Journal of Banking and Financial Technology
https://doi.org/10.1007/s42786-025-00056-3

ORIGINAL ARTICLE

An integrated cyber security risk management framework for online banking systems

Yiu Ting Yan Azura[1] · **Muhammad Ajmal Azad**[2] · **Yussuf Ahmed**[2]

Received: 25 March 2023 / Accepted: 11 April 2025

Abstract
Online banking systems have become an integral part of our daily lives, offering access to financial services through Internet technologies and applications, however, as these systems grow in prevalence, they also introduce significant security and privacy challenges. These systems can be exposed to various cybersecurity threats that can result in data breaches, compromise of sensitive financial information, reputational damage, and significant operational disruptions. The existing model designed to ensure the security of consumers and service providers often fails to address the unique security and privacy challenges posed by banking environments. This paper proposes an integrated management framework based on threat and risk models, specifically designed for online banking systems. The framework incorporates a comprehensive risk management process and systematic assessment techniques while considering security features attributed to the banking environment, threat landscapes, and accessible information within the banking. During the threat identification and vulnerability analysis phases, potential attack scenarios and their possible impacts are evaluated using pre-defined procedures while considering the context. The assessment process quantifies cybersecurity risks, facilitating the appropriate mitigation strategies to address identified threats and risks. The framework's applicability has been evaluated to determine its potential for effective real-world implementation in online banking systems. The evaluation addressed the security and privacy challenges of digital banking, and its ability to integrate with existing technologies and regulatory requirements.

Keywords Online banking · Banking security · Risk assessment and management

1 Introduction

The financial sector, including banking institutions, insurance companies, and investment firms, has undergone significant shifts in the last few decades due to technological advancements and digital transformation. Statistics highlight the significant growth of online banking, with usage in the United Kingdom skyrocketing from approximately 30% in 2007 to over 90% in 2022 [1]. This trend underscores the growing importance of digital banking solutions, as more consumers shift towards online channels for their everyday banking needs, driven by factors such as convenience, speed, and cost-effectiveness. Key innovations such as Artificial Intelligence (AI), Financial Technology (FinTech), Regulatory Technology (RegTech), and the adoption of cloud computing have emerged and are being deployed across the industry [2–7]. While these technologies enable smooth operations and offer value-added services to consumers, however, they also introduce new security vulnerabilities and privacy concerns that require measures to ensure the security of sensitive financial data and fulfil compliance obligations.

The banking models are built upon internet-based interfaces that enable users to interact with various banking services remotely. These interactions are typically facilitated through secure web applications, interfaces or mobile applications [8–12]. On the backend, these platforms rely on sophisticated payment processing systems, encryption measures and authentication frameworks to

✉ Muhammad Ajmal Azad
muhammadajmal.azad@bcu.ac.uk

Yiu Ting Yan Azura
azura.yiu@warwick.ac.uk

Yussuf Ahmed
yussuf.ahmed@bcu.ac.uk

[1] WMG, University of Warwick, Coventry, UK

[2] School of Computer Science, Birmingham City University, Birmingham, UK

Published online: 09 May 2025

ensure seamless and secure processing of user data and information. As the financial sector continues to grow, therefore, the associated security challenges become more pronounced. Given the sensitive nature of financial data, robust security protocols are essential to maintain the integrity of the system and protect user information. These protocols and security measures are crucial in safeguarding online banking environments against potential threats such as identity theft, data breaches, and fraudulent transactions. The adoption of these security measures, along with advancements in artificial intelligence and machine learning for fraud detection, are essential for ensuring that online banking remains secure, efficient, and trustworthy in the face of evolving cyber threats. As the industry continues to adapt to these changes, banks will need to bolster their risk management frameworks to address an expanding array of challenges. This includes the adoption of advanced fraud detection systems, compliance tools, and data privacy regulations to safeguard customer information and ensure trust in online banking services [13]. Consequently, risk management functions must be continuously updated to reflect these new demands and regulatory requirements, ensuring that financial institutions remain resilient in the face of increasingly sophisticated cyber threats and consumer expectations.

To effectively identify and manage the ever-evolving threat landscape, both regulators and financial institutions require a standardized and robust framework to address risks and develop appropriate mitigation strategies. The implementation of a Risk Management Framework (RMF) offers a structured, yet adaptable approach to integrating risk management into organizational processes. This framework not only supports informed decision-making but also enables proactive identification of potential vulnerabilities, thereby helping to reduce or eliminate risks and minimize the financial and operational impacts on banks. An RMF enables organizations to assess threats, understand their potential consequences, and align risk mitigation actions with business objectives. While a variety of existing risk management methods and frameworks offer general guidelines for addressing risks across sectors, the application of these frameworks to online banking systems (OBS) presents unique challenges. Factors such as dynamic risk elements, changing customer behaviours, and unintentional security lapses all contribute to the complexity of the banking systems. Furthermore, the interdependence of various security components within online banking systems introduces the risk of cascading failures, where a single security breach can quickly escalate across multiple systems and channels. The interconnectivity demands a more thorough and holistic approach to cybersecurity risk management, one that not only addresses individual system weaknesses but also accounts for the cumulative impact of interconnected risks.

To effectively address these challenges, a recursive and comprehensive management model is required. Such a model would allow for continuous monitoring, evaluation, and adaptation of security measures, capturing new knowledge and insights from each security incident to enhance the system's resilience. The primary objective of this paper is to examine and manage cybersecurity risks within online banking systems using a comprehensive and inclusive framework. The framework is designed to offer a structured approach for understanding, assessing, and mitigating cybersecurity threats in a way that is scalable and adaptable to the evolving landscape of online banking. By integrating insights from various security domains, the framework aims to guide the development of explicit design intent for enhancing online banking security. Through this, the paper aims to provide both theoretical and practical contributions to the field, enabling banks and financial service providers to better understand and manage cybersecurity risks while ensuring the protection of their digital infrastructures and customer data.

The novel contributions of this research are outlined as follows:

- We propose an integrated cybersecurity risk management framework that provides a comprehensive and holistic approach to identifying, assessing, and mitigating cybersecurity risks within online banking systems. Unlike traditional risk management models that focus on individual threats or isolated system components, this framework considers the entire digital banking ecosystem, including both technological and human factors, to offer a multidimensional perspective on risk.
- We proposed and designed assessment models that assess how risks in one area can cascade through the interconnected network, affecting both operational continuity and customer trust. This model provides banks with actionable insights that improve decision-making during risk evaluation, helping security teams to prioritize actions based on potential cascading consequences rather than isolated incidents.
- We evaluate the the proposed cybersecurity risk management framework approach, using real-world case studies while addressing the complex security challenges faced by banks. The evaluation focuses on assessing how well the framework facilitates proactive risk identification, mitigates the cascading effects of security breaches, and supports informed decision-making under dynamic conditions.

The structure of this paper is organized as follows: Sect. 2 provides an analysis of previous studies on risk management in banks, with a particular focus on cybersecurity aspects. It also offers an overview of existing approaches, highlighting the need for a new framework, which serves as

the motivation for the development of the proposed model. Section 3 presents the design of the proposed cybersecurity risk management framework, detailing its key components and the principles that guide its structure. Section 4 discusses the risk management strategies employed within the framework, emphasizing how they are applied to address the unique challenges faced by online banking systems. Section 5 evaluates the effectiveness of the proposed framework, comparing its performance against the expected outcomes. Finally, Sect. 6 provides the conclusions of the study and discusses the implications for future research and the ongoing development of cybersecurity risk management strategies in the banking sector

2 Related works

This paper examines the critical role that banks play in the functioning of modern financial systems, a principle that remains highly relevant in today's economies. Risk management within the banking industry has been a vibrant area of research, resulting in the publication of numerous studies on the subject. We reviewed the existing works into three categories: Risk Management in Banking; Cybersecurity in Online Banking Systems; and Risk Management Frameworks, Standards, and Guidelines.

2.1 Risk management in banking

Risk management has consistently been a core function in banking, with a primary focus on addressing profitability challenges. Traditional banking risks, as classified by [14], include financial risks such as credit, liquidity, and earnings risks. Numerous studies have underscored the strong relationship between credit and operational risks and their impact on financial performance [15–17], often highlighting the use of quantitative methods to assess these risks and mitigate potential losses.

The adoption of advanced technologies, such as machine learning, has significantly improved risk management in the banking sector. These technologies enable the analysis of vast, unstructured datasets, facilitating the identification of suspicious transactions and ensuring compliance with regulatory standards [18]. Despite the recognition of cybersecurity as a component of operational risk, limited attention has been directed toward leveraging advanced tools to address these challenges. Stojanovic et al. [19] stress the necessity of evolving risk management processes to account for emerging threats, particularly in electronic banking, where risks span credit, liquidity, compliance, reputation, and security domains.

The future of risk management in banking is expected to feature greater automation, real-time processing, and interactive reporting to enhance decision-making and regulatory compliance. This transformation requires embedding risk management into all organizational processes, reducing manual interventions, and ensuring seamless integration across operations.

The digitalization of banking services has introduced innovative solutions while simultaneously escalating cybersecurity risks. Research has explored user perceptions of online banking security, focusing on balancing usability with robust security measures [20, 21]. However, the increasing sophistication of cyberattacks such as identity theft, hacking, and malware-poses substantial challenges for financial institutions. Dupont et al. [22] highlight that current risk management practices are inadequate for addressing these threats, while Chen et al. [23] propose the AUSERA system, a tool designed to assess data vulnerabilities in banking applications. However, this approach has not yet been extended to online banking or developed into a comprehensive framework.

Various strategies and models have been proposed to mitigate cybersecurity risks, including threat modelling [24], security risk frameworks tailored for emerging economies [25], and multi-factor authentication systems [26]. Adaptive authentication methods, which analyze factors such as login time, browser type, and geographic location, offer an additional layer of protection by detecting high-risk login attempts [27]. Unified Authentication Platforms (UAPs) have also been introduced to integrate security mechanisms, ensuring system compatibility, enhancing user experiences, and reducing vulnerabilities.

