Cybersecurity

Overview

Focus Areas
1. Fundamental concepts
2. Top blockchain security risks
3. Blockchain cybersecurity risk management
4. Blockchain secure deployment

Tools and Resources
5. Risk management template
6. Secure deployment process
7. Key questions in securing a blockchain solution
Overview

As they make technology decisions, leaders these days are bombarded with constant headlines about costly enterprise hacks, ransomware, and stolen user data. Thus, any new technology implementation must include adequate safeguards against such nightmare scenarios.

Although blockchain technology is rapidly evolving, there are some fundamental security concepts that can be applied to the blockchain space effectively. After covering these focus areas, this module offers a risk management framework and a 10-step secure deployment plan that should be useful in a wide range of supply-chain projects.

Recommended reading - Inclusive Deployment of Blockchain for Supply Chains Part 5 – A Framework for Blockchain Cybersecurity
1. Fundamental concepts

What are the basics of blockchain security, including factors unique to this new technology and concepts that apply to other areas of IT as well?

It is important to keep in mind that a blockchain solution is part of wider technological, business and human systems. Blockchain solutions do not stand on their own; for instance, they require connectivity, users, and sound business processes. Thus the security of a blockchain is directly related to the security of other systems it is integrated with.

The hype around blockchain technology has also led to a polarised debate concerning security. On one end of the spectrum are those who view a blockchain as inherently insecure and unfit for use cases that would require robust privacy protections for individual users. On the opposite end are those who view blockchain as a cryptography-native, “unhackable” computational module, or even an unhackable solution overall.

The truth lies somewhere in the middle.

A blockchain requires proactive security management, like any other technology. There are information security considerations that cut across technologies that impact blockchain; there are also blockchain-specific security issues.

To better appreciate both the general needs and blockchain-specific considerations, it is necessary to understand a few cybersecurity basics. Once you get the basics of cybersecurity right, a team will be in a much better position to address the nuances related to blockchain. (Figure 11.1 – Cybersecurity basics and blockchain nuances).

Security basics:

- Security as a process: There is no security silver bullet. Instead, it is a cat-and-mouse game in which attackers and defenders continuously attempt to outsmart each other. No software solution, including any based on blockchain, is ever “secured” with finality. Security is consistently improved, not achieved.

"Often, I am in situations where I need to educate the client on security, since they would not have brought it up. Interestingly enough, investors also often ask about our approach to security.

Hanns-Christian Hanebeck, Founder and Chief Executive Officer, Truckl.io"
The CIA (confidentiality, integrity, and availability) triad: Security goals are defined by three properties - confidentiality, data integrity, and availability. However, it's worth noting that pursuing all three properties at once is usually not possible. Blockchain is designed to achieve data integrity in particular. But the confidentiality and availability objectives will conflict with each other, for example. While security controls can help, those deploying blockchain solutions will usually need to make trade-offs on one of the two other goals.

Data integrity and immutability:

In computer security, the terminology “data integrity” is preferred to convey the idea that data has not been altered or destroyed in an unauthorised manner. “Immutability” means perfection of data integrity in some professional context.

In a more commercial context, these terms may be used in a somewhat different way. But in this module we use the terminology as is customary among cybersecurity experts, for the sake of consistency.

Defence in depth: A system design principle that revolves around the idea of introducing multiple layers of defence so that attackers can be detected before they reach critical cores. For blockchain, this suggests security controls at multiple checkpoints, for example, using virtualised private clouds to secure blockchain nodes, opening only the required ports and using access control lists to restrict access to smart contracts.

Simple security: The best security measures are transparent and simple. The idea that hiding something or making it complex will make it secure has been proven wrong time and time again. In blockchain, that means to use tested-and-tried hash algorithms or consensus mechanisms rather than to try to innovate.

Blockchain nuances:

Traditional information security is required to secure the development stack supporting blockchain, from cable to communication network and software security. Beyond this, there are five key blockchain characteristics that require specific security measures:

Decentralisation: Whatever the blockchain type, the essence of the technology is to offer a certain degree of decentralisation. This has profound impacts in security governance, a discipline that has been mostly centralised in the past.

