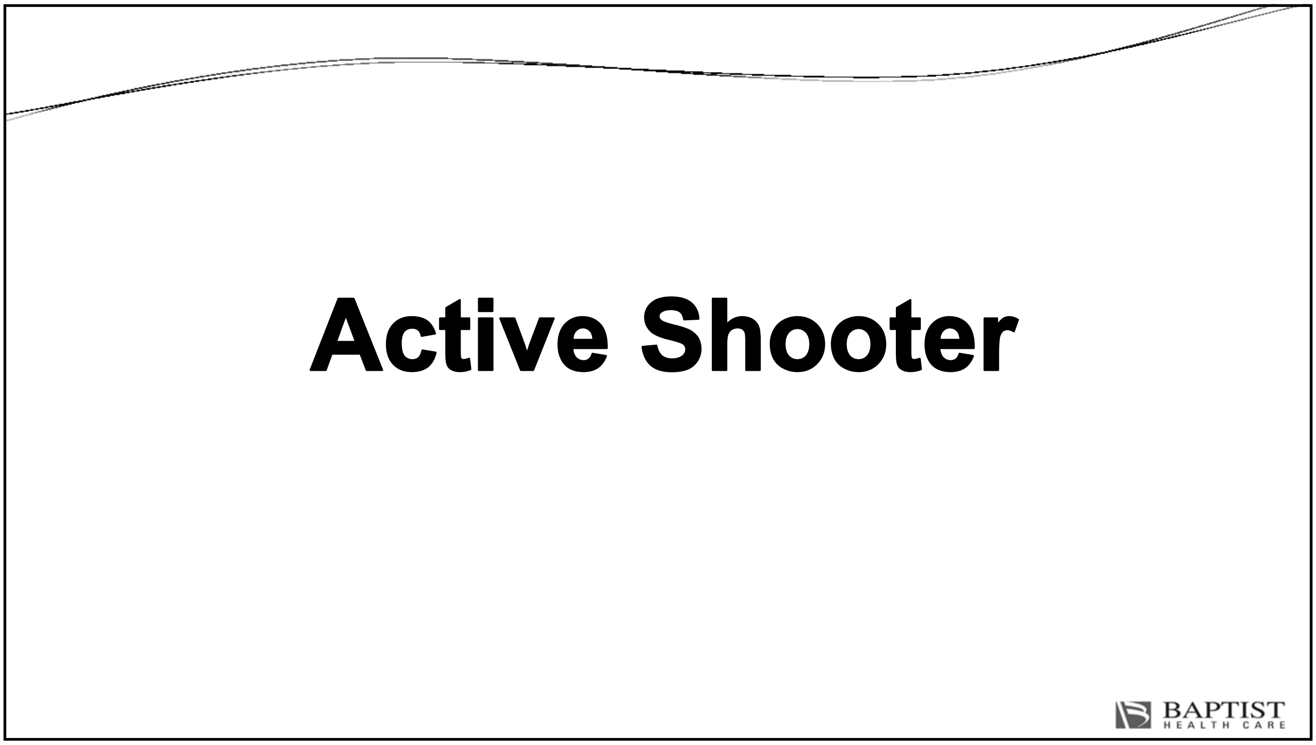
BAPTIST HEALTH CARE



Example and Group Discussion

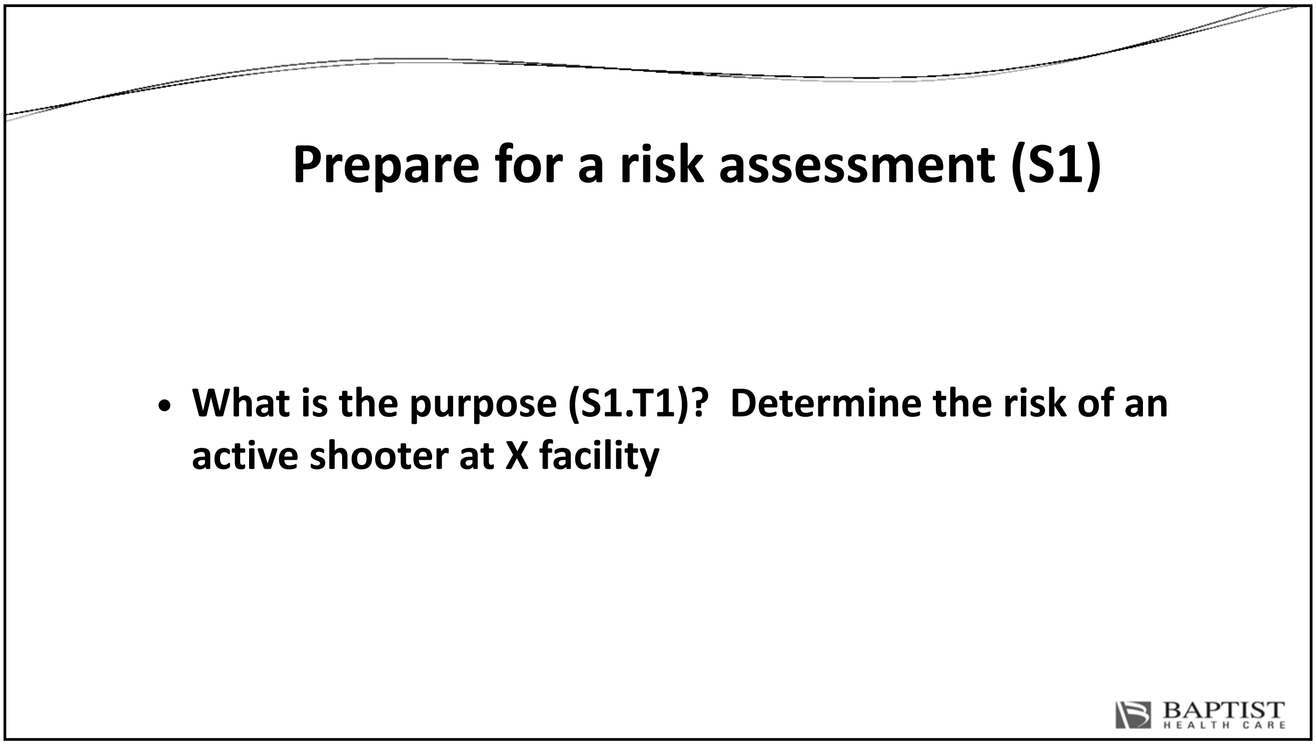


Consider Conducting Assessments Under Direction of Legal Council



Active Shooter

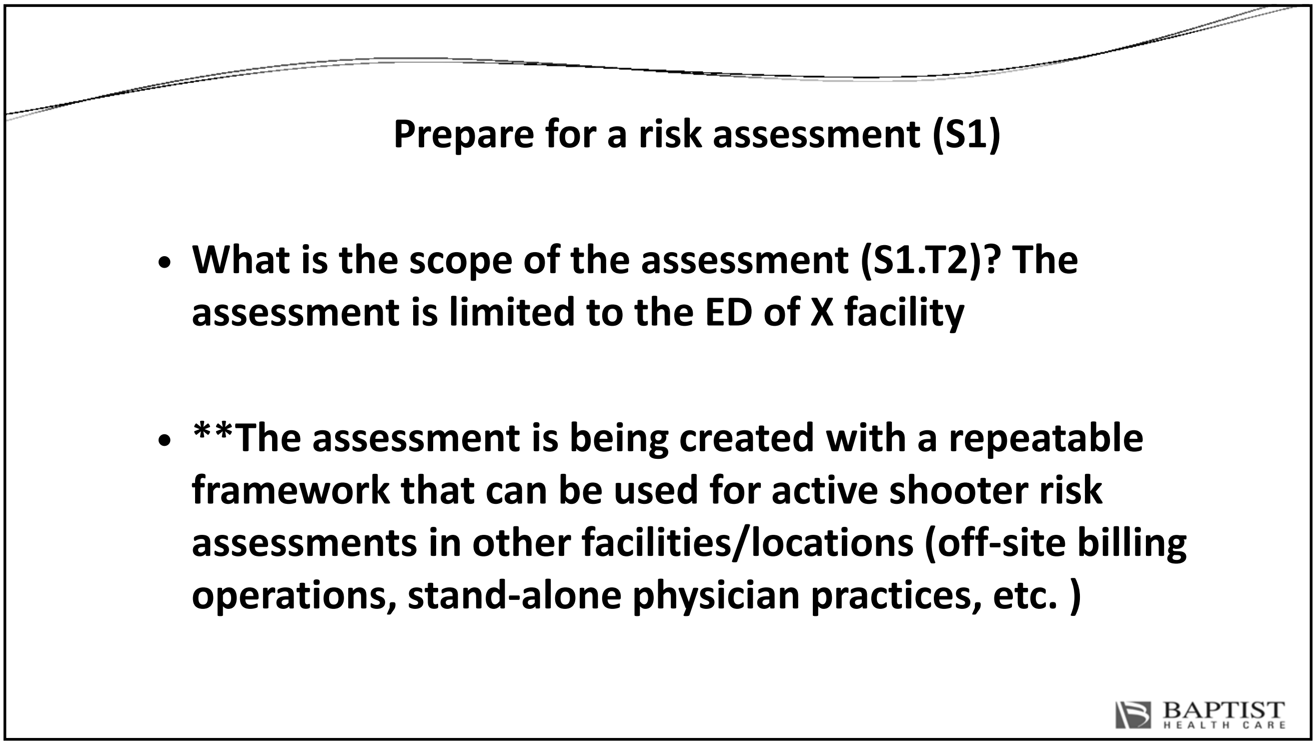
BAPTIST HEALTH CARE



Prepare for a risk assessment (S1)