2.2 Cyber security in online banking systems

The continuous digitalization of banking services has created opportunities for innovative and complex consumer solutions [28]. By 2030, internet-based banking is anticipated to be seamlessly integrated, insights-driven, and highly purposeful. Previous research has examined users' perceptions and awareness of security and threats in adopting online banking systems, focusing on the balance between usability and security features, such as digital certificates [20, 21, 29].

Despite these advancements, the digitalization of banking has increased cybersecurity risks. Cyberattacks, including identity theft, malware, and hacking, are rising threats to financial institutions. Dupont et al. [22] highlight that current risk management practices are insufficient to address the sophisticated and integrated nature of these threats. Chen et al. [23] proposed the AUSERA system to assess data vulnerabilities in banking applications, but its scope has yet to be extended to online banking or integrated into a comprehensive management framework. Studies also emphasize the cascading effects of technical failures, stemming from

malware attacks, data integrity issues, and system incompatibilities [22, 30].

Research has identified various strategies to address these risks. Commonly used methods include security policy enforcement and employee awareness training [31]. Models have been developed to assess cybersecurity risks in online banking, particularly in emerging economies [25]. Threat modelling has also been employed to evaluate vulnerabilities and locate attack paths [24, 32]. Additionally, Vinoth et al. [33] analyzed cybersecurity threats in cloud-based banking and e-commerce, offering insights into how these vulnerabilities can be mitigated.

A notable approach involves shifting security responsibilities away from users. Choubey and Choubey [34] propose ten essential security features to enhance protection, advocating for unified security mechanisms across banks to streamline testing and address compatibility issues. User access controls, such as biometric authentication and one-time PINs, have been widely examined [35–37]. In the United Kingdom, Strong Customer Authentication (SCA) regulations now mandate multi-layered security mechanisms for online banking and payments [38]

To further strengthen cybersecurity, adaptive authentication methods have been proposed. These systems analyze multiple parameters, including login time, browser type, and geographic location, to identify and mitigate high-risk login attempts [27]. Unified Authentication Platforms (UAPs) offer a consolidated solution, improving user experience and minimizing vulnerabilities by leveraging adaptive controls and behaviour analysis.

2.3 Risk management frameworks

Modern threat identification approaches in cybersecurity increasingly emphasize the logical decomposition of risk scenarios through attack, vulnerability, and fault tree analysis. While the banking industry cannot directly adopt a single risk assessment model for online banking, several frameworks can be tailored and integrated to address specific challenges. For example, the STRIDE model categorizes threats based on attackers' intentions, while attack trees provide a formalized method to describe potential attack paths. An integrated approach combining STRIDE and threat tree analysis [39] has been applied to online banking systems to identify security threats via a layered decomposition approach. Similarly, Threat, Vulnerability, and Risk Analysis (TVRA) incorporates threat tree modelling but does not fully utilize STRIDE elements [40].

Threat analysis is also supported by attack libraries such as MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) and the Open Web Application Security Project (OWASP) [41]. OWASP regularly updates its list of the top 10 common web application vulnerabilities, linking them to related hardware and software weaknesses (CWE). To quantify risks, frameworks like the Common Vulnerability Scoring System (CVSS) assign numerical scores to software vulnerabilities based on their severity, enabling organizations to prioritize actions and coordinate responses effectively [42].

Cybersecurity risk assessment tools and methods have matured, with some automated solutions leveraging real-time data to comply with international standards. Frameworks for critical infrastructure protection [43–46] explore cascading risks, the interdependencies of operations, and the broader organizational impacts of cyberattacks. Decision-support tools, such as the Integrated Risk Management System (IRMS), facilitate systematic risk identification and multi-user assessments, but they lack a specific focus on cybersecurity or banking-related applications [47]. Similarly, a decision-analysis-based framework proposed by Ganin et al. [48] prioritizes countermeasures by evaluating information, physical, and social aspects of cybersecurity risks. Further enhancements to this framework could incorporate adaptive threat characteristics and countermeasure effectiveness to assess attack likelihood more accurately.

Holistic approaches to cyber risk management, particularly to emerging technologies like the Internet of Things (IoT), have also been proposed. For example, Radanliev et al. [45, 46] developed an architecture for assessing the economic impact of cyber risks in Industry 4.0 networks. However, its application to the banking sector remains underexplored. A security risk management model for online services [49] has been validated in real-world organizational environments, emphasizing the importance of identifying attack scenarios and prioritizing risk treatments. The study concludes that grouping threats into predefined cases can expedite risk identification, and further work should focus on improving reporting metrics for more actionable insights.

The increasing dependence on online banking has escalated the need for robust cybersecurity frameworks to manage cyber risks effectively. Two widely recognized frameworks for cyber risk management are the ISO 27001 and the NIST Cybersecurity Framework (CSF). Both frameworks are used by organizations worldwide, including those in the financial sector, to ensure the confidentiality, integrity, and availability of their data and services. The ISO 27001 standard provides a systematic approach to managing sensitive company information through an Information Security Management System (ISMS). ISO 27005 focuses on the management of information security risks, offering a structured process for risk assessment, treatment, and mitigation. The NIST CSF provides a set of guidelines designed to help organizations manage cybersecurity risks based on five core functions: Identify, Protect, Detect, Respond, and Recover. It emphasizes risk-based decision-making and continuous improvement, focusing on aligning cybersecurity strategies

with business objectives. The ISO framework adopts a top-down approach, where risk management is driven by senior management. It places a significant emphasis on formal documentation and the establishment of an ISMS, which outlines the processes and controls required to protect information assets. In the context of online banking, ISO 27001 provides a robust and formal approach to ensuring that all aspects of the bank's information systems, from databases to customer interactions, are secure. The ISO approach can be resource-intensive, especially for smaller banks or fintech startups. The NIST framework is more flexible and adaptable, allowing organizations to choose cybersecurity practices that best align with their specific needs and maturity level. The framework's core functions-Identify, Protect, Detect, Respond, and Recover-provide a comprehensive, yet adaptable, approach to managing risks. NIST CSF's flexible approach is well-suited for online banking, where technological advancements and cyber threats are constantly evolving. Though NIST CSF offers flexibility, it can be difficult to implement without clear guidance on specific technical controls. This could be a challenge for smaller banks or those with less experience in cybersecurity risk management.

2.4 Limitations and research gaps

Traditional security risk assessment methods often begin by identifying critical infrastructure and assets with potential business impacts. While many studies emphasize quantifying risk ratings, few propose a comprehensive cybersecurity risk assessment and management framework. Existing approaches struggle to adapt to the evolving threat environment in online banking, where vulnerabilities emerge at different stages due to new features or attack vectors. Current methods rarely account for changes in threat landscapes, cascading impacts, or unique risk factors specific to the banking sector. Additionally, these methodologies often fail to integrate existing security features into their assessment processes, resulting in siloed evaluations rather than holistic risk management.

Risk management, being an iterative process, should move beyond a rigid, tick-box methodology. To address these gaps, a more integrated framework is needed-one that combines various models to continuously identify, assess, and manage risks in an interconnected and comprehensive manner. Such a framework should consider existing security measures within online banking systems and their interplay with vulnerabilities, enabling a more nuanced understanding of risk exposure. By tailoring this approach to the banking environment, it will provide a holistic solution rather than a one-size-fits-all model.

Developing a user-friendly yet effective framework poses challenges, particularly in ensuring that tools are both accessible to smaller organizations and capable of delivering meaningful results. One major hurdle is balancing timely decision-making in risk treatment with avoiding overly detailed analyses that may hinder actionable outcomes. This can be addressed by adopting a standardized, systematic, and partially automated methodology that simplifies processes while maintaining rigour.

The proposed framework aims to leverage well-established methodologies, such as NIST standards and the ISO series, and incorporate component-driven risk management approaches. These will serve as the foundation for creating a design that aligns with the unique requirements of online banking environments. By translating these requirements into actionable control objectives, the framework will ensure alignment with risk treatment tasks and compliance needs.

A key goal of the framework is to provide a comprehensive view of risk exposure. This involves assessing general threat scenarios for online banking systems alongside specific cybersecurity risks. The broader inclusivity of this approach will relate to vulnerability findings and control gaps, improving decision-making and prioritizing risk treatment activities. By ensuring that assessments address interdependencies rather than isolated risks, the framework will help organizations better understand their overall threat landscape and respond effectively.

3 Proposed integrated risk management framework

The proposed integrated risk management approach is intended to understand, manage, monitor and communicate risks for online banking systems. It included concepts that serve as a common language for describing security elements necessary for digital banking. The framework was designed to support systematic assessment and recursive management process better than the existing standalone approaches evaluated in Sect. 2.

3.1 Design objectives

The framework was created in line with ten objectives that were determined throughout the study of related artefacts, together with difficulties and motivations identified in earlier sections.

O-1 To define and apply unified taxonomy across risk management process: A unified taxonomy ensures that security risks in online banking systems are consistently categorized, facilitating clearer communication and more effective risk assessment. By standardizing risk terminology, this objective facilitate stakeholders-such as banks, regulators, and cybersecurity teams to understand and manage risks across various security domains, reducing the possibility of miscommunication or overlooked threats.

O-2 To consider dynamic environment and evolving technologies of banking sector: The banking sector is rapidly evolving, with technologies like AI, cloud computing, verifiability, zero-trust, and blockchain reshaping the ways to deliver the core services. This objective ensures that the framework stays relevant by addressing emerging threats associated with these emerging and new technologies, enabling banks to adapt quickly to new risks while maintaining robust security measures in online banking systems.

O-3 To enable usage by both service providers and consumers of online banking services: The framework should be accessible to both banks and customers, ensuring that service providers can manage risks effectively while allowing consumers to understand and take proactive steps to protect their own sensitive data. This collaborative effort between consumers and service providers could improve the security posture of both parties in the digital banking ecosystem.

O-4 To be applicable for banks of any size and type: The framework must be adaptable to suit organizations of all sizes. This flexibility ensures that both large and small financial institutions can adopt the framework to assess and mitigate risks, enhancing the overall security of online banking systems.