Consensus mechanisms: A blockchain’s data integrity is directly linked to the security of consensus mechanisms. For public blockchains, while Proof-of-Work and Proof-of-Stake are the most established consensus mechanisms to date, there are multiple ways in which these are implemented, with various degrees of security and different prerequisites for implementation. For private blockchains, a team can select the consensus mechanism that best aligns with the nature of the desired solution. In either case, it is critical to select the right consensus mechanism and implement it securely.

Smart contracts: A double-edged sword, in light of their data integrity. While the integrity aspect is a good thing to provide hardness to modify something that is agreed upon by multiple parties, it is also important to note that patching smart contracts is not trivial. This will be risky especially where there is transparency to all users of the blockchain in which smart contracts are created. Thus smart code auditing will be fundamental to include as well.

There is a trend emerging throughout the cybersecurity profession to treat all networks, users and endpoints as zero-trust. In that framework any information technology security work is analogous to the painting of San Francisco’s Golden Gate Bridge — the work is always ongoing in multiple areas, using multiple techniques, and with never-ending innovation. Blockchain developers need to think and act that way too.

Andrew Borene, JD, CISSP, Chief Executive Officer, Cipherloc Corporation and Fellow at Georgetown University’s Center for Security Studies

Example

Following the logic that blockchain builds upon traditional information technology, TradeLens, an industry platform developed by Maersk and IBM, obtained information security certification against the ISO/IEC 27000 standards, maintained by a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
• **Endpoint security:** While this is not strictly limited to blockchain, the absence of central entities pushes many security responsibilities to solution developers and users. Because it is very difficult to protect digital access points, solution providers must not just raise awareness among users. They must also clarify individual user responsibilities at the endpoints early on.

• **Cryptographic keys:** These are the foundation of security in blockchains. It is of utmost importance to securely generate, use and store these cryptographic keys.

For broader scope of discussion on decentralisation and its challenges, refer to the modules **Ecosystem**, **Consortium Governance**, and focus area **Risk identification checklist** in the module **Risk Factors**. More generally, those matters are also covered at length in the designated white paper about blockchain cybersecurity that the Forum has published.¹⁰⁴

### 2. Top blockchain security risks

**What are the top blockchain security risks, how can they be mitigated, and how do they compare to traditional databases or other familiar technologies?**

As mentioned previously, one of the goals of blockchain design is to achieve data integrity. While various types of blockchains have varying degrees of fault tolerance, most are considered better alternatives than traditional databases, from a data integrity perspective. As a result of the clear strength of data integrity inherent to public blockchains, the top cybersecurity risks related to public blockchains tend to be related to the confidentiality and availability goals. (See the CIA triad introduced earlier). In private blockchains, however, confidentiality will be a less challenging risk while the level of data integrity may be less than that of a public blockchain. It is important for non-technical expert leaders and policymakers to know that different settings and configurations can change the risk landscape in the deployed blockchain solution; there is not a “one size fits all” answer. In addition, data integrity can have its own risks related to the source and quality of the data that is registered.
The **decentralised** nature of the technology is probably its biggest risk. From a security governance procedure, there is nothing simple about managing incidents and crises with such loose controls over the infrastructure. Security governance has not been traditionally a shared, transparent and collective responsibility and finding the right balance between the new business models that blockchain foster and their security governance will require a trial and error process. There is no recipe, nor research on this at this stage. Decentralisation can have a major impact on data security. The data stored on blockchain is available to all the participating nodes. PII and PHI data should not be stored on blockchain.

**Confidentiality** is most difficult to enforce in public blockchains, in which the information is accessible to anyone. Information stored on-chain can be encrypted, but not all of it, and while homomorphic encryption seems promising, it is not yet widely available. As a general rule, we recommend avoiding storing sensitive or private data on a blockchain.

Securing **endpoints**, and in particular managing cryptographic keys, is closely related to confidentiality issues. It is not surprising then that public chains are most at risk when it comes to endpoint security. In particular, permissionless public blockchains are those for which end users are most at threat. Strong user awareness is essential in those constructs to ensure all stakeholders are aware of the risks they are taking by transacting on blockchain.

From an **availability** perspective, different blockchains show different strengths and risks. Private chains are relatively more at risk given the smaller number of validating nodes they are composed of and given the necessary presence of an entity dealing with access control. The latter can effectively become a single point of failure, preventing on-chain operators although nodes are available.