- **What is the purpose (S1.T1)? Determine the risk of an active shooter at X facility**

BAPTIST HEALTH CARE

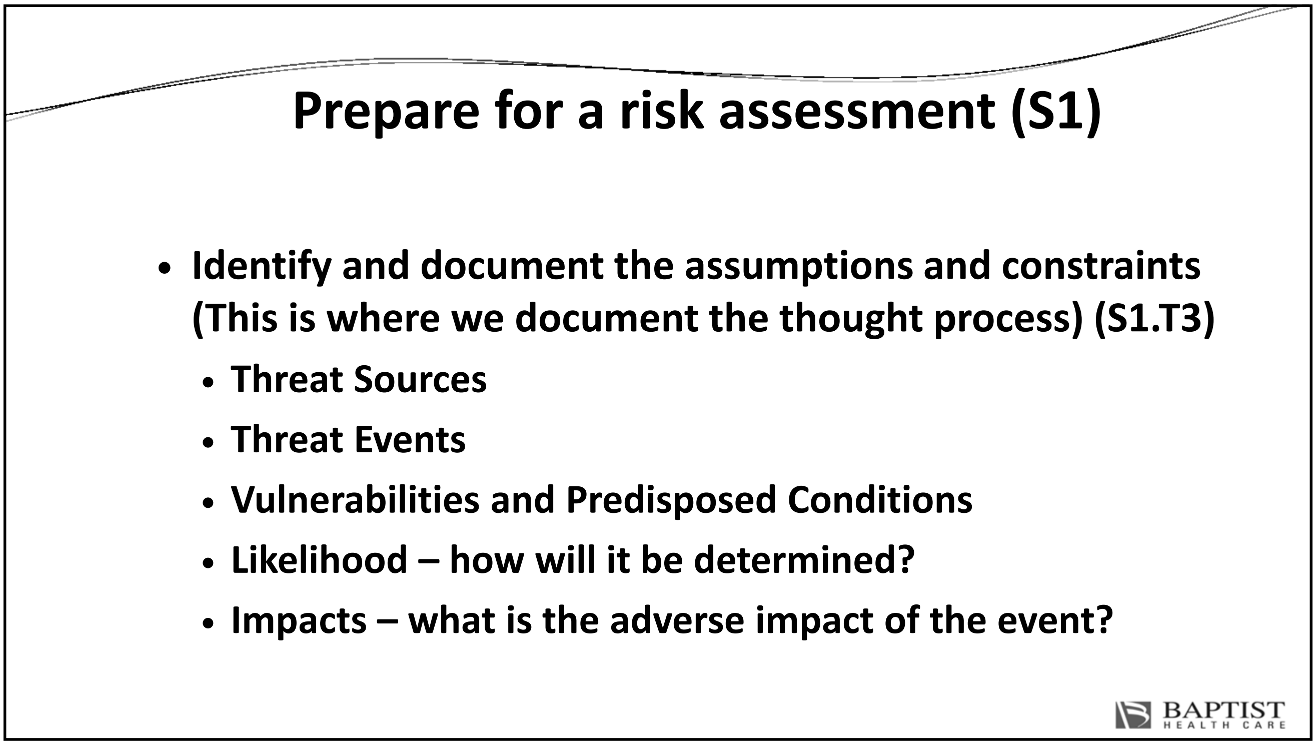


Prepare for a risk assessment (S1)

- What is the scope of the assessment (S1.T2)? The assessment is limited to the ED of X facility

- **The assessment is being created with a repeatable framework that can be used for active shooter risk assessments in other facilities/locations (off-site billing operations, stand-alone physician practices, etc.)

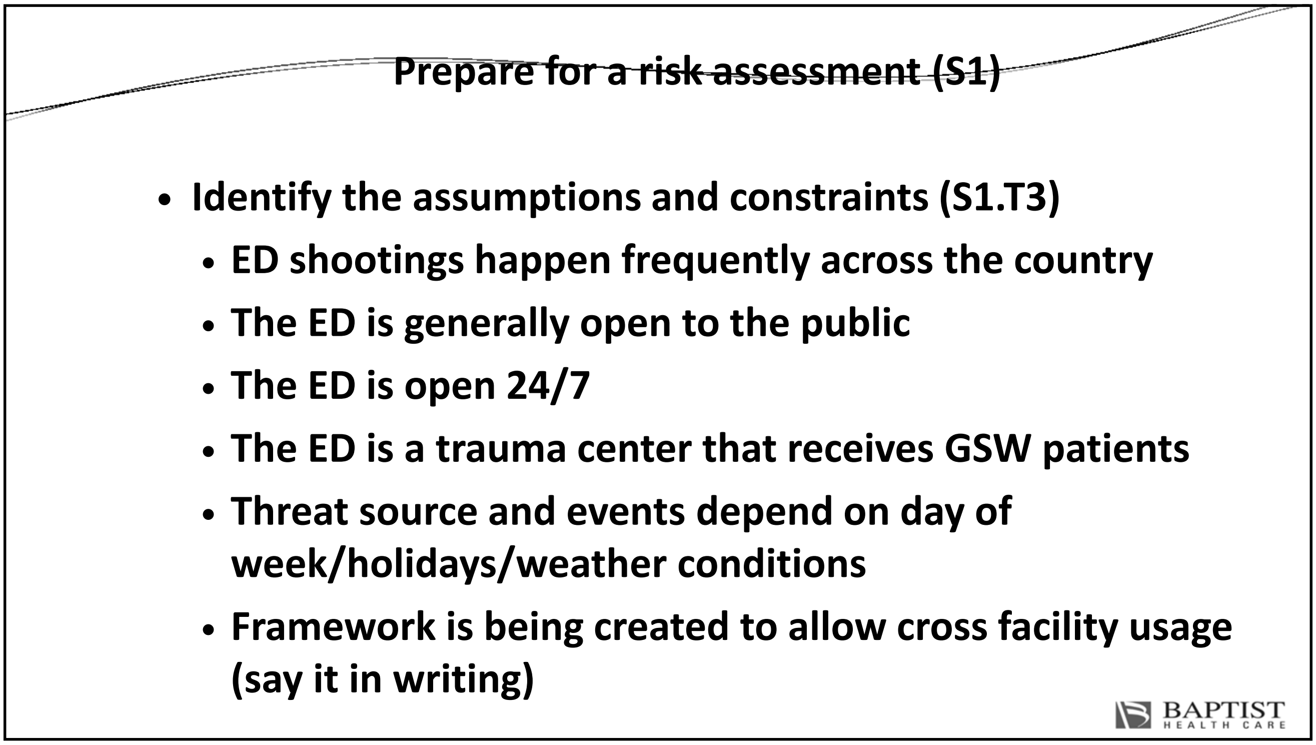
BAPTIST HEALTH CARE



Prepare for a risk assessment (S1)

- Identify and document the assumptions and constraints (This is where we document the thought process) (S1.T3)
  - Threat Sources
  - Threat Events
  - Vulnerabilities and Predisposed Conditions
  - Likelihood – how will it be determined?
  - Impacts – what is the adverse impact of the event?