O-5 To simplify identification of general threat scenarios: This objective ensures that unwanted communication is identified in timely fashion by providing a clear and straightforward method and policies for identifying common threats such as phishing, malware, and social engineering attacks. This would help banks and customers quickly address the most prevalent and damaging forms of cyberattacks in online banking environments.

O-6 To identify specific threat trends related to online banking systems: This objective focuses on recognizing and understanding specific threat patterns or trends that are unique to online banking systems, such as credential stuffing attacks or man-in-the-middle attacks. By identifying these trends early, banks can better protect their digital infrastructure and mitigate emerging threats in real-time.

O-7 To consider cascading effects of exploited security features: This objective ensures that the cascading effects-where one compromised security feature can lead to the exploitation of others are thoroughly considered. Addressing these effects is crucial for mitigating to ensure integrity of the entire online banking system.

O-8 To ease decision-making and facilitate communication on risk treatment tasks: This objective ensures that the framework provides a clear methodology for evaluating risks, enabling decision-makers to prioritize and implement risk treatment strategies efficiently. Additionally, it enhances communication between banking staff, regulators, and customers regarding the handling of security incidents.

O-9 To identify existing security controls and suggest additional countermeasures: This objective ensures that the framework helps institutions assess the effectiveness of existing security controls in their online banking systems, such as firewalls, multi-factor authentication (MFA), and encryption. Furthermore, it proposes additional countermeasures to fill gaps, ensuring a robust defense against evolving cyber threats.

O-10 To facilitate recurring and continuous risk monitoring: This objective aims to establish a framework that supports continuous monitoring and recurring assessments of risks. By doing so, banks can stay ahead of threats, maintain security hygiene, and adapt to new vulnerabilities as they emerge, ensuring the security of online banking systems.

3.2 Characteristics of the proposed framework

The proposed framework was built with characteristics designed to meet specific objectives outlined above. It is dedicated to manage cyber security risks for online banking systems through a centralised and recursive process. The execution of the framework can be optimised and ultimately be automated by software tools.

3.2.1 Integrated risk management process with zero-trust approach

Existing frameworks and standards have been referenced in developing the integrated risk management approach, including NIST SP800 [50, 51], ISO 31000:2018 (ISO 31000 Risk management, 2013) [52], ISO 27001:2013 (ISO/IEC 27001 Information security management, 2013) [51], and ISO 27005:2018 [53] are generally applicable to all types of organisations including online banking environments. The basic structure of the referenced process from ISO 27005 standard is illustrated in Fig. 1 [54]. Each iteration incorporates a risk assessment and analysis stage to determine appropriate treatment decisions, hence supporting risk communication and monitoring cycles. There are two decision points determining whether the risks identified would be accepted or should be treated with appropriate strategies. The zero-trust framework operates in the principle of least privileged access control mechanism which means first verifying the identity or communication and then granting access while considering policies in a dynamic and changing environment. The Zero Trust model assumes that no entity either from the inside or from the outside is trustworthy by default. Zero Trust can be pivotal in providing effective measures against zero-day attacks while considering continuous authentication, enforcing least-privilege access, and rigorous monitoring to prevent and mitigate potential zero-day security breaches.

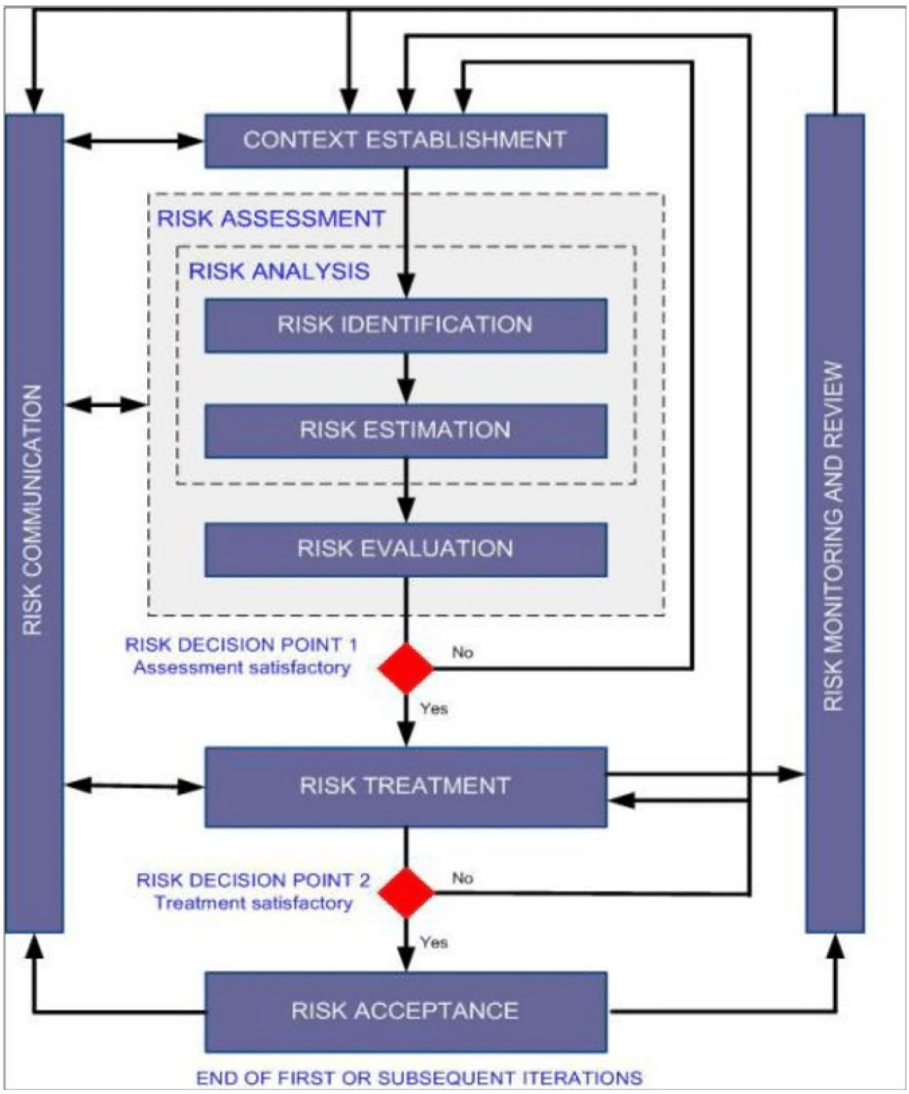

Fig. 1 Risk management process from ISO 27005 standard [54]

3.2.2 Adaptive and extensive capabilities

With the dynamic nature of banking operations and evolving technologies, the framework was designed to be extensible in capturing cascading effects of vulnerabilities and threats, and is adaptive in responding to emerging threats and security features. The risk identification steps within designed process have been generalised with pre-determined tables. The content is customisable to fit specific system design and features, yet generalised to be easily adopted by most users. The ability to record previous assessment results and predict future state based on data analysis is essential for updating existing tables and support an iterative management cycle. The proposed tool can be used to reflect the existing maturity of risk management practices and work towards desired level.

3.2.3 Risk management modeling

The proposal consists of multiple models that are essential to develop an integrated cyber security risk management approach. Based on the risk management process defined in the previous section, numerous concepts, models, and techniques have been explored to support the desired outcomes.

In this paper, terms and concepts composing the proposed framework are adopted from the NIST and explained as below [55]:

- **Event**: An occurrence or modification of specific circumstances.
- **Environment**: The settings and conditions of impacts on a system that are determined by context.

- **Vulnerabilities**: Any flaw that might be exploited or activated by a threat source in a system's implementation, internal controls, security protocols, or implementation.
- **Threats**: Any situation or event that could potentially have a negative impact on an organisation's operations, assets, or people through the use of an information system, such as unauthorised access, information destruction or disclosure, information modification, or denial of service. Additionally, it considers the likelihood that the malicious source will be successful in exploiting a certain information system vulnerability.
- **Threat agents/source**: Purpose and technique intended to target the deliberate exploitation of a vulnerability or a circumstance and technique that could unintentionally cause a vulnerability.
- **Risks**: A measure of the extent a situation or event would endanger an entity, often based on two factors: negative effects that would result if it happened, and the possibility that it would happen.
- **Risk treatment**: Process to determine and implement security measures using the Information Security Management System (ISMS) against risks identified. Treatment approaches include avoiding, reducing, transferring or accepting risks.
- **Threat scenarios**: A collection of discrete threat occurrences connected to one or more threat sources.
- **Security controls/features**: A precaution or countermeasure recommended for an information system or organisation that is intended to ensure the confidentiality, integrity, and availability of its data and to comply with a set of established security standards.

4 Risk management

The proposed framework offers benefits in terms of increased online banking service security from the perspectives of both consumers and providers. The component-driven framework focuses on risk management and can be partially automated through a software tool to support process execution and iterative activities. Previously defined modelling concepts including security features, vulnerabilities, threats, and specific environment types are utilised for risk identification and description.

A Threat Model, Risk Model, and Meta Model form the foundation of the framework. The Meta Model defines the entire framework as notated with ArchiMate modelling tool in Fig. 2, with both Threat Model and Risk Model regarded as significant autonomous components. The diagram denotes realisation/influence relationship between components in terms of information structure and will be explained in details in the coming sections.