**Nodes** indeed pose a potential security risk, most present in permissionless blockchains in which they are more exposed and not directly under the control of any organisation. It can hence be more difficult to secure these nodes, for instance patching them or forcing them to operate under certain conditions.

**Smart contracts** are at the intersection of availability and confidentiality risks: it is essential to use secure coding practices, and to have smart contracts undergo third party auditing before being released on a blockchain. This risk is most prominent in permissionless blockchains given that KYC procedures in permissioned chains reduce the likelihood of a validated user attacking the smart contracts.

*Figure 11.2 – Top blockchain security risks*

For further references in the toolkit, there are suggestions at the end of the previous section on **Fundamental concepts**. Confidentiality is the main topic discussed in the toolkit module **Data Protection**. And availability, which carries some performance-related risks, is discussed in the module **Risk Factors**.
3. Blockchain cybersecurity risk management

What specific steps can project teams take to manage blockchain security risks, including initial assessment of potential pitfalls and ongoing management?

A risk is defined as the probability that a threat uses a vulnerability and that this results in a given impact. In light of the risks presented in focus area “Top blockchain security risks” in this module, organisations deploying a blockchain solution must perform a risk assessment. This is an essential step in the blockchain secure deployment process presented below in focus area “Blockchain secure deployment” of this module. For further reading, blockchain project teams are recommended to follow the same framework used by organisations for other information technology deployments, such as the US National Institute of Standards and Technology, “Guide for Conducting Risk Assessments, 2012” (NIST SP 800-30).

Risk assessment generally follows a five-step approach (Figure 11.3 – Five-step approach for blockchain cybersecurity risk management):

**Step 1: Define security objectives**
This is the foundation of the risk assessment as such, it informs all following steps. In light of the business model that will be supported by blockchain, what are the key security objectives to foster? Would confidentiality be more or less important than availability? Should anonymity be guaranteed? Also, such security features must be upheld by a holistic solution. Which parts of the system must preserve data integrity other than a blockchain platform?

**Step 2: Perform a threat assessment**
A threat assessment helps the organisation understand what the blockchain solution will need to be protected from, ranging from human accidents to natural catastrophes and deliberate cyberattacks. Differentiating among threats by categorising them according to capabilities and intent is a good way to measure the potential for disruption. For instance, a government agency may have capabilities but no intent to attack a particular blockchain.
Hacktivists, by contrast, may be interested in harming the reputation of a particular organisation but lack the ability to overcome certain security barriers.

**Step 3: Perform a vulnerability assessment**

A vulnerability assessment helps the project team better appreciate the part of the blockchain solution that will be disclosed to attackers and what weak spots could lead to adverse outcomes down the line. Identifying vulnerabilities is difficult, and all organisations should regularly perform penetration testing on all aspects of the blockchain solutions they deploy. In particular, attention needs to be paid to testing smart contracts. Defining a process early on to secure smart contract code is critical to reduce the vulnerabilities.

**Step 4: Define risk probabilities**

Defining risk probabilities allows for their prioritisation. Risks emerge from the intersection of vulnerabilities and threats as defined in the previous steps. Prioritise risks by determining the likelihood of particular vulnerabilities intersecting with particular threats, and if that happens, determine the criticality of the impact. A highly impactful risk that is very unlikely to occur will be managed differently from a somewhat impactful risk that is likely to occur regularly. The matrix depicted in Figure 11.4 can be used to define priorities of risks associated with blockchain implementation solutions.

**Step 5: Decide what to do with each risk**

Once you have identified specific risks that may arise in your project, it is time to address each one individually. There are four strategies for managing any particular risk. (See Figure 11.5 – Strategies to manage specific security risks to a project):

- **Mitigate or reduce the risk.** Tackle the threat and/or the vulnerability directly to contain its impact. In blockchain, containing impact is perhaps more challenging than with other technologies, and emphasis should probably be placed on reducing vulnerabilities and deterring threats. This strategy offers the best risk control but is generally costly. It is best advised for high and critical risks.
- **Accept the risk.** Acknowledge its existence and budget for it should it materialise. This approach is best advised for low to medium risks.
- **Avoid the risk.** Re-work the systems approach in order to eliminate the specific security challenge entirely. Doing this generally involves trade-offs and accepting the removal of certain functionalities or solution users.
• **Transfer the risk.** Involve a third party, such as an insurance company or an external service provider, to address the risk.