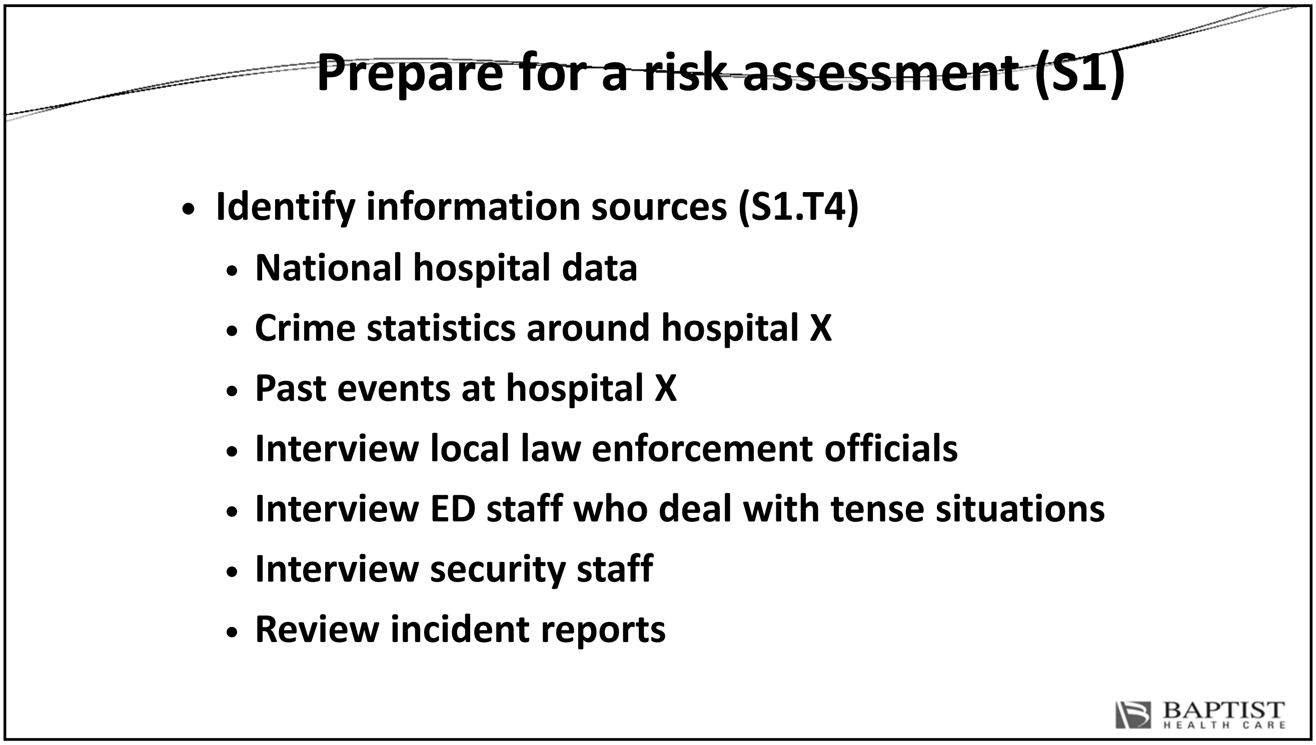
BAPTIST HEALTH CARE



Prepare for a risk assessment (S1)

- Identify the assumptions and constraints (S1.T3)
  - ED shootings happen frequently across the country
  - The ED is generally open to the public
  - The ED is open 24/7
  - The ED is a trauma center that receives GSW patients
  - Threat source and events depend on day of week/holidays/weather conditions
  - Framework is being created to allow cross facility usage (say it in writing)

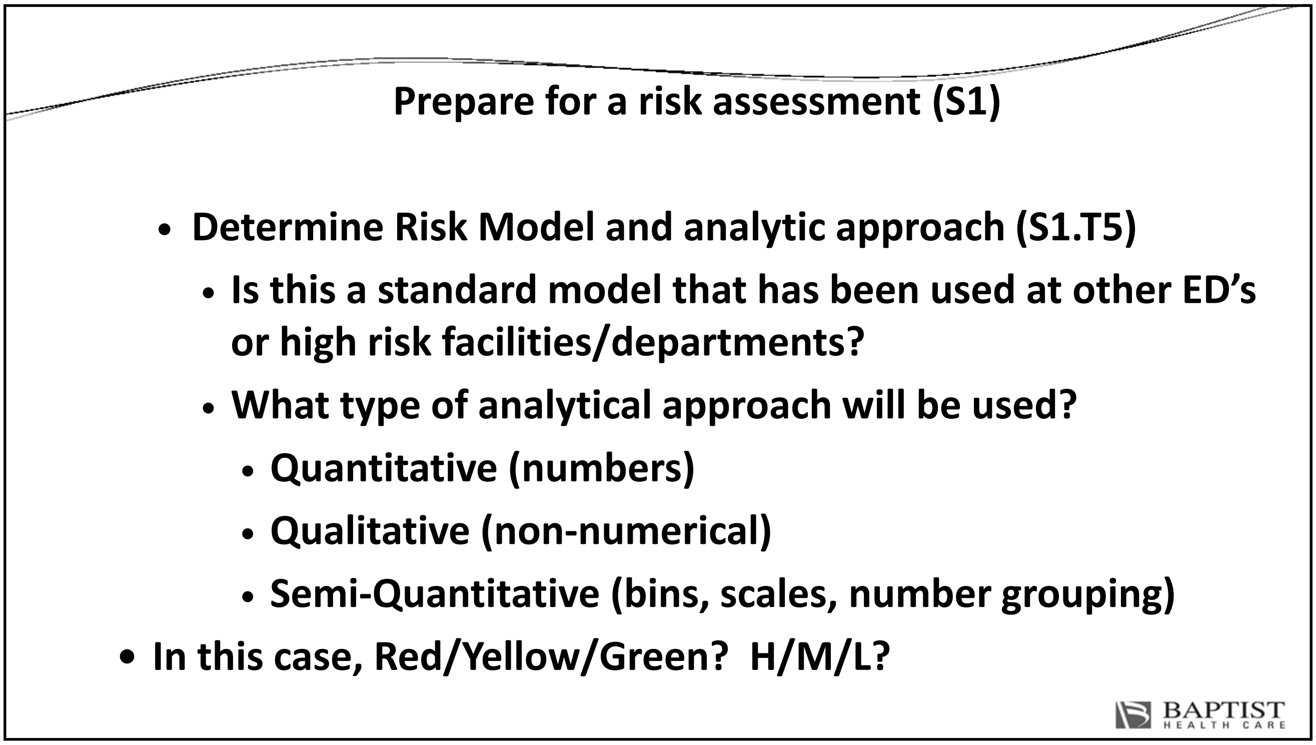
BAPTIST HEALTH CARE



Prepare for a risk assessment (S1)

- Identify information sources (S1.T4)
  - National hospital data
  - Crime statistics around hospital X
  - Past events at hospital X
  - Interview local law enforcement officials
  - Interview ED staff who deal with tense situations
  - Interview security staff
  - Review incident reports

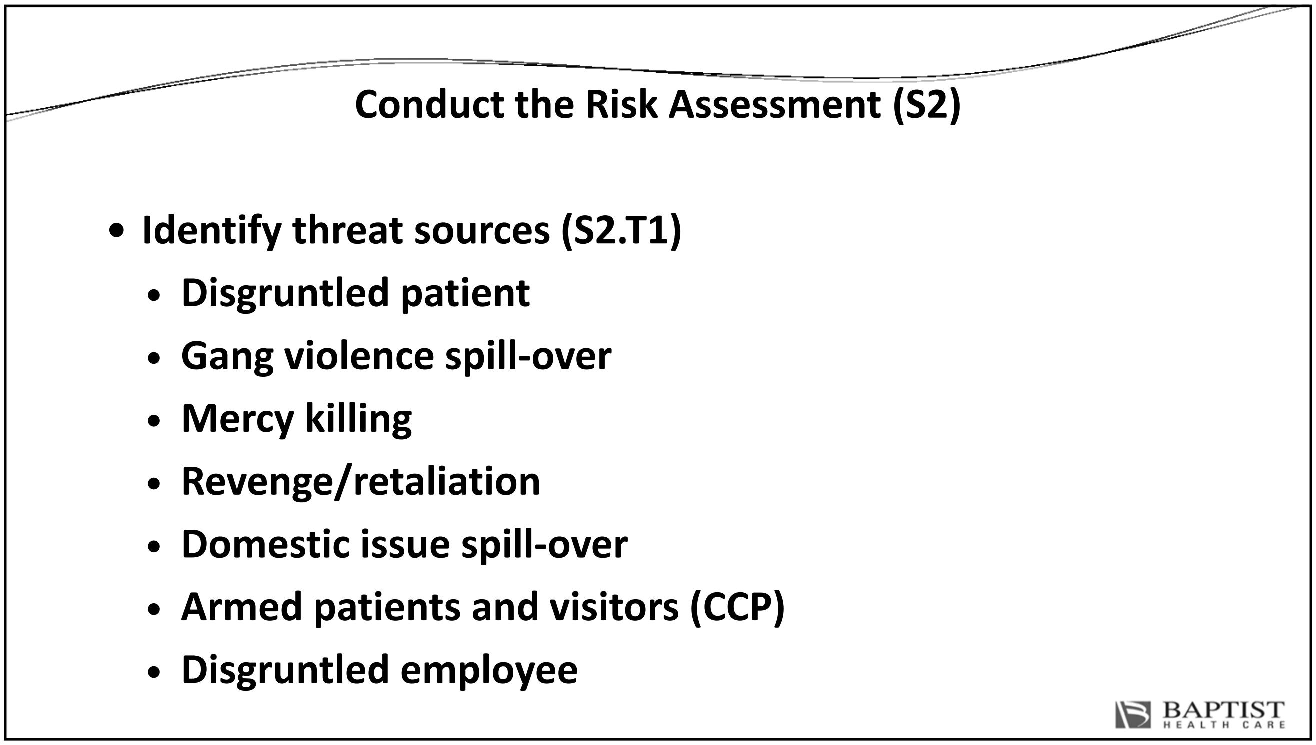
BAPTIST HEALTH CARE



Prepare for a risk assessment (S1)

- Determine Risk Model and analytic approach (S1.T5)
  - Is this a standard model that has been used at other ED’s or high risk facilities/departments?
  - What type of analytical approach will be used?
    - Quantitative (numbers)
    - Qualitative (non-numerical)
    - Semi-Quantitative (bins, scales, number grouping)
- In this case, Red/Yellow/Green? H/M/L?