4.1 Threat modelling

The main goal of the Threat Model is to allow the proposed process to recognise and understand any potential threat scenarios that can be relevant in the context of online banking services. It is designed to support identification, categorisation and threat description. Based on the asset and environment types, the Threat Model can describe a threat with the characteristics of certain security features and agents that may attempt to exploit different domains. It considers

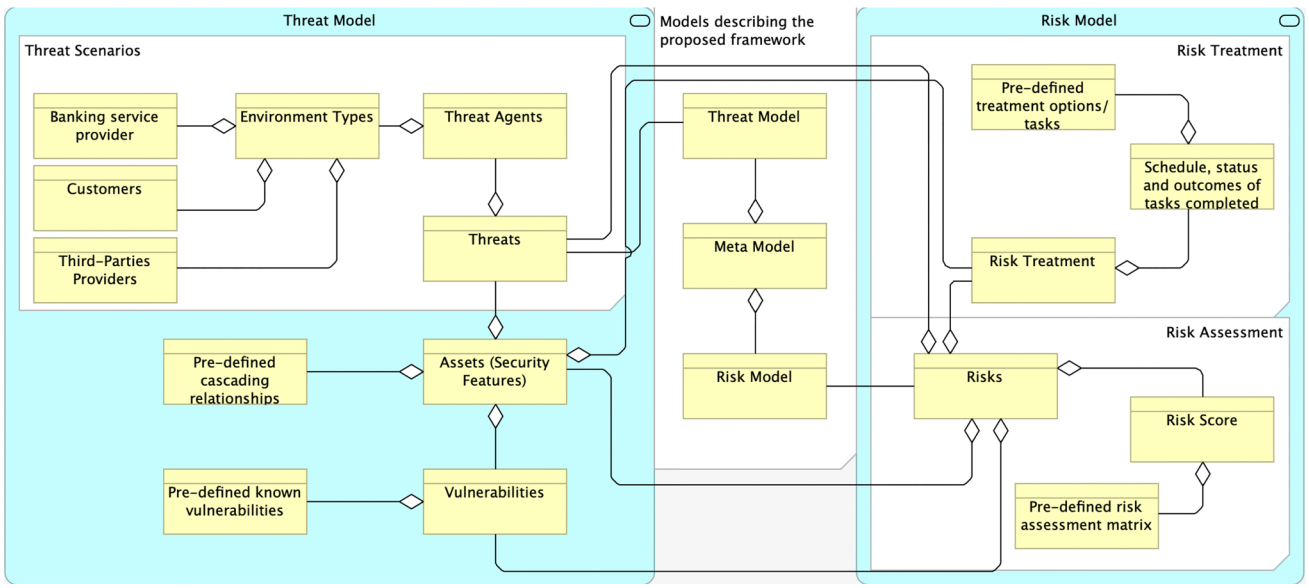

Fig. 2 Components of the proposed framework with information structure viewpoint

known weaknesses and pre-defined cascading relationships in existing security measures.

Figure 2 illustrates the core components of the proposed cybersecurity risk management framework for online banking systems. It consists of three important models: the Meta Model, the Threat Model, and the Risk Model. The Meta Model is the key model of the management process which interacts with the threat and the risk models. The Threat Model is responsible for identifying and categorizing potential threats relevant to online banking services, while the Risk Model evaluates and manages the risks associated with these threats on a scale of 0–10. Figure 2 highlights the flow of information and present the way how threats are identified, risks are analyzed, and decisions for risk treatment are facilitated under the Meta Model's guidance. Security features containing certain vulnerabilities may be exploited by one or more threats, and multiple relationships among security elements could exist and affect one another by means of cascading effects. The approach ignores any further potential collateral damage that threats may cause and not every environments along the supply chain have been discussed in detail since they may not be particularly relevant to the online banking services.

4.2 Assets (security features)

The model perceives security features defending unauthorised access and penetration of the online banking systems to be assets. Through the use of technical solutions and management activities, banks are dedicated to safeguarding three aspects of information: confidentiality, integrity, and availability. Any banking solution that does not comprehend specific attack strategies or the full process of online banking transactions may fail to offer counteract capabilities to stop various attacks.

Online banking systems are built on defense-in-depth strategy that layers a variety of security mechanisms, and are designed to safeguard both users' and the bank's environments during the whole transaction process. Security features defined in the proposed framework have been categorised into three areas as inspired by previous works [21, 25, 27, 56]. Examples of features in each category are summarised in following tables and can be further customised or expanded based on system design and future development.

- **Secure communication** (Table 1)—mechanisms in place to achieve functionality, security, and privacy during communication.
- **Authentication** (Table 2)—procedures that a system uses to compare users' credentials to that stored in databases or authentication servers in order to confirm their identities before granting access to the system.

Table 1 Security features of online banking systems—secure communication controls

Security features	Description
Digital certificates	Users and the banking system itself can be authenticated and an encrypted connection is established to the customers' or third-parties' browsers. The security protocol, Secure Sockets Layer (SSL) supports data confidentiality and security for online transactions. Digital certificates depend on the existence of a Public Key Infrastructure (PKI) and a trusted third-party, also known as the Certificate Authority (CA) to sign and attest to the authenticity of the certificates
Data encryption	Sensitive and private user data should be protected when in transit or stored at rest, especially under Open Banking which allows customers to share financial information across multiple banks and third parties

- **Monitoring** (Table 3)—usually refers to logging and threat detection techniques that constantly check for control flaws or suspicious transactions through automated tool such as a Security Incident and Event Management system.

Flaws may be contained in security measures safeguarding information assets and examples of particular vulnerabilities will be outlined in next section. Figure 3 illustrates an example of cascading relationships with potential flaws or assaults that allow attackers to further infect or bypass subsequent controls. Each asset identified in the framework may serve as a driver in realising additional exploitation channel, for example, a compromised digital certificate or encryption algorithm may provide opportunities for malicious actors to escalate their attacks towards other authentication and monitoring controls.

Due to the destructive effects such occurrence have on other assets and the complicated interdependence of features with increasing system integration, cascading impacts are regarded as a challenge that the organisation should be aware of and reviewing regularly to facilitate the risk management function. Additional features or changes in components should be tracked and updated in a timely manner to reflect any new influences that should be taken into considerations under the framework.

4.3 Threat scenarios

Based on the previous definition of threat scenarios, an appropriate combination of security feature and associated threat agents by environment type is considered as a threat scenario. The Threat Model maps potential source with its

Table 2 Security features of online banking systems—authentication controls

Security features	Description
Multi-factor authentication (MFA)	At least two verification factors are required from the following categories: something you know (username, password, positive identification or pass-phrase that refers to information only known to the users), something you have (One-Time Passwords (OTP) tokens or Short Message Service (SMS)), something you are (biometric features)
Adaptive authentication	Attribute factors such as usual login time, geolocation, application accessed through Single Sign-On (SSO) and the type of browsers or operating systems are analysed to create user profiles and define normal behaviour in login attempts. This mechanism can detect suspicious access attempts and prevent unauthenticated users from accessing online banking environments
Completely automated public Turing test to tell computers and humans apart (CAPTCHA)	Mechanism to prevent automated programmes (known as bots) from gaining unauthenticated access to the system. Users are required to input information from scrambled graphics which are designed to be difficult for automated robots to process
Device register	Users can only access the Online Banking Systems through pre-registered and known devices
Redirection authentication	Credentials are handed off or redirected to other third-parties sites for authenticating or processing transactions

Table 3 Security features of online banking systems—monitoring controls

Security features	Description
Continuous session monitoring	Automatic timeout from the banking session after a certain inactive period can prevent unauthorised intercept of information with unattended users. Concurrent login attempts can be detected with sessions to alert users or automatically logout from the banking system. It can be an indicator of compromised accounts with illegitimate attackers trying to gain access with authorised users at the same time

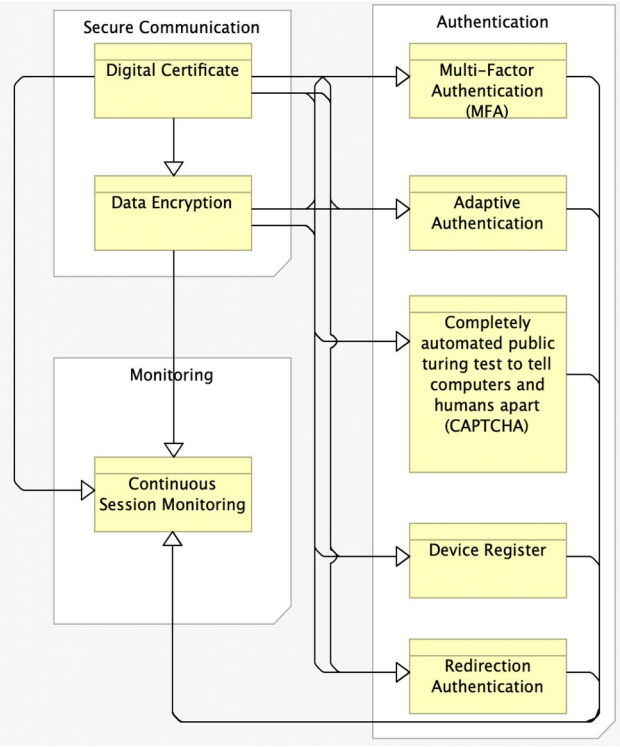

Fig. 3 Assets' dependence with cascading structure viewpoint

corresponding environment to raise awareness of concerns that may have previously gone unnoticed or unrecognised under ordinary risk management approach.

An entity that intends to compromise the security of an online banking service or has the potential to do so is referred to as a threat agent. They may be found in any one or more of the following three types of environments: Banking service provider's environment, Customers' environments and Third-Parties Providers' environments. Threat agents include both human and technological sources, the former includes both internal and external parties that may violate security of online systems by engaging in inadvertent, purposeful, or inactive behaviors, while the latter covers incidents involving malware, technical difficulties or failures.

The proposed model has neglected entities that make up surrounding environment that have no direct connection to the operation of banking system, which can also be referred to as cyberspace in general. Examples of threat types are specified in Table 4 grouped by environment as inspired by preceding studies [25, 39, 57, 58] and each indexed with an unique identifier. The identifiers are then used for mapping security features and applicable vulnerabilities in the coming sections.