Due to the complexity of blockchain, using external expertise to develop a solution, and another entity to review and audit its results, is highly recommended.

![Likelihood vs Impact](image)

Depending on the level of engagement in security engineering, it is recommended that the reader refer to topics in other modules, such as **Data Protection**, **Data Integrity**, and **Personal Data Handling**. Also, cybersecurity risk management should be treated as part of overall risk management, as explained in the module **Risk Factors**.

### 4. Blockchain secure deployment

**What are the key steps to maintaining the security of a new blockchain solution as it moves from planning and development into everyday use by end users?**

This focus area introduces a ten-step blockchain secure deployment process (Figure 11.6 – Ten-step blockchain secure deployment process). It is important to integrate these steps into a system’s design and implementation for a blockchain solution. This is a complex process, so it is highly recommended to use and refer to more complete documents on integrating security engineering into software development lifecycles, such as one in the US National Institute of Standards and Technology, Special Publication.¹⁰⁶
Step 1: Acquire blockchain expertise
Depending on the organisation’s resources, and the criticality and objectives of the blockchain use case, this can range from outsourcing to a trusted third party to hiring or training staff with the necessary skills to oversee a secure deployment. With regards to blockchain security expertise, it may prove more effective and efficient for project teams to retain qualified cybersecurity experts and train them in blockchain technology rather than to hire blockchain advocates and train them as security experts. To assist project leaders in assessing credentials, there are several international information security accrediting bodies.¹⁰⁷

Step 2: Define security goals
Defining which security goals the organisation will prioritise in the CIA triad is a prerequisite. These goals must align with the organisation’s strategy, crisis management, and business continuity policies.

Step 3: Configure blockchain
Depending on the business objectives and the security goals, choose which blockchain type would provide the best platform. Pay attention as well to other basic configurations such as whether smart contracts will be used and which consensus mechanism will verify transactions. It is quite probable that the business rationale and functional specifications will inform these decisions. While this is not true security-by-design, it is the means by which most real-world implementations will begin.

Step 4: Perform a risk assessment
Determining which specific risks are associated with a particular blockchain is key to being able to deploy it securely. Refer to focus area Top blockchain security risks and Blockchain cybersecurity risk management in this module for more details on how to perform a risk assessment.

Example
The Port of Valencia recently commissioned a blockchain solution to enable different entities working at the port to share data in a more efficient way. Before developing a proof of concept, the leadership team defined the following high-level security objectives, among others:

- Data confidentiality is critical
- The availability of the blockchain solution must be better than the one currently in place
- Ability to identify all entities participating in the consortium

The blockchain network must be compliant with the European Union’s General Data Protection Regulation (GDPR).
Example
To better understand the risks of a planned blockchain solution, the Port of Valencia had the opportunity to assess the security risks of a blockchain solution during a proof-of-concept implementation.

Examples of the main potential vulnerabilities identified:

- The scenario where an attacker rewrites the ledger by compromising a sufficient number of nodes. This will put the community (this case a consortium) at serious risk.
- The administrator’s secret key becomes accessible to other parties, who can then impersonate the administrator and even change the smart contracts.
- Node administrators are able to access confidential data stored in the node.
- The administrator leaves the organisation.

Examples of the main potential threats:

- A competitor in the consortium with administration rights to the node could be accessing confidential data from other organisations in the ledger.
- Someone with administration rights can access the data stored in an external database that is linked to data found on the blockchain.
- Hacktivists could be drawn to the blockchain network.

Step 5: Define security controls
Security controls may be able to reduce risks by technical countermeasures before residual risks are transferred, avoided or accepted. Further details about mitigation strategies are outlined in focus area Blockchain cybersecurity risk management.

Step 6: Design security governance
It is critical for a governance model and security-related processes to be defined prior to development kick-off. Once development starts, even a test version of the use case can be a source of security threats. The governance processes will largely depend on the risks to be monitored. The more risks there are to manage, the more thorough the governance process will need to be.

Step 7: Choose a security vendor
Choose the right security products and services, then evaluate vendors. There are several established enterprise solutions out there, all offering broad levels of security service. In addition, boutique companies and smaller consulting firms can help with niche needs.

