

Cyber in the front and center



In line with the acceleration of digitalization and remote work, the prevalence of cybercrime has increased during the Covid-19 pandemic. For banks, the threat is pronounced and growing. Luckily, the banking sector has broadly invested in cybersecurity and is better prepared than other sectors for new threats posed by cyber perpetrators.

There are several key developments that are shaping cybersecurity investments in the banking sector.

Open banking

Open banking is a practice that provides third-party financial service providers open access to consumer banking, transaction and other financial data from banks and non-bank financial institutions using application programming interfaces (APIs). It also allows for greater financial transparency for customers and uses open source technology to build the ecosystem. At each level, cybersecurity measures and policies will determine the success of open banking.

As stakeholders in Jordan develop their own open banking initiatives, they should recognize the importance of security. All third-party providers have to comply with regulator and bank



As stakeholders in Jordan develop their own open banking initiatives, they should recognize the importance of security.

data protection rules, which should be focused on customer privacy protection. The provider must inform the bank and the customer what data it intends to use and how it will use it, as well as how long it will remain within their system.

Cyber in the audit (CitA)

CitA provides a framework and guidance for a structured approach and risk-based decision making for assurance.

Traditionally, auditors have tested their clients' general IT controls (GITCs). However, as risks evolve, so too does the role of the auditor. Just as an IT audit supports a financial audit by testing automated controls, CitA supports the IT audit by testing the cybersecurity measures in place to prevent an attack on an IT system.

The emphasis for CitA is a forward-looking approach where the controls are designed to provide an assurance on the IT dependencies that a bank relies upon. It gives insight into a bank's cybersecurity controls and makes plans for, in case of a cyberattack or compromise, what steps need to be taken to respond and recover.

Data privacy

Whether a bank started its privacy journey because of a regulation or as an initiative, privacy is now firmly a sector-wide priority. Full engagement across the bank is key as privacy professionals look to embed privacy into the DNA of business operations and customer engagement.



Banks must chart a plan that not only encompasses the immediate regulatory challenges, but also a plan for increasing consumer expectations of greater individual control of data. In creating a sustainable and effective data protection strategy, companies should develop a solid framework of best practices and infuse those practices—both procedurally and culturally.

While data should be viewed as a valuable asset, it should not be seen as such in and of itself. It is what a bank does with its data that gives it value—like creating better customer experiences and offering customized products. Additionally, businesses that proactively manage and protect personal data

the way users expect will come out ahead of their competition. Banks will have to better understand their data practices and the impact of new regulations on their business strategies and business models. Waiting to the last minute is not a viable option, because the goal is building customer trust and loyalty.

Penetration testing and red teaming

Though better prepared than most sectors, the banking sector still lags behind the cyber threats landscape. Hackers will find opportunities to exploit flaws in the way banks currently fund, manage, enable, organize and implement their information protection capabilities. Thus, it

is important to stay ahead of the threat by testing what your defenses are capable of.

