

THREAT-BASED RISK ANALYSIS

Understanding the security risks facing your organization is no longer optional. But where to start? We believe that Threat-Based Risk Analysis must be done in context to each organization which starts by clearly agreeing on the purpose, scope, assumptions, and constraints of the engagement.

These factors allow Online to customize the process for your organization's unique needs. By doing so, we are able to deliver more than the common security risk analysis, which tend to be limited to a security controls assessment or HIPAA gap analysis.

"Our approach to security risk analysis goes beyond adherence to HIPAA Security Rule. We identify realistic threats to the organization's information and systems."

Online's approach is based on the standards and guidance published by NIST and the Health and Human Services Office for Civil Rights (OCR) for performing actual threat-based analysis.

Our approach takes advantage of proprietary advanced tooling and a methodology that enables our security experts to deliver optimized results for each Client.

It also delivers a framework for our Clients through which they can protect the confidentiality, integrity, and availability of critical assets and information across the organization going forward.



How can our Risk Analysis Benefit Your Organization?

- Collaborative and Flexible Approach
- Aligns with Enterprise Risk Models
- Focus on realistic threats to critical assets
- Assess Business Impact
- Allows CISOs and CIOs to prioritize scarce resources

Our Threat-based Security Risk Analysis starts by analyzing realistic threats and developing a customized threat profile. This Threat Profile is a critical part of our approach and is based on our Baseline Threat Profile which we continually maintain and update using industry sources such as NIST, HHS, and US-CERT.

Our Approach Works

This all-inclusive approach to your requirements provides reassurance to our valued Clients and their data.

1. Preparation
2. Asset Identification
3. Consideration of Threats
4. Controls Assessment
5. Perform Risk Analysis
6. Document Results and Recommend Corrective Actions

Our methodology is aligned with the requirements of the HIPAA Security Rule, NIST SP 800-30 Guide for Conducting Risk Assessments, and the OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule.

Working with you, we will carefully select the appropriate categories of your risk profile that need to be analyzed. This will include details about your Organizational Profile, Asset Identification, Threat Profile, and your Control Assessment.

Our team will then cross-reference those unique areas and consider adversarial, accidental, and environmental threats accordingly. By focusing on realistic threats, the organization can identify and focus on security controls that provide the greatest value in protecting critical assets and, ultimately your business



Contact:

Online Business Systems
1.800.668.7722
info@obsglobal.com

Founded in 1986, Online Business Systems is North America's leading Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.