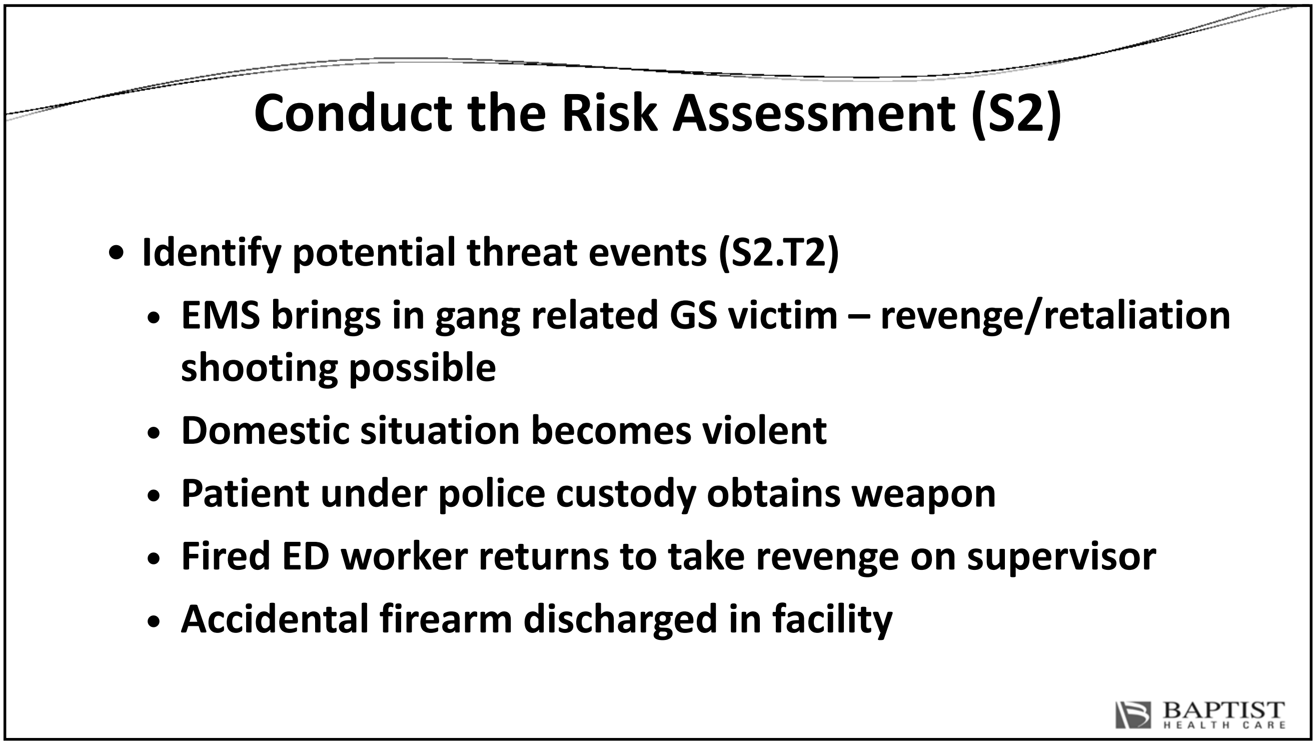
BAPTIST HEALTH CARE



Conduct the Risk Assessment (S2)

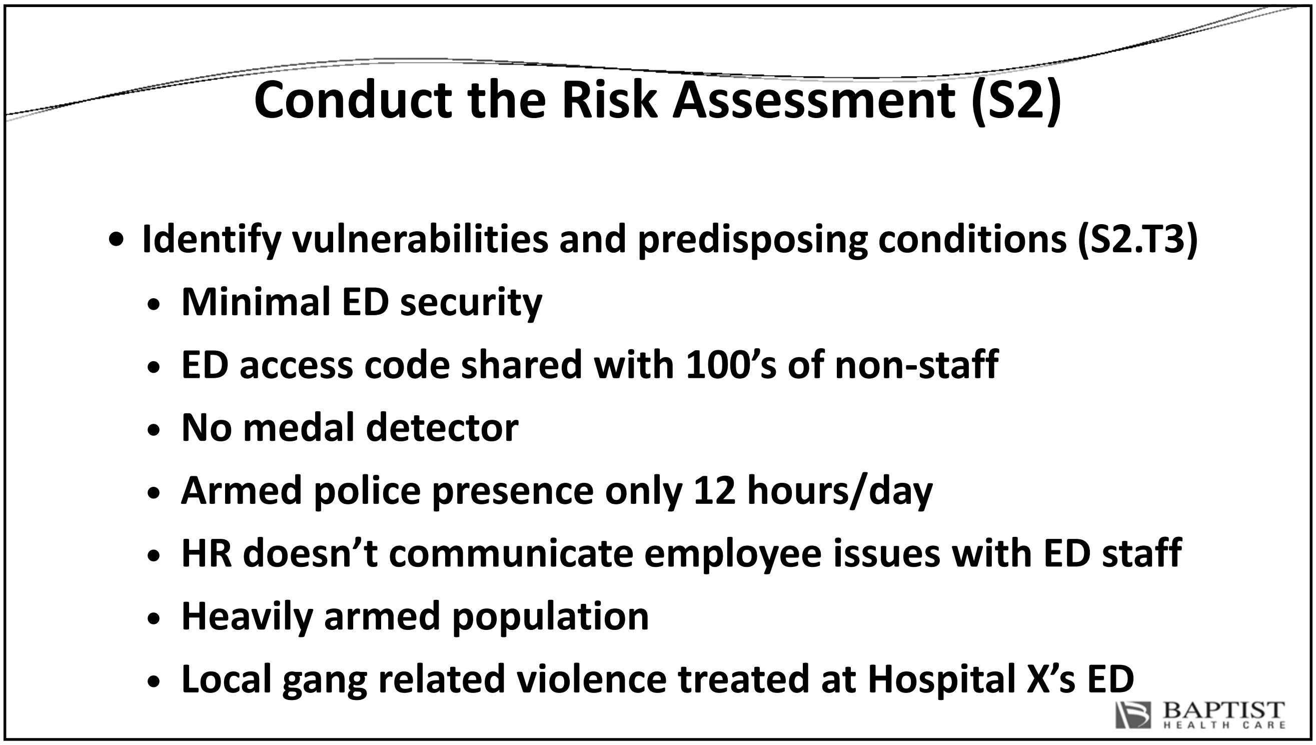
- Identify threat sources (S2.T1)
  - Disgruntled patient
  - Gang violence spill-over
  - Mercy killing
  - Revenge/retaliation
  - Domestic issue spill-over
  - Armed patients and visitors (CCP)
  - Disgruntled employee