Step 8: Develop securely
Ensure that the development team follows secure development practices, also known as DevSecOps, and, in particular, a secure software development life cycle (S-SDLC) methodology. S-SDLC ensures that security assurance activities such as penetration-testing, smart code auditing or architecture analysis are embedded in the development of the blockchain solution.

Step 9: Monitor and audit security
Blockchain is an information technology like any other, so it is wise to integrate procedures and runbooks regarding the blockchain solution into the organisation’s existing overall security plans. On top of these, a blockchain solution will require more collaborative actions with external organisations including node owners and consortium members. In addition to regular
exercises to test staff, it is important to check external communication required upon a potential incident and distributed decision-making processes. Blockchain security incident response will require multiple stakeholders.

For further reference, the major blockchain configuration over public or private is discussed in the module **Structure: Public / Private**. For security goals, the modules such as **Data Protection**, **Data Integrity**, and **Personal Data Handling** are most relevant. Designing governance on security aspects is part of topics in the module **Consortium Governance**.

## 5. Risk management template

Table 11.1 is an example of the worksheet for risk assessment which is introduced in focus area **Blockchain cybersecurity risk management**. The table is followed by a guide illustrated with an example to fill the risk assessment worksheet (Table 11.2).

**Table 11.1 – Worksheet for risk assessment with a demonstrative example**

<table>
<thead>
<tr>
<th>Security objective</th>
<th>Type of information</th>
<th>Vulnerability</th>
<th>Threat actor</th>
<th>Risk likelihood</th>
<th>Risk impact</th>
<th>Mitigation strategy</th>
<th>Security controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Cargo manifest</td>
<td>Encryption key stolen from an unpatched client PC</td>
<td>Monetarily incentivised attacker</td>
<td>High</td>
<td>Medium</td>
<td>Reduce</td>
<td>Advanced key management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Instructions for filling in the above table are given below. Overall, the security objective and type of information will specify what to protect. Vulnerabilities and threats are related to the potential attack on the information. From these, risk likelihood and risk impact are evaluated. After comparing across rows, one prioritises and assigns resources and defines the mitigation strategy and security control for each entry.
Inclusivity • Integrity • Responsibility

Confidentiality, data integrity, or availability

Confidentiality: the type of information should be readable only by legitimate users

Trade secret information described in cargo manifest. This is secured by encryption

Encryption key disclosure due to hack on an unpatched client PC that stores the encryption key

Monetarily motivated attacker to frighten and try to draw money from the cargo owner

Advanced key management including frequent key updates, machine generated keys, biometric authentication to get access to the key, etc.

Table 11.2 – Guide and example to fill the risk assessment worksheet

<table>
<thead>
<tr>
<th>Column item</th>
<th>What to fill in</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security objective</td>
<td>Confidentiality, data integrity, or availability</td>
<td>Confidentiality: the type of information should be readable only by legitimate users</td>
</tr>
<tr>
<td>Type of information</td>
<td>Information asset that the solution tries to secure, for example information, data, history, or code to protect</td>
<td>Trade secret information described in cargo manifest. This is secured by encryption</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Potential weakness of the solution that an attacker may exploit</td>
<td>Encryption key disclosure due to hack on an unpatched client PC that stores the encryption key</td>
</tr>
<tr>
<td>Threat actor</td>
<td>Type of attackers. Incentive and capability</td>
<td>Monetarily motivated attacker to frighten and try to draw money from the cargo owner</td>
</tr>
<tr>
<td>Risk likelihood</td>
<td>High, medium, or low</td>
<td>High (the cargo owner is a large enterprise)</td>
</tr>
<tr>
<td>Risk impact</td>
<td>Large, medium, or small</td>
<td>Medium (trading secret may be an advantage to competitors, but not so large)</td>
</tr>
<tr>
<td>Mitigation strategy</td>
<td>Accept, transfer, reduce, or avoid</td>
<td>Reduce</td>
</tr>
<tr>
<td>Security controls</td>
<td>Method for the chosen mitigation strategy</td>
<td>Advanced key management including frequent key updates, machine generated keys, biometric authentication to get access to the key, etc.</td>
</tr>
</tbody>
</table>

6. Secure deployment process

Table 11.3 summarises the blockchain secure deployment process which is described in focus area Blockchain secure deployment. Refer to the focus area for details regarding each step.

