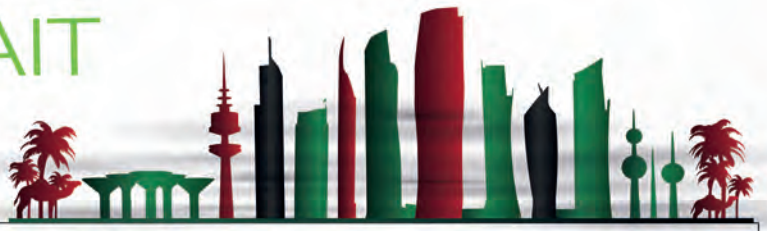
الاتحاد الدولي للمصرفيين العرب
World Union of Arab Bankers

اتحاد مصارف الكويت
Kuwait Banking Association

BANKING ON CYBERSECURITY:

PROTECTING DIGITAL FINANCIAL LANDSCAPES

4-5 OCTOBER 2023
KUWAIT CITY KUWAIT



WUAB ANNUAL SPONSORS 2023

بنك القاهرة Banque du Caire | بنك مصر Banque Misr | الاعتماد اللبناني Credit Libanais | بنك كاك الدولي International Bank | مصرف الجمهورية Jumhouria Bank

OVERVIEW

The training on cybersecurity of financial institutions and digital banking is specifically tailored to equip professionals in the finance industry with the necessary knowledge and skills to protect sensitive data, prevent security breaches, and ensure the safety of digital transactions. The comprehensive 2-day program delivers essential knowledge to help banks and financial organizations secure critical assets and customer data against emerging cyber threats targeting the finance sector.

The training utilizes real-world case studies to provide participants with insights into previous bank breaches, including the drivers, exploits, impacts, and lessons learned. These case studies cover various scenarios such as phishing attacks, third-party risks, unpatched systems, insider threats, and more. By analyzing these real cases of breaches, participants gain a better understanding of potential threats and the importance of implementing robust cybersecurity practices. One of the key components of the training is the focus on ISO 27001, which is introduced as a vital tool to effectively mitigate cybersecurity risks. Participants learn about its relevance to the financial sector and digital banking, understanding how it establishes a systematic approach to information security management. The training delves into the key components of ISO 27001, including its 4 to 10 clauses that cover crucial aspects such as risk assessment, security policy, information security controls, and incident management. A significant portion of the training is dedicated to Annex A of ISO 27001, which outlines a comprehensive set of security controls that can be tailored to the specific needs of financial institutions and digital banking platforms. Participants learn about various control domains, including access control, cryptography, physical and environmental security, supplier relationships, and incident response. Case studies of successful ISO 27001 implementations in the financial industry are presented to highlight the effectiveness of this approach. Furthermore, the training covers best practices for securing applications to bolster cybersecurity in financial institutions and digital banking platforms. Participants gain insights into the software development lifecycle and the importance of implementing security measures at each stage. This includes code reviews, vulnerability assessments, and secure coding practices. The training emphasizes the significance of regularly updating and patching applications to mitigate emerging threats effectively.

WHO SHOULD ATTEND:

- **IT and Security Professionals in Financial Institutions:** This audience comprises individuals responsible for managing IT systems, networks, and security infrastructure within financial organizations. They play a crucial role in implementing cybersecurity measures, conducting risk assessments, and ensuring compliance with ISO 27001 standards.
- **Cybersecurity Specialists and Analysts:** These professionals specialize in monitoring and analyzing security threats, investigating incidents, and proposing strategies to protect financial institutions and digital banking platforms from cyber-attacks.
- **Risk and Compliance Officers:** This group of professionals is responsible for assessing and managing risks related to cybersecurity and ensuring the organization's adherence to regulatory requirements and ISO 27001 standards.
- **Information Security Managers and Officers:** Individuals in this role are responsible for overseeing the development, implementation, and maintenance of information security policies, procedures, and controls in financial institutions.
- **Auditors and Assessors:** Professionals involved in auditing and assessing the security practices and compliance of financial institutions and digital banking platforms may benefit from this training to better evaluate the effectiveness of cybersecurity measures and ISO 27001 implementation.
- **Security Consultants and Service Providers:** Individuals or companies providing cybersecurity consulting and services to financial institutions and digital banking entities can use this training to enhance their expertise and deliver more effective solutions.

TOPICS

1. **Real Cases of Breaches:** The training begins with a detailed examination of real-world cybersecurity breaches that have impacted financial institutions and digital banking platforms. These case studies shed light on the vulnerabilities that led to breaches and the consequences faced by the affected entities. Some prominent examples may include the 2017 Equifax data breach, the 2020 Capital One breach, and others. By analyzing these cases, participants understand the potential threats they face and the importance of robust cybersecurity practices.
2. **ISO 27001 as a Mitigation Framework:** ISO 27001 is introduced as a vital tool to mitigate cybersecurity risks effectively. Participants learn about its relevance to the financial sector and digital banking, understanding how it establishes a systematic approach to information security management. The training delves into the key components of ISO 27001, including its 4 to 10 clauses, which cover crucial aspects such as risk assessment, security policy, information security controls, and incident management.
3. **Annex A - Controls for Information Security:** A significant portion of the training is dedicated to Annex A of ISO 27001. This annex outlines a comprehensive set of security controls that can be tailored to the specific needs of financial institutions and digital banking platforms. Participants learn about various control domains, such as access control, cryptography, physical and environmental security, supplier relationships, and incident response. Case studies of successful ISO 27001 implementations in the financial industry are presented to highlight the effectiveness of this approach.
4. **Securing Applications:** To bolster cybersecurity in financial institutions and digital banking, the training covers best practices for securing applications. Participants gain insights into the software development lifecycle and the importance of implementing security measures at each stage. This includes code reviews, vulnerability assessments, and secure coding practices. The training also addresses the significance of regularly updating and patching applications to mitigate emerging threats.

CONCLUSION:

The training concludes with a call to action for financial institutions and digital banking platforms to prioritize cybersecurity. By leveraging ISO 27001 as a mitigation framework and implementing robust security measures, they can protect sensitive data, thwart cyberattacks, and safeguard their reputation and trust among customers. Continuous education and adaptation to evolving threats are emphasized as critical aspects of maintaining a resilient cybersecurity posture in the rapidly evolving digital landscape

ABOUT THE SPEAKER

Tony Chebli

Tony Chebli stands as a beacon in the information security landscape, with a special penchant for ISO standards. His meticulous analysis of the ISO/IEC 27005:2022 has offered clarity and insights to many, thanks to the comprehensive webinar he spearheaded. Mr. Chebli's leadership and significant strides as the Head of the Information Security Department at Credit Libanais Bank have not gone unnoticed. His triumphant three-year streak of receiving the CISO 100 Award distinguishes him as one of the Middle East's premier information security figures. Passionate about knowledge transfer, he has steered several webinars, one of which meticulously unpacked the ISO 27001:2013 Information Security Management System, elucidating critical facets like gap and risk assessments crucial for organizations on the certification journey. Beyond his accolades and educational endeavors, Mr. Chebli's commitment to the highest echelons of information security standards and practices is unwavering. His endeavors, marked by a blend of excellence and innovation, position him as an invaluable pillar in the industry. Young professionals and peers alike look to his journey and contributions as a testament to what dedication and expertise can achieve.

BANKING ON CYBERSECURITY

World Union of Arab Bankers
Tel: +9611364976/8
Email: wuab@wuab.org
webmaster@wuab.org