BAPTIST HEALTH CARE



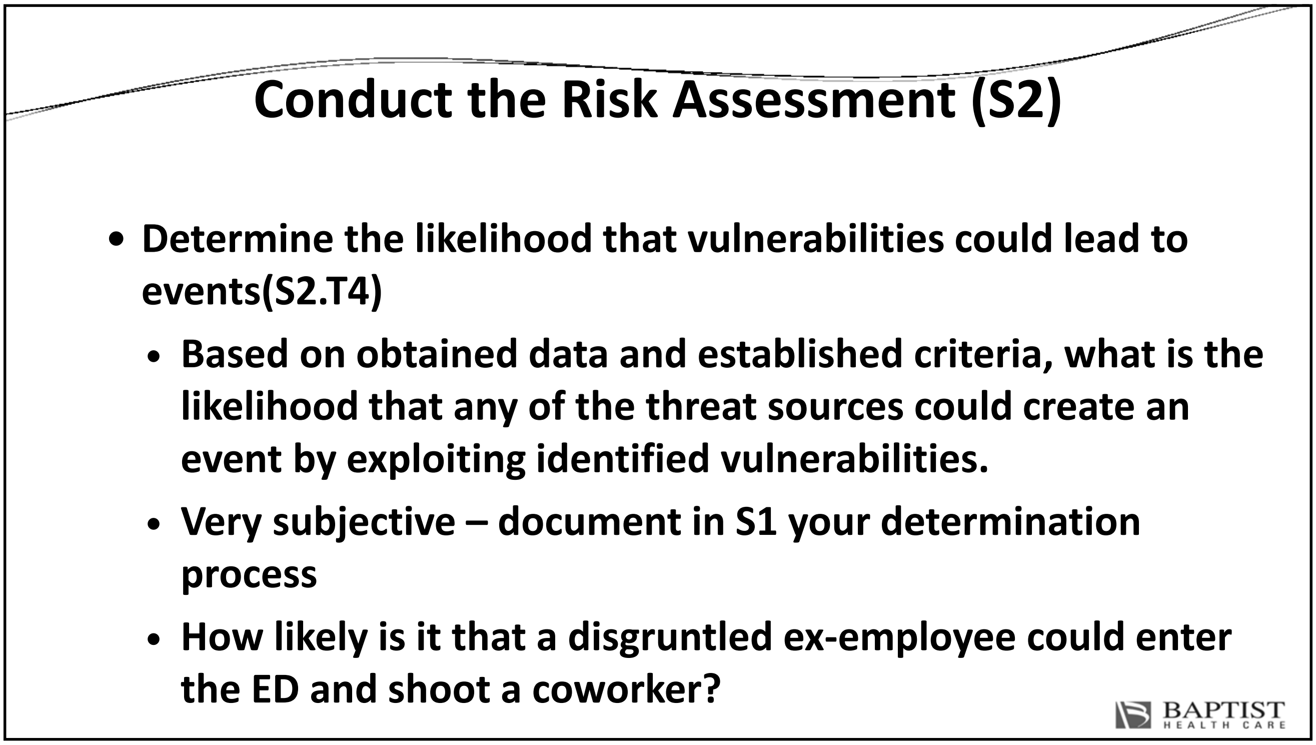
Conduct the Risk Assessment (S2)

- **Identify potential threat events (S2.T2)**
  - **EMS brings in gang related GS victim – revenge/retaliation shooting possible**
  - **Domestic situation becomes violent**
  - **Patient under police custody obtains weapon**
  - **Fired ED worker returns to take revenge on supervisor**
  - **Accidental firearm discharged in facility**



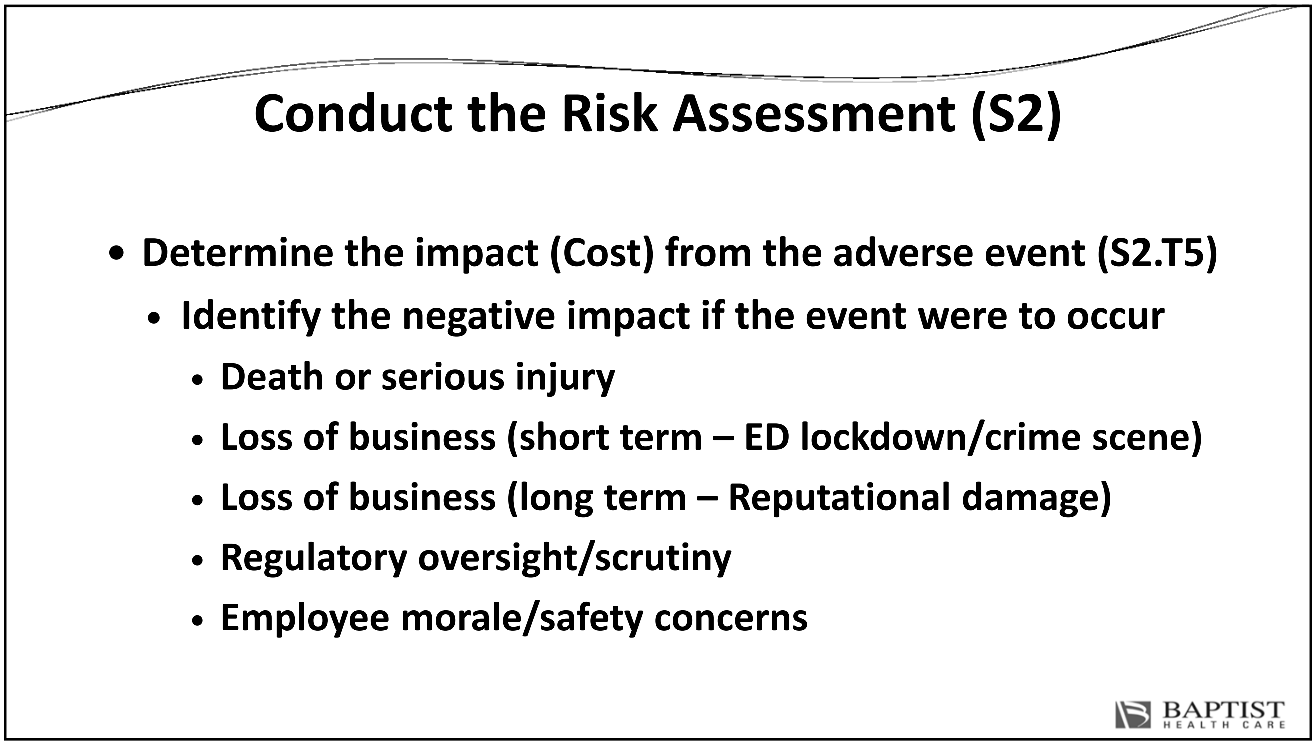
Conduct the Risk Assessment (S2)

- **Identify vulnerabilities and predisposing conditions (S2.T3)**
  - **Minimal ED security**
  - **ED access code shared with 100's of non-staff**
  - **No medal detector**
  - **Armed police presence only 12 hours/day**
  - **HR doesn't communicate employee issues with ED staff**
  - **Heavily armed population**
  - **Local gang related violence treated at Hospital X's ED**



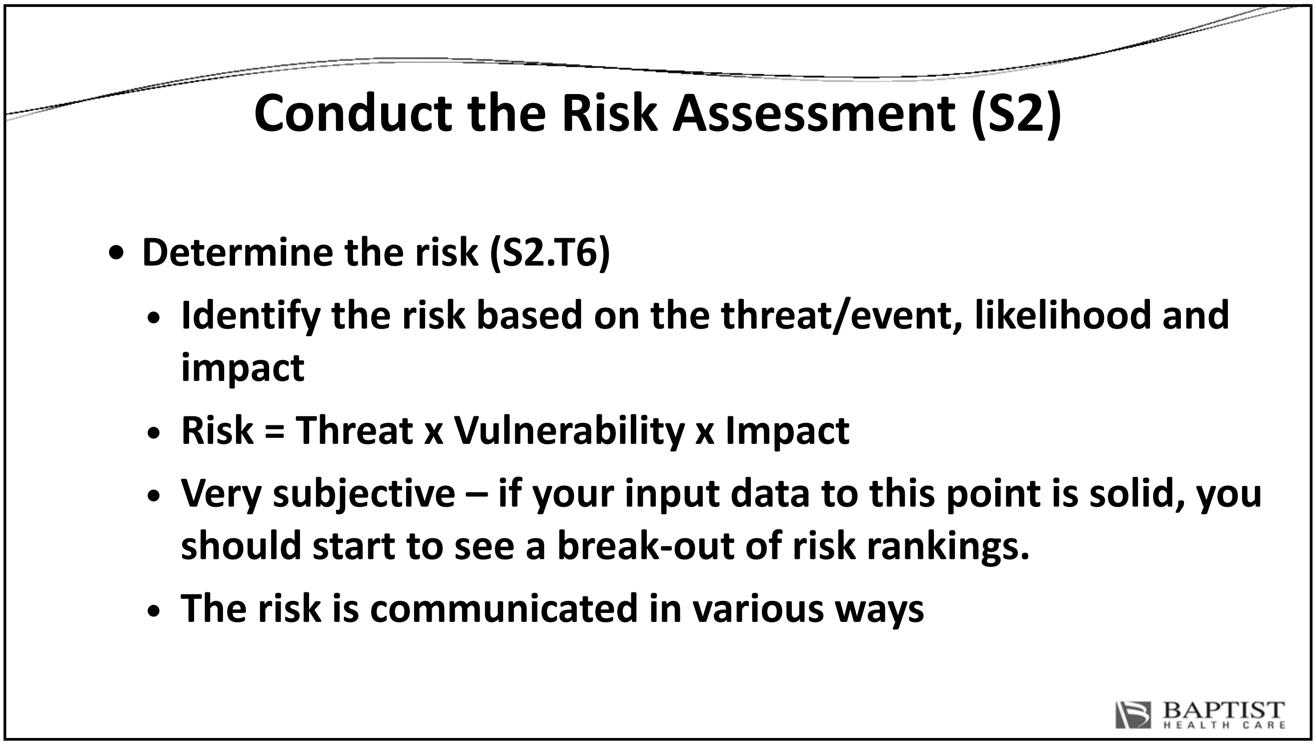
Conduct the Risk Assessment (S2)

- Determine the likelihood that vulnerabilities could lead to events(S2.T4)
  - Based on obtained data and established criteria, what is the likelihood that any of the threat sources could create an event by exploiting identified vulnerabilities.
  - Very subjective – document in S1 your determination process
  - How likely is it that a disgruntled ex-employee could enter the ED and shoot a coworker?