4.4 Vulnerabilities

The Threat Model identifies common flaws for specific asset types that different threat agents may attempt to exploit (see

Table 4 Threat agents grouped by environment types

Threat	Name	Description	Banks	Customers	TPPs
TA.1	Spoofing	In order to deceive users into disclosing personal information or account login credentials that can be used for fraudulent activities, hackers may mimic a bank's website, email address, or phone number to appear genuine		✓	✓
TA.2	Tampering	Malicious party modifies data or content within the targeted system	✓		
TA.3	Repudiation	A harmful or unlawful action is carried out in the system by a bad actor, who subsequently denies the attack since insufficient capacity is in place to detect whether a certain person performed a specific activity	✓	✓	✓
TA.4	Information disclosure	When a website mistakenly shares sensitive information with unauthorised users, also known as information leakage	✓		
TA.5	Denial of service (DoS and distributed DoS)	An attacker attempts to interfere with permitted access to resources or the postponement of critical operations. A distributed attack blocks visitors from accessing linked websites and online services by overburdening a server with internet traffic	✓	✓	✓
TA.6	Elevation of privilege	Threat actors start with a first infiltration in the environment before launching a privilege escalation assault. Further escalation to accounts with administrative, root, or more advantaged privileges than the account that was first hacked is typically the second stage in the cyberattack chain. There are two categories of escalation attacks, horizontal privilege escalation entails getting access to another account's rights and vertical attack attempts to elevate beyond what a user, program, or other assets currently has in terms of privileged access	✓	✓	✓
TA.7	Fraud or theft	The use of stolen identity in criminal behaviour to gain access or tamper banking services via deceit is known as identity fraud. Identity theft occurs when sufficient information about a person's identity has been obtained by malicious actors to commit certain actions	✓	✓	✓
TA.8	Malicious hackers	The act of compromising the network or system through unauthorised access to an account or the online banking system	✓	✓	✓
TA.9	Malware	Malware refer to malicious software created by online crooks to steal data, and harm or crash systems. Typical types that are often encountered include worms, trojan horses, spyware, adware, and ransomware. A type of spyware, keyloggers, is a practice of tracking and recording each keystroke input without the user's knowledge or consent. Keystroke logging may be used to deduce user habits and private information	✓	✓	✓
TA.10	Man-in-the-middle (MitM) or man-in-the-browser (MitB)	It occurs when a perpetrator positions into a dialogue in the application layer between users and the browser, either to eavesdrop or to pretend to be one of the participants, creating the impression that regular information is being exchanged. The adversary is given access to read, write, modify, and delete browser data without the user's knowledge	✓	✓	✓

Table 4 (continued)

Threat	Name	Description	Banks	Customers	TPPs
TA.11	Open redirect attack	A person can manipulate a redirect or forward to another URL when the banking system has an open redirect vulnerability. An attacker might provide a URL that sends an unwary victim from a legal domain to an attacker's site if the system fails to authenticate untrusted user input	✓		
TA.12	Buffer overflow	By overwriting some of the application's memory, attackers take advantage of buffer overflow flaws to change the route of execution. The malicious data can include code that is intended to set off particular events, thereby delivering the attacked program new instructions that might lead to unauthorised access to the system	✓		
TA.13	Session hijacking	Attackers attempting to compromise the session token by stealing or foretelling a working session token in order to visit the web server without proper authorisation	✓	✓	✓
TA.14	Cryptography attack	A strategy for getting beyond a system's security by identifying a flaw in a code, cypher, cryptographic protocol, or key management system	✓	✓	✓
TA.15	Injection	Injection can occur in different aspects including browsers or Structured Query Language (SQL) when malicious code is being inserted into servers	✓	✓	✓
TA.16	Logic bomb	When certain logical conditions is satisfied, such as amount of transactions that have been performed or on a certain date, a series of software instructions that may attack an operating system, an application, or a network and convey a malicious payload will be executed	✓		
TA.17	Optical character recognition (OCR)-based attack	OCR technology that can identify and extract text included in images such as photos and papers	✓		
TA.18	Side-channel attack (SCA)	A security exploit that tries to acquire data from or affect the program execution of a system by measuring or exploiting indirect effects of the system or its hardware rather than focusing on the program or its codes directly. It includes information gathered from data leaks that occur during communication or system access. For example, characteristics of the targeted device's hardware, software, or communication media can be aggregated to gain valuable sensitive information	✓	✓	✓
TA.19	Sniffing	The process of intercepting communication or directing it toward a destination so that it may be recorded, examined, and kept track of. Attackers may intercept and read any network packet containing plain-text data. Usernames, passwords, secret phrases, financial information, or any other information that the attacker might find valuable can be obtained to launch further attacks	✓	✓	✓
TA.20	Password attack	Attackers may utilise malicious cracking or guessing tools and techniques to compromise authentication controls. Common types of techniques include brute-forcing, dictionary attacks and credential stuffing	✓	✓	✓
TA.21	Device registration Attack	Attackers gaining unauthorised access can enrol additional devices to the associated accounts. It would be possible to strengthen the attackers' position, surreptitiously spread the assault, and move lateral across the targeted network	✓	✓	✓

Table 4 (continued)

Threat	Name	Description	Banks	Customers	TPPs
TA.22	Security assertion markup language (SAML) Attack	It allows actors to access federated services such as SSO by forging SAML replies and avoiding Active Directory Federation Services (ADFS) verification	✓	✓	✓

Table 5 General vulnerabilities identified from CWE Top 25:2022 and OWASP Top 10:2021

Vulnerability	OWASP ID and Name	CWE ID and Name
VG.1	A01:2021 Broken Access Control	CWE-22 Improper limitation of a pathname to a restricted directory (Path Traversa)
VG.2	A01:2021 Broken Access Control	CWE-352 Cross-Site Request Forgery (CSRF)
VG.3	A01:2021 Broken Access Control	CWE-862 Missing authorisation
VG.4	A01:2021 Broken Access Control	CWE-276 Incorrect default permissions
VG.5	A03:2021 Injection	CWE-79 Improper neutralisation of input during webpage generation (Cross-Site Scripting/XSS)
VG.6	A03:2021 Injection	CWE-20 Improper input validation
VG.7	A03:2021 Injection	CWE-78 Improper neutralisation of special elements used in an operating system command (OS Command Injection)
VG.8	A03:2021 Injection	CWE-77 Improper neutralisation of special elements used in a command (Command Injection)
VG.9	A03:2021 Injection	CWE-94 Improper control of generation of code (Code Injection)
VG.10	A04:2021 Insecure Design	CWE-434 Unrestricted upload of file with dangerous type
VG.11	A05:2021 Security Misconfiguration	CWE-611 Improper restriction of XML external entity reference
VG.12	A07:2021 Identification and Authentication Failures	CWE-287 Improper authentication
VG.13	A07:2021 Identification and Authentication Failures	CWE-798 Use of hard-coded credentials
VG.14	A07:2021 Identification and Authentication Failures	CWE-306 Missing authentication for critical function
VG.15	A08:2021 Software and Data Integrity Failures	CWE-502 Deserialization of untrusted data
VG.16	A10:2021 Server-Side Request Forgery (SSRF)	CWE-918 Server-Side Request Forgery (SSRF)
VG.17 to VG.25	Not Defined	CWE-787 Out-of-bounds write, CWE-89 Improper neutralisation of special element (SQL-injection),CWE-125 Out-of-bounds read,CWE-416 Use after free,CWE-476 Null pointer, CWE-189 Integer overflow, CWE-119 error in-memory buffer,CWE-362 Concurrent execution using shared resource with improper synchronisation,CWE-400 Uncontrolled resource consumption

Table 5). It is suggested to use the well-known CWE Top 25 list as of 2022 [59], which represents the prevalent and significant weaknesses at the moment and mapped against OWASP Top 10:2021 categories (OWASP Top Ten, 2021) as the most critical security risks to web applications, as the foundational list of vulnerabilities associated with security elements in place. These can result in exploitable weaknesses that enable adversaries to entirely take over a system, steal data, or stop the online banking systems from functioning properly. Since they are published regularly and are frequently simple to detect, it facilitates vulnerability management and assessment processes. The classification scheme can be altered and customised in accordance to user needs and system designs or interactions with individual components.

Apart from published general flaws, a register of specific vulnerabilities in the OBS context should be maintained according to the asset inventory and control design of each banking system. Examples of pre-defined weaknesses are described in Table 6 according to security features identified from the proposal.

Examples of defined threats and vulnerabilities are mapped using identifiers, which are listed in Table 7. They are associated with applicable security features to form comprehensive risk scenarios as the input for Risk Model to perform assessment and decision-making on risk treatment strategies.

4.5 Risk models

The basic goal of the Risk Model is to detect, evaluate, and manage risks in a way that takes into consideration all significant risk perceptions. The model is made up of

Table 6 Specific vulnerabilities for online banking systems

Vulnerability	Name	Description
VS.1	Weak cryptography algorithms	Inappropriate cyphers such as short key lengths, shoddy encryption techniques, and careless key handling are examples of poorly constructed cryptographic methods
VS.2	Unpatched known vulnerabilities	Neglected flaws may become a preferred entry point for malicious actors to compromise networks and perform ransomware attacks
VS.3	Obsolete, unsupported or unapproved components	These components are not covered by proper security updates and patches that can shield users from known vulnerabilities
VS.4	Issues in specifications or integration among systems and with third-party components	Since third-party applications are created, distributed, and maintained by independent organisations, it implies that the bank usually has little control over known security flaws and takes considerations into configuring integration along the supply chain
VS.5	Improper certificate validation	A certificate is either not validated by the system or is validated erroneously. An attacker may be able to impersonate a trusted entity by interfering with the communication between the host and client when a certificate is malicious or incorrect
VS.6	Missing CAPTCHA protection in URLs	Sending a specially crafted request to the web interface would allow an attacker to take advantage of this weakness. A successful vulnerability could enable the attacker to determine the validity of a username and the user's identity
VS.7	Improper generation and protection of session identifier token	Session ID should not be re-used or predictable to attackers. Any transfer of the value must be encrypted as regarded as sensitive data
VS.8	Improper restriction of invalid sessions	Sessions fail to be invalidated when users quit the browsers without logging out, or both session objects on the server and the session identifier cookie on the client browser have not been rendered invalid

two important components, each of which is discussed in the parts that follow.