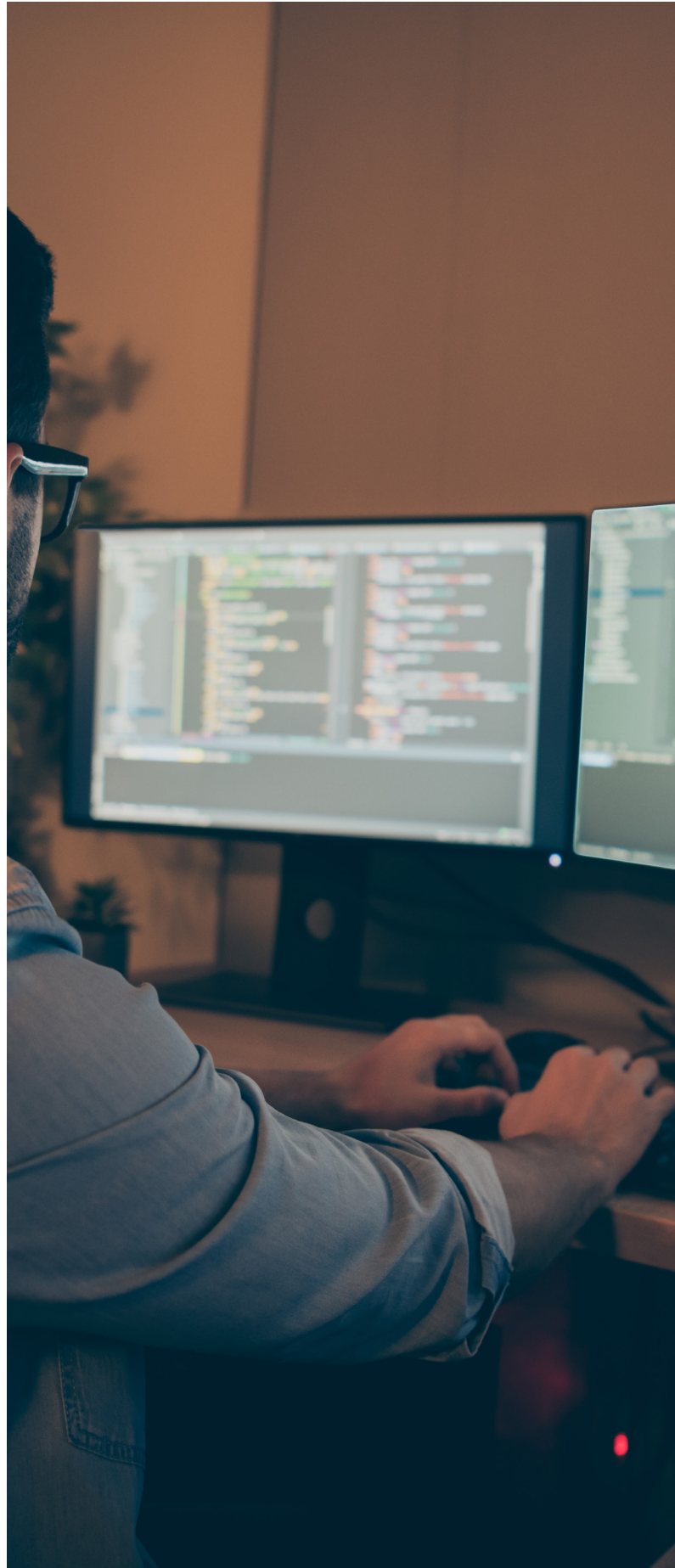
Why red teaming

- Your bank has done penetration testing for a few years and you have implemented security monitoring and incident response processes.
- It is time for the next step in your cybersecurity maturity, you want to know how resilient you are against real attacks.

What you need to do

- Simulate real attackers (including phishing and malware).
- Simulate real tactics, techniques and procedures (TTPs)
- Test your incident response and threat management.





Secure DevOps

DevOps is a philosophy based on combining the traditional roles and responsibilities of development teams and IT operations teams to accelerate the delivery of business value through the two teams. When work flows smoothly through development and IT operations, new software features come to market more frequently and the business becomes more competitive and adaptive in a constantly shifting market.

The central concept of secure DevOps is the integration of security into the development and IT operations teams. By adding security into the original mix, the velocity for security changes increases as well. The likelihood of vulnerabilities being introduced is reduced, and banks are able to more quickly mitigate risks that remain. It is paramount that banks focus on custom implementations for their environment and goals. This includes discussing tangible actions within IT, development and security to enhance the existing culture, processes and technologies in the transition to secure DevOps capabilities. Across the three groups, necessary changes to the cultures of the groups are similar. Because of the vast changes to various processes, the individuals involved must be willing to undertake new programs and processes and different approaches to traditional work. And because of the assortment of new processes and technologies adopted in order to support secure DevOps, it is crucial banks encourage their workforce to share challenges and failures.



Ton Diemont
Head of Cybersecurity and Data Privacy
E: antondiemont@kpmg.com

Tax technology

Within the banking sector, digitalization is impacting every facet of a bank's operations, including tax accounting. Banks hold an immense amount of data about their customers – both retail and commercial – and the effective use of tax technology depends on a bank's ability to organize and use that data.

Regulators providing a catalyst for change

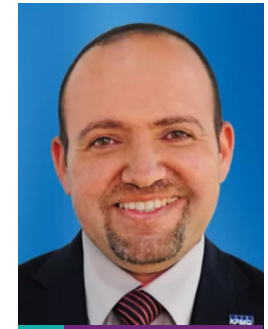
Tax administrations around the world are going digital. They are using sophisticated technology tools and platforms that allow them to have full visibility of every step of the supply chain that impact taxation.

Organizations are struggling not only with trying to keep up with global updates but also when attempting to implement the required changes and when trying to create a tax technology strategy that includes e-invoicing and digital reporting. However, banks and other organizations should view tax modernization as a huge opportunity. Vast amounts of new data can be utilized to optimize their operations and the customer experience, and the technology used to gather this data can lead to a more integrated, digitalized operation.

Tax technology

Technology will play a role, but — as with the introduction of any new technology — its effectiveness depends on a bank's capacity to use and manage technologies, both from a people and operating model perspective. Banks need to implement end-to-end operating models for tax before technology introduced. From a governance perspective, it is wise to have a voice at board-level to make sure the needs of the tax team are not ignored when setting up such systems.

Modernizing a bank's tax system often does not mean technology first, but rather the other way around — first modernizing its operating model, then its people, and then the compatible technology. With more changes coming to the tax environment in Jordan, the need for a strong tax operating model to support the management of tax risk is becoming ever more urgent.



Khaled Tuffaha
Director, Tax Lead



Technology will play a role, but its effectiveness depends on a bank's capacity to use and manage technologies, both from a people and operating model perspective.