Conduct the Risk Assessment (S2)

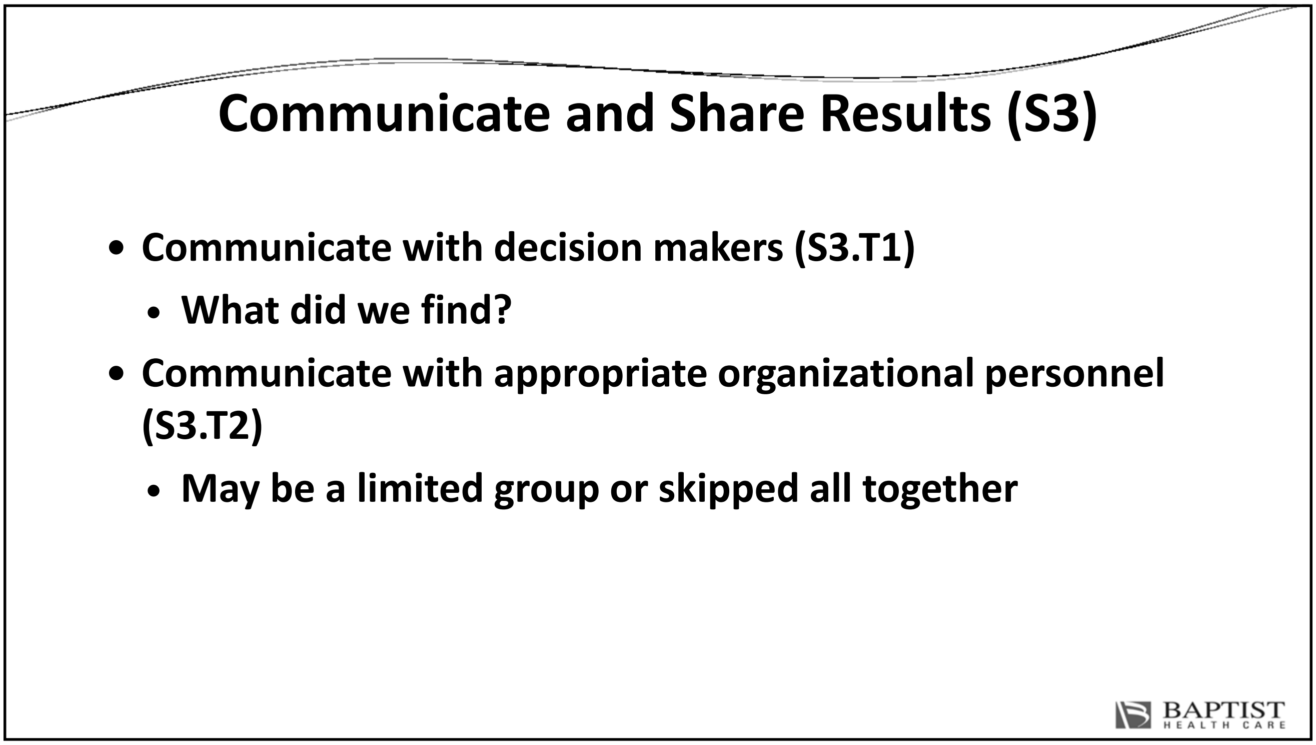
- Determine the impact (Cost) from the adverse event (S2.T5)
  - Identify the negative impact if the event were to occur
    - Death or serious injury
    - Loss of business (short term – ED lockdown/crime scene)
    - Loss of business (long term – Reputational damage)
    - Regulatory oversight/scrutiny
    - Employee morale/safety concerns



Conduct the Risk Assessment (S2)

- Determine the risk (S2.T6)
  - Identify the risk based on the threat/event, likelihood and impact
  - Risk = Threat x Vulnerability x Impact
  - Very subjective – if your input data to this point is solid, you should start to see a break-out of risk rankings.
  - The risk is communicated in various ways

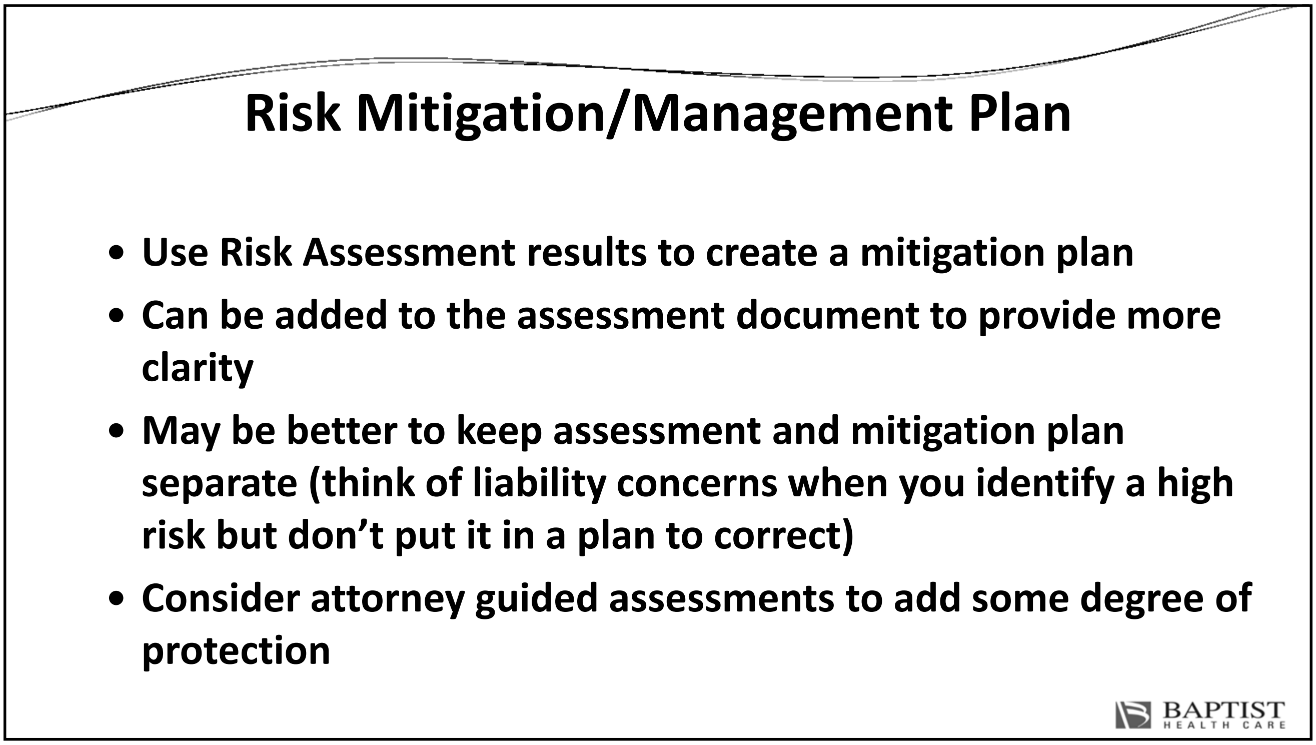
BAPTIST HEALTH CARE



Communicate and Share Results (S3)

- Communicate with decision makers (S3.T1)
  - What did we find?
- Communicate with appropriate organizational personnel (S3.T2)
  - May be a limited group or skipped all together