4.6 Risk assessment module

The purpose of this component is to assess the severity of a specific risk identified using a pre-defined qualitative matrix. For ease of use, this module describes likelihood and impact on a scale as suggested by ISO/IEC 27005:2018 standard, which yields risk scores on a scale of 0–8 and five-level impact/likelihood ranging from very low to very high (Table 8). In order to explain risk score values as the combination of likelihood and impact values, both levels can also be expressed as numbers. Score ranging from 0–2 would be classified as low risk, 3–5 as medium risk and 6–8 as high risk.

Other appropriate risk assessment methodologies can be applied and customised in the framework, such as the OWASP Risk Rating Methodology which estimates likelihood and impact levels on a three-level scale (low, medium and high).

4.7 Risk treatment module

For this component, four risk treatment strategies set out by the ISO/IEC 27005:2018 standard are taken into account for determining decision-making options: risk modification, retention, avoidance, and sharing. Risk modification tasks are pre-defined additional security controls based on objectives (preventative, detective, or corrective), which will be determined and scheduled by severity levels. The selected actions will be tracked with their completion status as well as outcomes for updating the inventory of security features in place and to initiate the next management cycle.

Risk treatment options and classification can be customised and should be updated regularly to reflect changes in the system or previous assessment results. The current proposal focuses on technical security tasks and controls with administrative nature are out of scope. The model also abstracts away future actions or suggested tasks for alternative treatment including risk retention, avoidance, and sharing options.

A list of pre-determined tasks help select appropriate treatments based on threat classifications. Table 9 indicates a

Table 7 Mapping between assets, threats and vulnerabilities

Threat	Threat name	Applicable vulnerabilities	Applicable assets
TA.1	Spoofing	VG.1, VG.2, VG.3, VG.11, VG.16, VS.2, VS.3, VS.4, VS.5, VS.6	Digital certificate
TA.2	Tampering	VG.4, VG.5, VG.10, , VG.12, VG.13, VG.14, VG.15, VG.17, VS.2, VS.3, VS.4	Data encryption, MFA, adaptive authentication, device register
TA.3	Repudiation	VG.2, VG.4, VG.6, , VG.12, VG.14, VG.24, VS.2, VS.3	All
TA.4	Information disclosure	VG.1, VG.2, VG.3, VG.4, VG.6, VG.7, VG.8, VG.9, VG.10, VG.11, VG.12, VG.13, VG.14, VG.15, VG.16, VG.17, VG.18, VG.19, VG.24, VS.1, VS.2, VS.3, VS.4, VS.6, VS.7, VS.8	All
TA.5	Denial of service (DoS and distributed DoS)	VG.5, VG.10, VG.17, VG.21, VG.22, VG.23, VS.2, VS.3	All
TA.6	Elevation of privilege	VG.1, VG.2, VG.3, VG.4, VG.6, VG.10, VG.12, VG.13, VG.14, VG.16, VG.17, VS.2, VS.3, VS.4, VS.6	All
TA.7	Fraud or theft	VG.1, VG.2, VG.3, VG.6, VG.10, VG.12, VG.13, VG.14, VG.16, VG.19, VG.24, VS.1, VS.2, VS.3, VS.6	All
TA.8	Malicious hackers	VG.1, VG.2, VG.3, VG.4, VG.5, VG.6, VG.7, VG.8, VG.9, VG.10, VG.11, VG.12, VG.13, VG.14, VG.15, VG.16, VG.17, VG.18, VG.19, VG.20, VG.21, VG.22, VG.23, VG.24, VG.25, VS.1, VS.2, VS.3, VS.4, VS.5, VS.6, VS.7, VS.8	All
TA.9	Malware	VG.5, VG.10, VS.2, VS.3, VS.4	All
TA.10	Man-in-the-middle (MitM) or man-in-the-browser (MitB)	VG.1, VG.7, VG.8, VG.9, VG11, VG.18, VG.19, VS.2, VS.3, VS.4	All
TA.11	Open redirect attack	VG.1, VG.5, VG.6, VG.7, VG.8, VG.9, VG.11, VG.12, VG.13, VG.14, VG.16, VG.18, VG.24, VS.2, VS.3, VS.4, VS.6	Redirection authentication
TA.12	Buffer overflow attack	VG.17, VG.20, VG.21, VG.22, VG.23, VG.25, VS.2, VS.3	All
TA.13	Session hijacking	VG.5, VG.7, VG.8, VG.9, VG.18, VG.24, VS.2, VS.3, VS.4, VS.7, VS.8	Continuous session monitoring
TA.14	Cryptography attack	VG.10, VG.19, VS.1, VS.2, VS.3	Digital certificate and data encryption
TA.15	Injection	VG.5, VG.7, VG.8, VG.9, VG.10, VG.18, VS.2, VS.3, VS.4	All
TA.16	Logic bomb	VG.5, VG.6, VG.21, VG.22, VG.23, VG.24, VS.2, VS.4	All
TA.17	Optical character recognition (OCR)-based attack	VG.5, VG.6, VG.10, VG.16, VG.19, VS.2, VS.3	Adaptive authentication
TA.18	Side-channel attack (SCA)	VG.12, VG.13, VG.14, VG.16, VG.19, VG.25, VS.2, VS.3, VS.4	All
TA.19	Sniffing	VG.5, VG.7, VG.8, VG.9, VG.19, VS.2, VS.3, VS.4, VS.7, VS.8	All
TA.20	Password attack	VG.4, VG.6, VG.10, VG.12, VG.13, VG.14, VG.15, VG.16, VS.2, VS.3, VS.4	All
TA.21	Device registration attack	VG.2, VG.3, VG.4, VG.12, VG.13, VG.14, VG.15, VG.16, VG.24, VS.2, VS.3	All authentication controls
TA.22	Security assertion markup language (SAML) attack	VG.2, VG.4, VG.7, VG.8, VG.9, VG.11, VG.13, VG.16, VG.24, VS.2, VS.3, VS.4, VS.7, VS.8	All authentication controls

Table 8 Example of risk matrix by risk likelihood, impact, severity and scores

Impact/likelihood	Very low	Low	Medium	High	Very high
Very low	Low (0)	Low (1)	Low (2)	Medium (3)	Medium (4)
Low	Low (1)	Low (2)	Medium (3)	Medium (4)	Medium (5)
Medium	Low (2)	Medium (3)	Medium (4)	Medium (5)	High (6)
High	Medium (3)	Medium (4)	Medium (5)	High (6)	High (7)
Very high	Medium (4)	Medium (5)	High (6)	High (7)	High (8)

Table 9 Examples of pre-defined risk treatment tasks

Task	Name	Applicable threats
RT.1	Code review	TA.2, TA.4, TA.6, TA.8, TA.9, TA.12, TA.15, TA.16, TA.22
RT.2	Deploying anti-malware softwares	TA.9
RT.3	Forensic investigation	TA.1, TA.2, TA.3, TA.4, TA.5, TA.6, TA.7, TA.8, TA.9, TA.10, TA.11, TA.12, TA.13, TA.14, TA.15, TA.16, TA.17, TA.18, TA.19, TA.20, TA.21, TA.22
RT.4	Fraud detection and prevention	TA.1, TA.3, TA.7
RT.5	Identity and privileged access management and review	TA.2, TA.4, TA.6, TA.7, TA.8, TA.21
RT.6	Incident response and recovery planning	TA.1, TA.2, TA.4, TA.5, TA.8, TA.9
RT.7	Inventory and patching management	TA.4, TA.8, TA.19, TA.21
RT.8	Monitoring and audit logging	TA.3, TA.4, TA.5, TA.6, TA.8, TA.9, TA.10, TA.11, TA.14, TA.15, TA.18, TA.19
RT.9	Network defence and traffic monitoring	TA.2, TA.3, TA.4, TA.5, TA.6, TA.8, TA.10, TA.11, TA.12, TA.13, TA.19, TA.22
RT.10	Penetration testing	TA.2, TA.4, TA.5, TA.6, TA.8, TA.9, TA.10, TA.12, TA.13, TA.14, TA.15, TA.17, TA.18, TA.19, TA.20, TA.21, TA.22
RT.11	Security configuration review	TA.2, TA.4, TA.5, TA.6, TA.7, TA.8, TA.9, TA.10, TA.11, TA.12, TA.13, TA.14, TA.15, TA.17, TA.18, TA.19, TA.20, TA.21, TA.22
RT.12	Security requirements specification	TA.2, TA.4, TA.5, TA.6, TA.7, TA.8, TA.9, TA.10, TA.11, TA.12, TA.13, TA.14, TA.15, TA.17, TA.18, TA.19, TA.20, TA.21, TA.22
RT.13	Service provider management	TA.1, TA.2, TA.3, TA.5, TA.6, TA.8, TA.9, TA.10, TA.11, TA.13, TA.14, TA.15, TA.18, TA.19, TA.20, TA.21, TA.22
RT.14	System hardening	TA.2, TA.4, TA.5, TA.6, TA.8, TA.9, TA.10, TA.11, TA.12, TA.13, TA.14, TA.15, TA.17, TA.18, TA.19, TA.20, TA.22
RT.15	Vulnerability scanning	TA.2, TA.4, TA.5, TA.6, TA.8, TA.9, TA.10, TA.11, TA.12, TA.13, TA.14, TA.15, TA.17, TA.19, TA.20, TA.22

list of countermeasure examples that are appropriate for the majority of situations as inspired by former work and critical security controls suggested by Center for Internet Security [25, 60]) and can be extended with unique assignments.

4.8 Risk managment processes

The suggested method was developed in accordance with ISO 27005:2018 standard (justified in Sect. 4.2). The architecture of the process allows frequent and repeated iterations. The risk management process is shown in Fig. 4 from a business process viewpoint, and each of its component steps is elaborated below. All pre-defined tables and records that are concurrently being updated within the framework are illustrated in green colour, with business processes indicated in yellow with their associated input and/or output relationships with data sources.