Table 11.3 – Ten-step process of secure deployment

<table>
<thead>
<tr>
<th>Secure deployment steps</th>
<th>Prior steps</th>
<th>Parties involved</th>
<th>End goal / deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] Acquire blockchain expertise</td>
<td>-</td>
<td>Human resources department</td>
<td>Creation of a blockchain security team with in- and out-sourced resources</td>
</tr>
<tr>
<td>[2] Define security goals</td>
<td>1</td>
<td>Blockchain security team, Chief Information Security Officer (CISO), Chief Strategy Officer</td>
<td>A one-pager outlining the security goals</td>
</tr>
<tr>
<td>[3] Configure blockchain</td>
<td>1,2</td>
<td>Blockchain security team, blockchain experts</td>
<td>A list of security and business advantages and trade-offs of the various blockchain configurations considered</td>
</tr>
<tr>
<td>[4] Perform risk assessment</td>
<td>1,2,3</td>
<td>Blockchain security team, IT security department</td>
<td>A list of the risks and the different management strategies chosen. See risk management template</td>
</tr>
<tr>
<td>[5] Define security controls</td>
<td>1,4</td>
<td>Blockchain security team, IT security department</td>
<td>A list of the security functional specifications of the blockchain and recommended security controls for the development team</td>
</tr>
<tr>
<td>[6] Define security governance</td>
<td>1,3,5</td>
<td>Blockchain security team, CISO and CISOs of all the organisations that play a relevant role in the operation of the blockchain</td>
<td>Revised business continuity and disaster recovery plans</td>
</tr>
<tr>
<td>[7] Choose security vendors</td>
<td>1,5</td>
<td>Blockchain security team, blockchain security vendor</td>
<td>One or more contracts with security vendors</td>
</tr>
<tr>
<td>[8] Develop securely</td>
<td>1,7</td>
<td>Blockchain security team, blockchain solution vendor</td>
<td>Well-documented source code and planned security activities</td>
</tr>
<tr>
<td>[9] Monitor and audit security</td>
<td>1,6,8, 10</td>
<td>Blockchain security team, security operations centre, third party auditors</td>
<td>Active monitoring of the blockchain solution in the SOC</td>
</tr>
<tr>
<td>[10] Respond to incidents</td>
<td>1,6,9</td>
<td>Blockchain security team, incident response team or consultants</td>
<td>Timely mitigation of security incidents</td>
</tr>
</tbody>
</table>
7. Key questions in securing a blockchain solution

Below is a checklist meant for assisting organisations in structuring their thoughts around key questions to secure a blockchain solution.

- Does a blockchain solution improve the project effort’s overall security posture?
- What nuances does blockchain security entail and how will the project team achieve a satisfactory level of security?
- What are the specific cybersecurity considerations to have in mind before developing a blockchain solution?
- What are the security trade-offs in using one particular type of blockchain over another?
- What should you absolutely not store on a blockchain?
- Which are the most relevant information security risks that impact blockchain solutions specifically?
- How should security be managed throughout the lifecycle of a blockchain solution, from ideation to inception, and through development, deployment, and operation?
- Have you considered needed cybersecurity and blockchain security expertise prior to developing the blockchain solution?
- Have you referred to the wider security goals of the organisation prior to developing the blockchain solution?
- Have you defined the security objectives that the blockchain solution will need to meet?
- How confident are you that the blockchain solution’s underlying infrastructure allows the organisation to achieve both its business and security objectives?
- Have you listed, prioritised, and acted upon the different information security risks the blockchain solution will face?
- Have you implemented security controls for residual risks?
- Have you discussed with the other parties involved in the operation of the blockchain solution how security governance will take place?
- Have you researched various security vendors and are you confident that the blockchain developers will follow a secure development lifecycle process?
- What will you do to monitor the security of the blockchain solution over time?
- Have you updated the crisis management and business continuity procedures in light of the blockchain solution?
- Have you identified Security Operations Centre resources to monitor and respond to blockchain incidents?
- Are you committed to ongoing penetration testing, monitoring, and innovation in the security of the blockchain throughout the entire lifespan of the project?