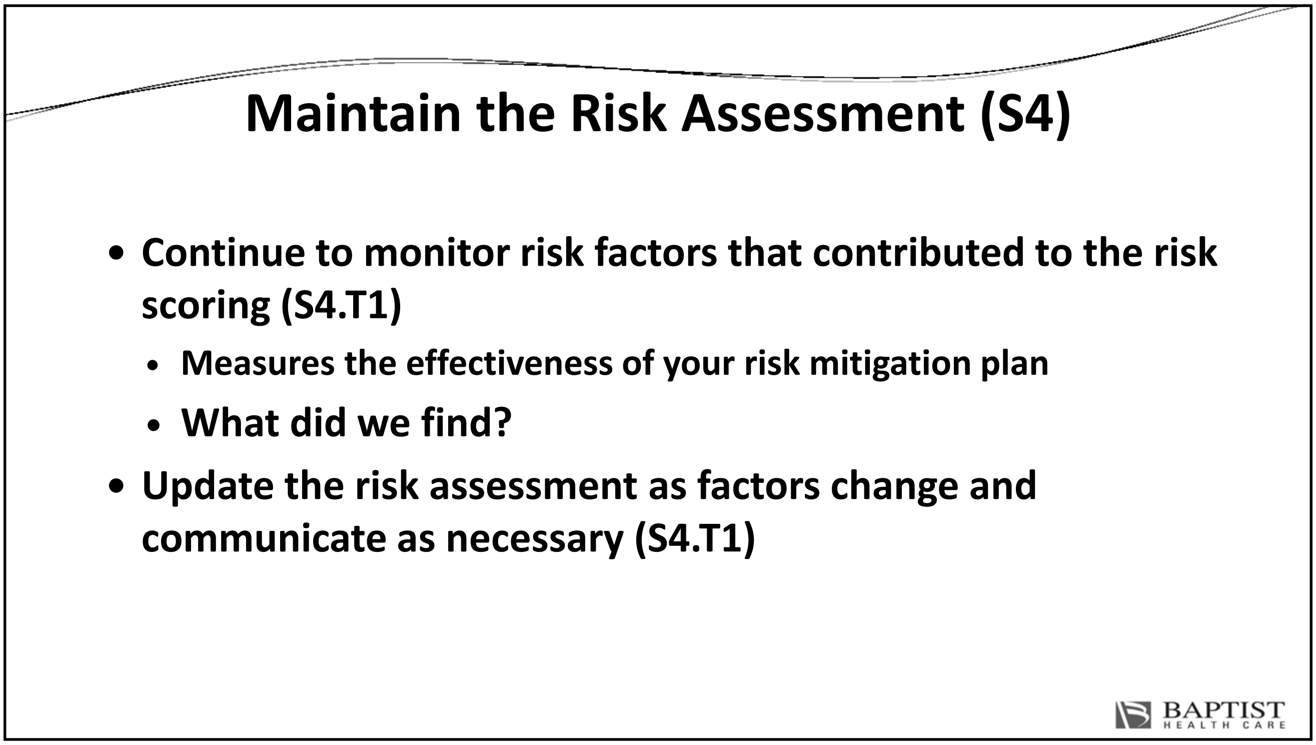
BAPTIST HEALTH CARE



Risk Mitigation/Management Plan

- Use Risk Assessment results to create a mitigation plan
- Can be added to the assessment document to provide more clarity
- May be better to keep assessment and mitigation plan separate (think of liability concerns when you identify a high risk but don’t put it in a plan to correct)
- Consider attorney guided assessments to add some degree of protection

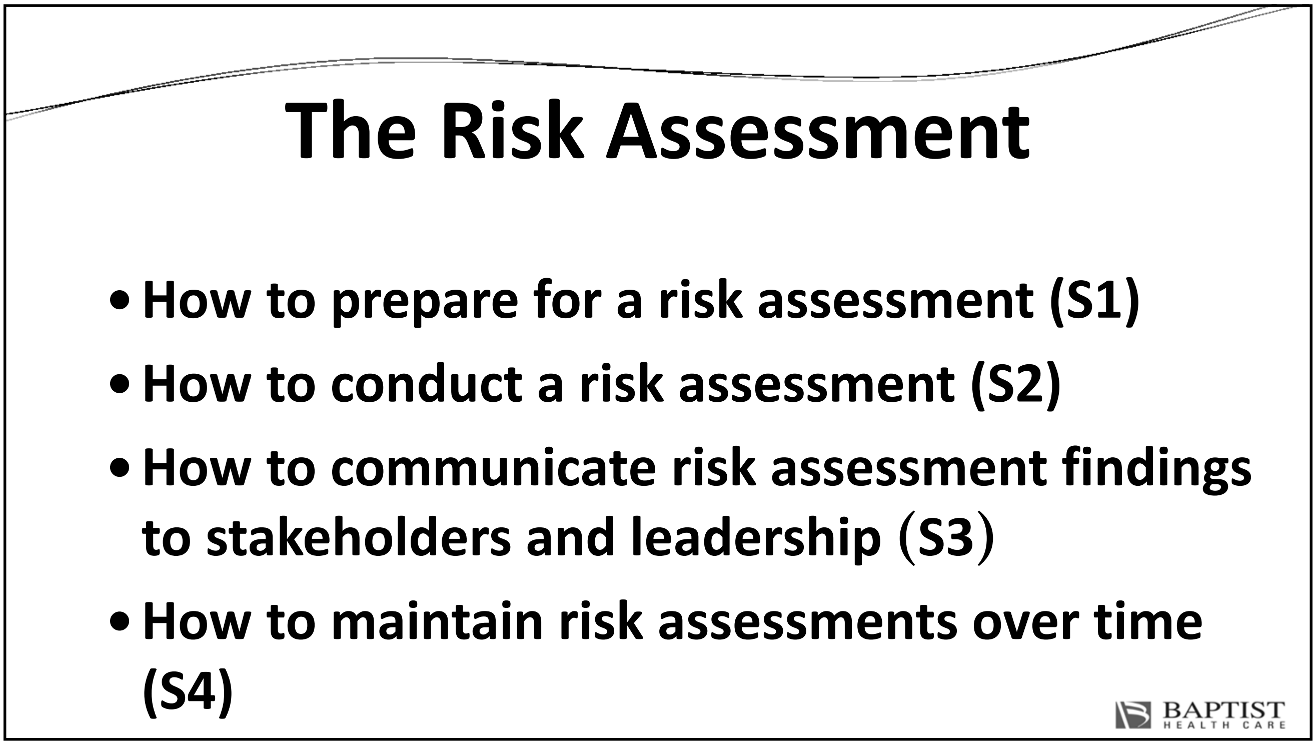
BAPTIST HEALTH CARE



Maintain the Risk Assessment (S4)

- Continue to monitor risk factors that contributed to the risk scoring (S4.T1)
  - Measures the effectiveness of your risk mitigation plan
  - What did we find?
- Update the risk assessment as factors change and communicate as necessary (S4.T1)