5 Evaluation of the proposed framework

Based on the projected cyber-attack scenarios that are pertinent to the online banking services context, the proposed framework is targeted at delivering a thorough and holistic analysis of the security features, cascading vulnerabilities, and potential attacks. The proposal is evaluated with relevant applicability and comparison with existing risk management methodologies, as well as a review of objectives determined at the beginning of the research.

5.1 Applicability of the proposal and comparison with existing approaches

The proposed strategy is a methodical framework that incorporates all steps of detecting risks from a

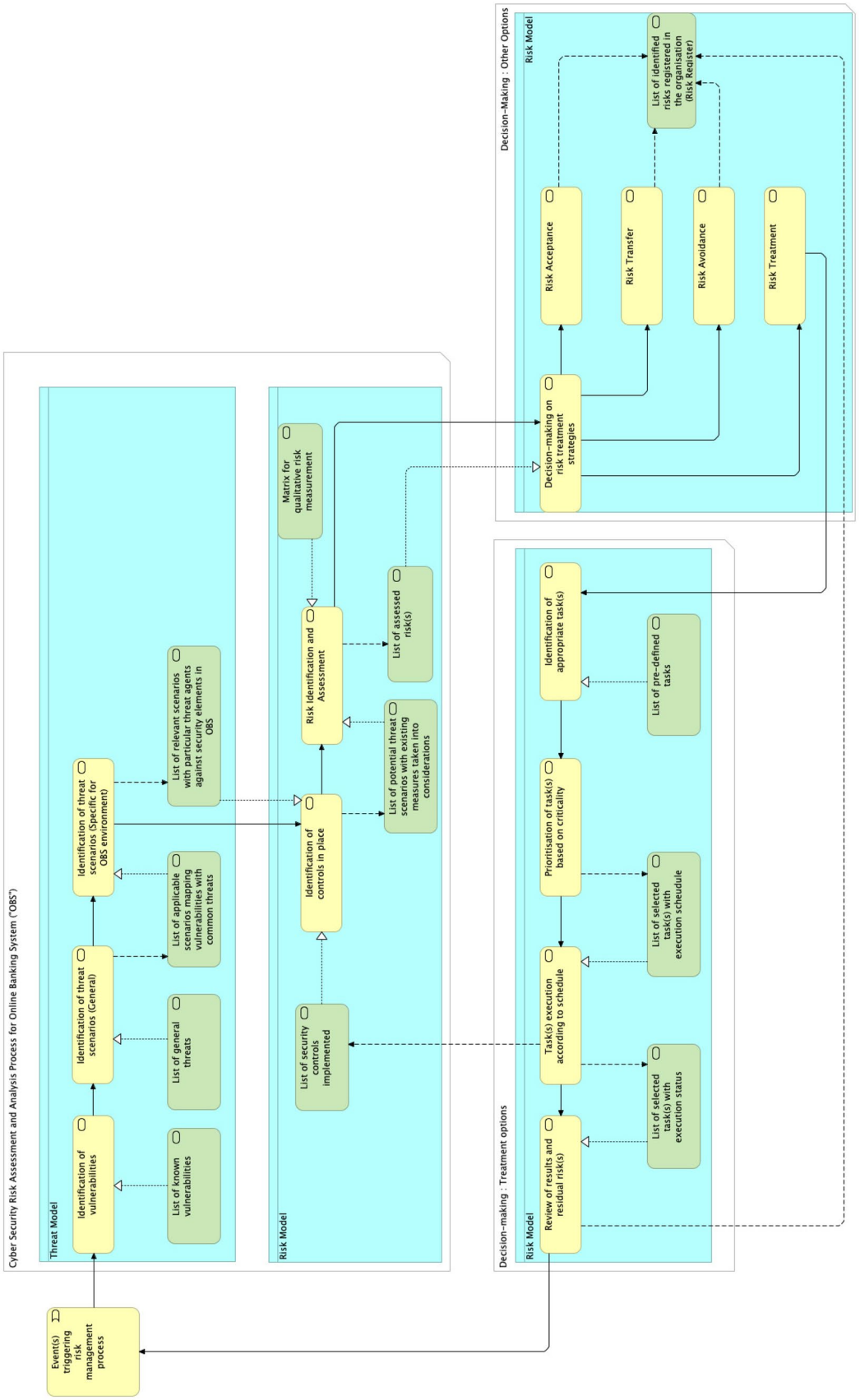

Fig. 4 Risk management process from ISO 27005 standard

comprehensive viewpoint. Stakeholders are made aware of hidden risks that might affect their vital usage and financial transactions, enabling them to take required precautions and security controls to prevent risks and threats from realising.

By incorporating existing standards into building an online banking services-specific risk management approach, the proposed framework addressed the gap identified (see Sect. 2.4). Following are the key distinctions and benefits between the proposal and present frameworks described in Sect. 2.3 which were explored throughout the research.

As security features are considered to be significant assets at initiating the proposed risk management process, ordinary asset identification and value estimation are not stressed in this research. Traditional decomposition and analysis of asset inventory management and identification would be more time-consuming compared to the novel proposal. In this research, users can focus on considering security components or supplementary features that are actually affected within the risk management cycles. The method described in this research facilitates the identification of weaknesses in an online banking service's security points and aids in prioritising risk management activities. The framework places less emphasis on in-depth studies and more on automated task selection and execution that leads to standardised risk treatment and comprehensive oversight capabilities. None of the existing approaches evaluated focuses on the initial impacts of vulnerabilities that may be influenced by the effects of cascading relationships.

5.2 Objective analysis

Every objective outlined in Sect. 4.1 for the suggested proposal has been achieved, as justified in this section.

- **O-1 To define and apply unified taxonomy across risk management process.** Different categorisation methodologies have been defined and established in the proposed framework with unified modelling concepts.
- **O-2 To consider the dynamic environment and evolving technologies of the banking sector.** A customisable approach which was designed for rapid and repeated iterations is able to reflect dynamic and adaptive nature against the evolving changes in the online service context.
- **O-3 To enable usage by both service providers and consumers of online banking services.** The framework was designed with the ease-of-use concept, which aimed at simplifying the overall risk management process with the capability to be updated and monitored within a single framework.
- **O-4 To be applicable for banks of any size and type.** Usability has been examined during the design phase and the proposal was designed to be adaptable by organisations or users with immature practices as a foundation to develop proper risk management function.
- **O-5 To simplify the identification of general threat scenarios.** The Threat Model was designed to pre-define and identify generic scenarios pertinent to online systems. Locating hidden or previously unidentified threats was facilitated by the threat scenarios and threat types set out in the framework.
- **O-6 To identify specific threat trends related to online banking systems.** The Threat Model was capable of extending into specific threat agents and scenarios in particular to the OBS context and can be tailored to fit certain circumstances or unique threat actors.
- **O-7 To consider cascading effects of exploited security features.** Dependency between components is evaluated and pre-established within the framework to automatically take potential cascading effects into consideration.
- **O-8 To ease decision-making and facilitate communication on risk treatment tasks.** The Risk Model was designed to be simple to comprehend and consistently applied throughout the recursive decision-making process, the outputs for treatment strategies can be easily tracked and communicated with different parties.
- **O-9 To identify existing security controls and suggest additional countermeasures.** The framework takes security features into consideration in assessing risks and contains a list of pre-defined countermeasures to be utilised, avoiding extra time and effort in performing in-depth analysis.
- **O-10 To facilitate recurring and continuous risk monitoring.** The initial process execution for a given online banking service is exacting, with subsequent iterations to be built on the adjustments established from the initial cycle. Changes triggered by security features or incidents can then be monitored and responded to within the framework.

6 Conclusions and future direction

This research proposes an integrated risk management framework tailored for online banking systems, designed to help banking service providers and consumers assess and manage cybersecurity risks associated with digital banking services. The framework aligns with recognized standards, such as ISO/IEC, and comprises four core components: a Threat Model, a Risk Model, a comprehensive Risk Management Methodology, and predefined treatment tasks.

Unlike traditional approaches that prioritize asset value and business criticality, this framework begins with identifying relevant threat scenarios based on existing security features. It then maps risks to specific assets, such as controls

and online service components, that could be affected. Risks are evaluated and addressed using decision-making rules and predefined tasks, ensuring a focused approach that targets the most likely sources of adverse events. This process facilitates efficient risk management across complex online banking systems by concentrating on actionable measures to mitigate potential threats. All initial design objectives for the framework have been achieved.

While the framework introduces several advantages, there are areas for further refinement and enhancement to encourage broader adoption and ease of use. Automation tools can support the framework's implementation, enabling consistent record-keeping and streamlining iterative processes. Initial threat scenario identification and vulnerability analysis can be enhanced by leveraging data on emerging threat trends specific to the financial sector. Additionally, automating risk matrix calculations tailored to the context of OBS would simplify risk level determination across different users while maintaining standardization.

Further details could be added to the predefined treatment activities, particularly with recommendations for methodologies that incorporate existing risk transfer and acceptance practices. Reporting metrics and logging mechanisms should also be explored as areas for future research, providing a foundation for tracking progress and outcomes. As technology evolves, the framework must be regularly updated to address new threats and vulnerabilities, ensuring its long-term relevance. It could also be generalized and validated through case studies, allowing for practical insights and feedback to improve the framework.

However, the research has some limitations. Access to confidential data and undisclosed vulnerabilities in online banking components was restricted, limiting the framework's ability to account for real-world complexities. The design and evaluation relied on publicly available vulnerability databases and known threat factors, potentially underestimating the actual risk exposure. Time constraints further restricted the validation of the framework with automated tools, which would enhance its ability to customize contexts and support decision-making processes.

Data availability No data is used.