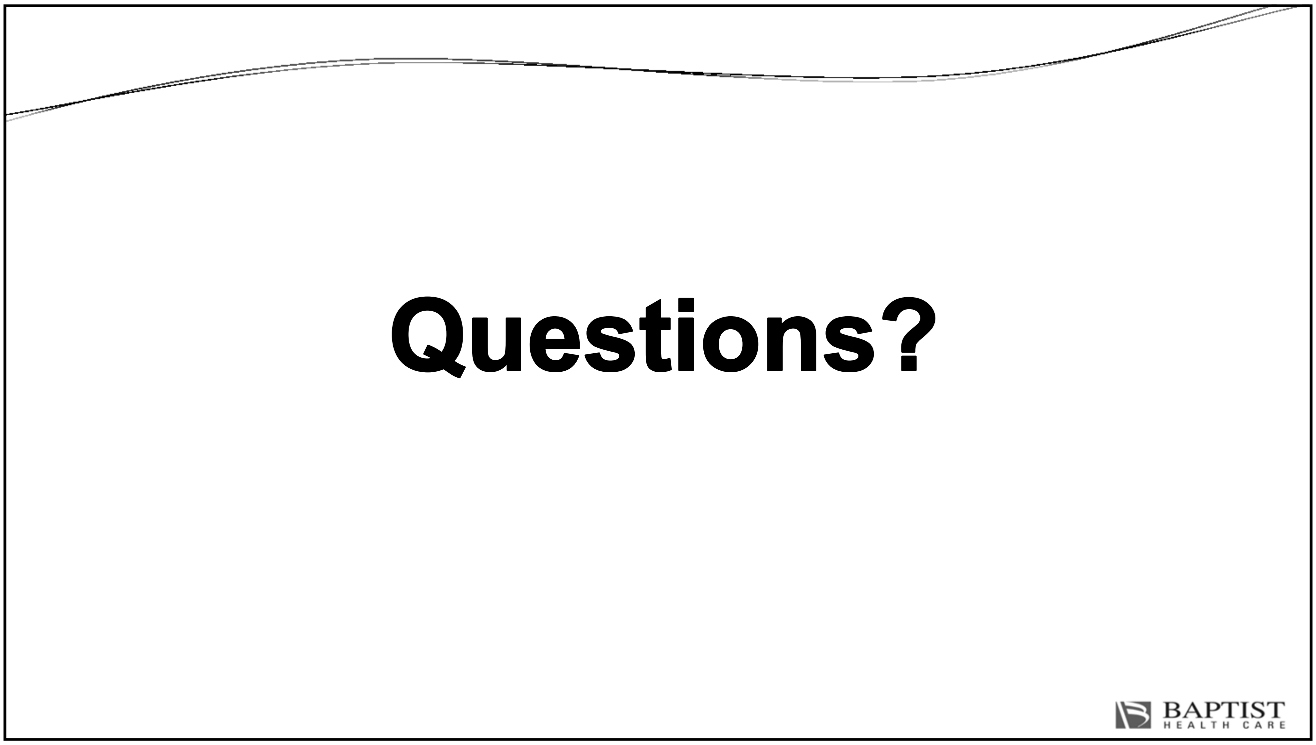
BAPTIST HEALTH CARE



The Risk Assessment

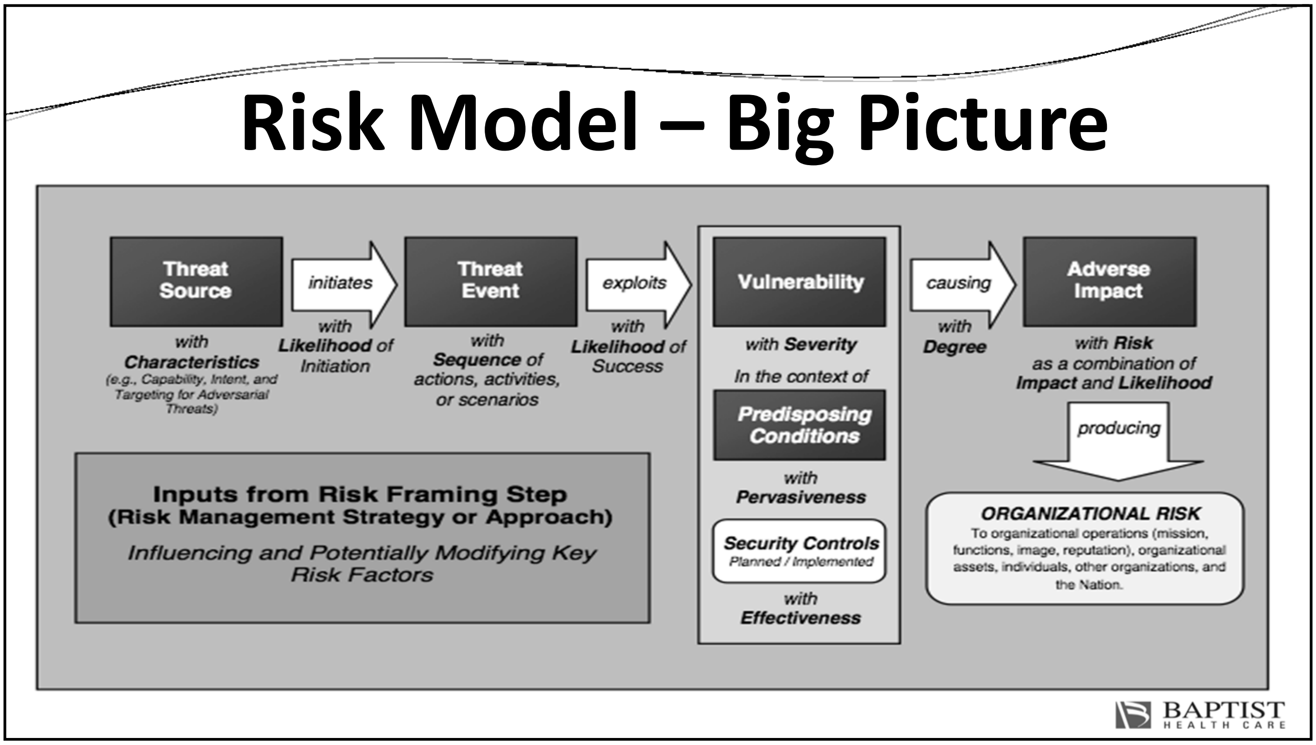
- How to prepare for a risk assessment (S1)
- How to conduct a risk assessment (S2)
- How to communicate risk assessment findings to stakeholders and leadership (S3)
- How to maintain risk assessments over time (S4)

BAPTIST HEALTH CARE



Questions?

BAPTIST HEALTH CARE



Risk Model – Big Picture

Threat Source with **Characteristics** (e.g., Capability, Intent, and Targeting for Adversarial Threats)

initiates with **Likelihood** of Initiation

Threat Event with **Sequence** of actions, activities, or scenarios

exploits with **Likelihood** of Success

Vulnerability with **Severity**

In the context of

Predisposing Conditions with **Pervasiveness**

Security Controls Planned / Implemented with **Effectiveness**

causing with **Degree**

Adverse Impact with **Risk** as a combination of **Impact and Likelihood**

producing

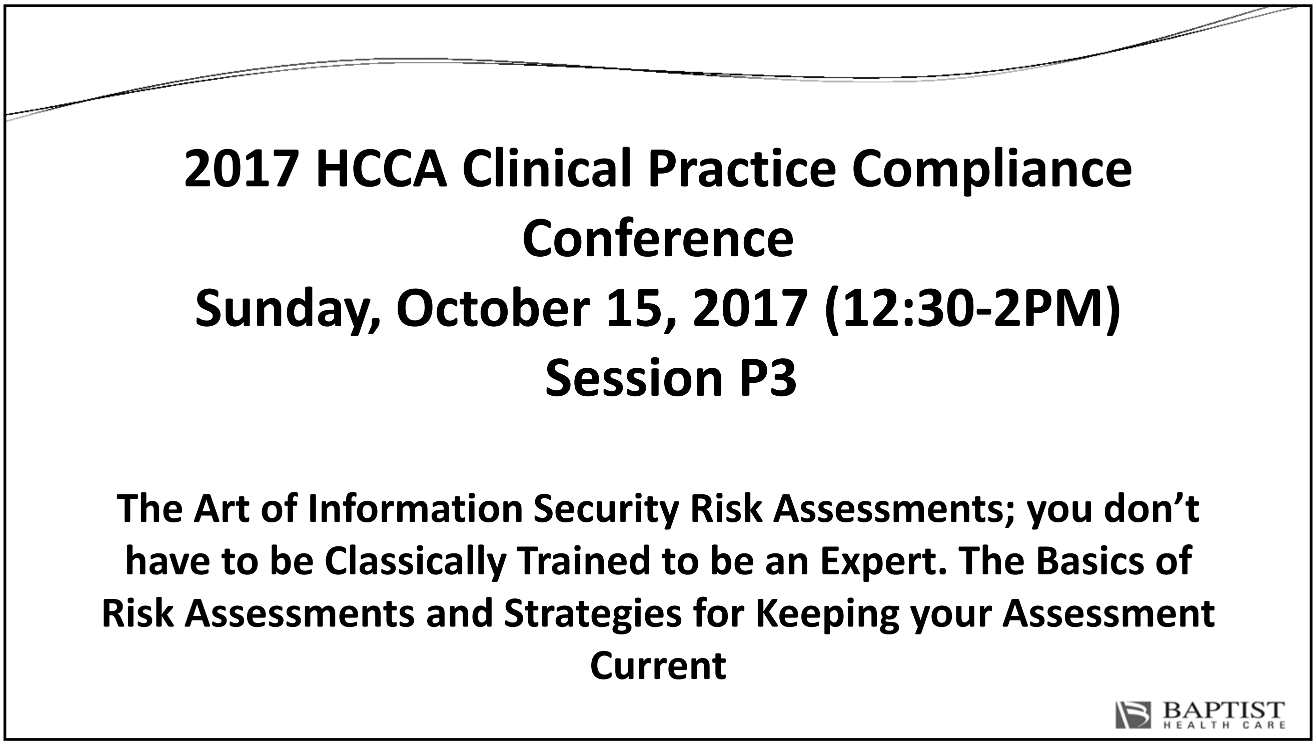
ORGANIZATIONAL RISK

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

BAPTIST HEALTH CARE



2017 HCCA Clinical Practice Compliance Conference
Sunday, October 15, 2017 (12:30-2PM)
Session P3

The Art of Information Security Risk Assessments; you don't have to be Classically Trained to be an Expert. The Basics of Risk Assessments and Strategies for Keeping your Assessment Current

BAPTIST HEALTH CARE