References

1. Statista (2022) Online banking usage in Great Britain from 2007 to 2022. https://www.statista.com/statistics/286273/internet-banking-penetration-in-great-britain/. Accessed 12 May 2022
2. Alhaddad MM (2018) Artificial intelligence in banking industry: a review on fraud detection, credit management, and document processing. ResearchBerg Rev Sci Technol 2(3):25–46
3. Anagnostopoulos I (2018) Fintech and regtech: impact on regulators and banks. J Econ Bus 100:7–25
4. Dubey V, Sonar R, Mohanty A (2020) Fintech, regtech and contactless payments through the lens of covid 19 times. Int J Adv Sci Technol 29(6):3727–3734
5. Dzhaparov P (2020) Application of blockchain and artificial intelligence in bank risk management. Bank Risk Manag J 17(1):43–57
6. Li F, Lu H, Hou M, Cui K, Darbandi M (2021) Customer satisfaction with bank services: the role of cloud services, security, e-learning and service quality. Technol Soc 64:101487
7. Singh M, Tanwar KS, Srivastava VM (2018) Cloud computing adoption challenges in the banking industry. In: 2018 International conference on advances in big data, computing and data communication systems (icABCD), IEEE. pp 1–5
8. Amin M (2016) Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. Int J Bank Market 34:280–306
9. Chong AYL, Ooi KB, Lin B, Tan BI (2010) Online banking adoption: an empirical analysis. Int J Bank Market 28:267–287
10. Lipton A, Shrier D, Pentland A (2016) Digital banking manifesto: the end of banks? Massachusetts Institute of Technology, Cambridge
11. Mbama CI, Ezepue PO (2018) Digital banking, customer experience and bank financial performance: UK customers' perceptions. Int J Bank Mark 36:230–255
12. Mehdiabadi A, Tabatabeinasab M, Spulbar C, KarbassiYazdi A, Birau R (2020) Are we ready for the challenge of banks 4.0? Designing a roadmap for banking systems in industry 4.0. Int J Financ Stud 8(2):32
13. McKinsey &Company (2015) The future of bank risk management. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-future-of-bank-risk-management. Accessed 13 May 2022
14. Tursoy T (2018) Risk management process in banking industry. https://doi.org/10.13140/RG.2.2.14737.74085
15. Konovalova N, Kristovska I, Kudinska M (2016) Credit risk management in commercial banks. Polish J Manag Stud 13:90–100
16. Monnin P (2018) Integrating climate risks into credit risk assessment-current methodologies and the case of central banks corporate bond purchases. Council on Economic Policies, Discussion Note 4
17. Moradi S, Mokhatab Rafiei F (2019) A dynamic credit risk assessment model with data mining techniques: evidence from Iranian banks. Financ Innov 5(1):1–27
18. Leo M, Sharma S, Maddulety K (2019) Machine learning in banking risk management: a literature review. Risks 7(1):29
19. Stojanović D, Krstić MSM (2017) Modern approaches and challenges of risk management in electronic banking. Unspecified journal
20. Mahmadi FN, Zaaba ZF, Osman A (2016) Computer security issues in online banking: an assessment from the context of usable security. IOP Conf Ser Mater Sci Eng 160:012107
21. Svilar A, Zupančič J (2016) User experience with security elements in internet and mobile banking. Organizacija 49(4):251–260
22. Dupont B (2019) The cyber-resilience of financial institutions: significance and applicability. J Cybersecur 5(1):013
23. Chen S, Fan L, Meng G, Su T, Xue M, Xue Y, Liu Y, Xu L (2020) An empirical assessment of security risks of global android

banking apps. In: 2020 IEEE/ACM 42nd international conference on software engineering (ICSE), pp 1310–1322
24. Arachchilage NAG, Love S (2014) Security awareness of computer users: a phishing threat avoidance perspective. Comput Hum Behav 38:304–312
25. Alghazo JM, Kazmi Z, Latif G (2017) Cyber security analysis of internet banking in emerging countries: user and bank perspectives. In: 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS). IEEE, pp 1–6
26. Dhoot A, Nazarov AN, Koupaei ANA (2020) A security risk model for online banking system. In: 2020 Systems of signals generating and processing in the field of on board communications. IEEE, pp 1–4
27. Bakar KAA, Haron GR (2014) Adaptive authentication based on analysis of user behavior. In: 2014 Science and information conference. IEEE, pp 601–606
28. Bilan Y, Rubanov P, Vasylieva TA, Lyeonov S (2019) The influence of industry 4.0 on financial services: determinants of alternative finance development. Polish J Manag Stud 19:70–93
29. Yoon HS, Occeña LUIS (2014) Impacts of customers' perceptions on internet banking use with a smart phone. J Comput Inf Syst 54(3):1–9
30. Najaf K, Mostafiz MI, Najaf R (2021) Fintech firms and banks sustainability: why cybersecurity risk matters? Int J Financ Eng 8(02):2150019
31. Al-Alawi AI, Al-Bassam MSA (2020) The significance of cybersecurity system in helping managing risk in banking and financial sector. J Xidian Univ 14(7):1523–1536
32. Ngalo T, Xiao H, Christianson B, Zhang Y (2018) Threat analysis of software agents in online banking and payments. In: 2018 IEEE 16th international conference on dependable, autonomic and secure computing, 16th international conference on pervasive intelligence and computing, 4th international conference on big data intelligence and computing and cyber science and technology congress (DASC/PiCom/DataCom/CyberSciTech). pp 716–723. https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00125
33. Vinoth S, Vemula HL, Haralayya B, Mamgain P, Hasan MF, Naved M (2022) Application of cloud computing in banking and e-commerce and related security threats. Mater Today Proc 51:2172–2175
34. Choubey J, Choubey B (2013) Secure user authentication in internet banking: a qualitative survey. Int J Innov Manag Technol 4(2):198
35. Hammood WA, Abdullah Arshah R, Hammood O, Mohamad Asmara S, Al-Sharafi MA, Muttaleb A (2020) A review of user authentication model for online banking system based on mobile IMEI number. IOP Conf Ser Mater Sci Eng 769:012061. https://doi.org/10.1088/1757-899X/769/1/012061
36. Lupu C, Găitan VG, Lupu V (2015) Security enhancement of internet banking applications by using multimodal biometrics. In: 2015 IEEE 13th international symposium on applied machine intelligence and informatics (SAMI). IEEE, pp 47–52
37. Priya R, Tamilselvi V, Rameshkumar GP (2014) A novel algorithm for secure internet banking with fingerprint recognition. In: 2014 International conference on embedded systems (ICES). IEEE, pp 104–109
38. FCA (2022) deadline extension for strong customer authentication. https://www.fca.org.uk/news/statements/deadline-extension-strong-customer-authentication. Accessed 18 May 2022
39. Xin T, Xiaofang B (2014) Online banking security analysis based on stride threat model. Int J Secur Appl 8(2):271–282
40. Monteuuis J-P, Boudguiga A, Zhang J, Labiod H, Servel A, Urien P (2018) SARA: security automotive risk analysis method. In: Proceedings of the 4th ACM workshop on cyber-physical system security. CPSS '18, pp 3–14. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3198458.3198465
41. Owasp.org (2022) OWASP Top Ten | OWASP Foundation. https://owasp.org/www-project-top-ten/. Accessed 19 Jun 2022
42. Wang Y, Wang Y, Qin H, Ji H, Zhang Y, Wang J (2021) A systematic risk assessment framework of automotive cybersecurity. Autom Innov. https://doi.org/10.1007/s42154-021-00140-6
43. Kure HI, Islam S (2019) Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber Phys Syst Theory Appl 4(4):332–340
44. Kure HI, Islam S, Razzaque MA (2018) An integrated cyber security risk management approach for a cyber-physical system. Appl Sci 8(6):898
45. Radanliev P, Roure D, Nurse J, Nicolescu R, Huth M, Cannady S, Montalvo R (2019) Cyber risk impact assessment—assessing the risk from the IoT to the digital economy. https://doi.org/10.20944/preprints201903.0109.v1
46. Radanliev P, De Roure D, Nurse J, Nicolescu R, Huth M, Cannady S, Montalvo RM (2018) Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. https://doi.org/10.1049/cp.2018.0041
47. Arıkan A, Dikmen T, Birgönül MT (2009) A prototype risk management decision support tool for construction projects
48. Ganin A, Quach P, Panwar M, Collier Z, Keisler J, Marchese D (2017) Multicriteria decision framework for cybersecurity risk assessment and management. Risk Anal. https://doi.org/10.1111/risa.12891
49. Meszaros J, Buchalcevova A (2017) Introducing OSSF: a framework for online service cybersecurity risk management. Comput Secur 65:300–313
50. Csrc.nist.gov (2022) NIST risk management framework. https://csrc.nist.gov/projects/risk-management/about-rmf. Accessed 2 Jul 2022
51. ISO (2013) ISO/IEC 27001—information security management. https://www.iso.org/isoiec-27001-information-security.html. Accessed 2 Jul 2022
52. ISO (2018) ISO 31000—risk management. https://www.iso.org/iso-31000-risk-management.html. Accessed 2 Jul 2022
53. Fahrurozi M, Tarigan SA, Tanjung MA, Mutijarsa K (2020) The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at data and information center of ministry of defence). In: 2020 12th International conference on information technology and electrical engineering (ICITEE). IEEE, pp 86–91
54. ISO (2018) ISO/IEC 27005:2018. https://www.iso.org/standard/75281.html. Accessed 2 Jul 2022
55. Csrc.nist.gov (2022) Glossary CSRC. https://csrc.nist.gov/glossary. Accessed 11 Jun 2022
56. Khrais LT (2015) Highlighting the vulnerabilities of online banking system. J Internet Bank Commer. https://doi.org/10.4172/1204-5357.1000120
57. Azad S, Jain K (2013) CAPTCHA: attacks and weaknesses against OCR technology. Glob J Comput Sci Technol 13:15–17
58. Edge K, Raines R, Grimaila M, Baldwin R, Bennington R, Reuter C (2007) The use of attack and protection trees to analyze security for an online banking system. In: 2007 40th Annual Hawaii international conference on system sciences (HICSS'07), pp 144–144. https://doi.org/10.1109/HICSS.2007.558
59. Cwe.mitre.org (2022) CWE–2022 CWE top 25 most dangerous software weaknesses. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html. Accessed 23 Jun 2022
60. CIS (2022) The 18 CIS controls. https://www.cisecurity.org/controls/cis-controls-list. Accessed 24 Jul 2022