**OXF BCH Module 6 Unit 3 Activity submission**

**PLEASE NOTE:** **Plagiarism cases will be investigated in line with the Terms and Conditions for participants.**

|  |
| --- |
| **Plagiarism declaration:** |
| **1. I know that plagiarism is wrong. Plagiarism is to use another’s work and pretend that it is one’s own.**  **2. This assignment is my own work.**  **3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.**  **4. I acknowledge that copying someone else’s assignment (or part of it) is wrong, and declare that my assignments are my own work.** |

**1. Submission information**

**Name:** Nikunj Mathur

**2. Instructions**

1. Complete the submission information above.
2. Save the file as: **First name Surname M6 U3 Activity Submission – e.g. Lilly Smith M6 U3 Activity Submission**. **NB:** *Please ensure that you use the name that appears in your participant profile on the Online Campus.*
3. Write all your answers in this document. There is an instruction that says, “Start writing here” under each question. Please type your answer there.
4. For the full question guidelines and grading criteria, refer to the instructions on the Online Campus or in the downloadable PDF.

**3. Questions**

### Question 1:

1.1 Which use case are you analysing?

Write your use case name and description here:

(max. 200 words)

My use case is blockchain based Security Risk Assessment solution, security risk assessment highlighting security risk in sharing confidential or priority data with the vendor and integral part of Risk Assessment or Vendor On-boarding process due to compliance requirement. Two primary examples of this are compliance with the US Sarbanes-Oxley Act and the US Health Insurance Portability and Accountability Act (HIPAA), require a periodic risk assessment.

Based on the identified security risk, Information Security or Cybersecurity Team provides Cybersecurity contract language to be included in the contract. Vendor are required to share confidential information like infrastructure / application penetration test result, security policies, application logical architecture, network connectivity details, datacentre location, etc. with Clients Information Security or Cybersecurity Team to understand the security risk and provide recommendations accordingly. Vendor’s are usually skeptical in sharing any confidential or priority information over third-party platform and prefer sharing the information directly with their client over the email. My blockchain based solution will provide an interactive platform for vendors to address their client question and upload/share requested information with Clients. Since the information is centrally located, clients would be able to track status of security assessments and generate security assessment reports in required format.

1.2 Key criteria:

1. Is there a predictable, repeatable process that lends itself well to automation?

Start writing here: (Max. 50 words)

Yes, security risk assessment is required by each Client therefore same set of questions (predictable) addressed by vendors repeatedly. My solution will allow Vendor to share information required for this security risk assessment proactively with their multiple clients in a secure fashion with traceability and trackability.

1. Is there an ongoing or long-running transaction or process, rather than a process that only occurs once?

Start writing here: (Max. 50 words)

Yes, security risk assessment is an ongoing process, critical or high-risk vendor are usually reviewed annually therefore vendors are usually required to share the potential confidential or sensitive information annually. My solution will allow Clients to track critical vendors and request for the information required for the security risk assessment.

1. Are there multiple stakeholders in this process or value chain?

Start writing here: (Max. 50 words)

Yes, At least two entities (Client & Vendor) are required for the security risk assessment. Within an entity, multiple other teams are also involved. For instance, post security assessment Cybersecurity contract language is shared with Legal to be included in the contract. This solution provides view of active security assessments.

1. Is the role of reconciling disparate data usually played by one party or a limited number of parties?

Start writing here: (Max. 50 words)

Yes, In the existing security risk assessment process the role of reconciling disparate data played by Client. Client’s Information Security Team manage data provided by Vendor.

1. Is there an element of value transfer? Remember, value is not only monetary.

Start writing here: (Max. 50 words)

Yes, In the security risk assessment process the vendor’s proprietary or confidential information is the element of value transfer. For instance, application penetration test includes vulnerabilities associated with the application. This information is highly sensitive and confidentially, leakage to this could potentially impact brand image and increase cyber-attacks.

1. Is there value in an immutable record? Or is an immutable record a requirement?

Start writing here: (Max. 50 words)

Yes, very limited set of the information associated with Vendor or Client like name, location, service offered is immutable. Security risk assessment is a continuous process and focus on security risk based on exiting known vulnerabilities. The list of existing vulnerabilities is mutable.

### Question 2

**Protocol layer**

* Is it possible to use public blockchains, or is there a defined need for a private implementation?
* What are the design expectations regarding speed, programmability, or functionality?
* Do you have developer resources available, or is the protocol you are using supported by a robust, sustainable open-source developer community with access to resources? Or will you need to foster creation of a developer community?

(Max. 250 words)

Start writing here:

* Yes, it’s possible to use public blockchain but since potential sensitive and confidential data is involved. I think customers will be more comfortable with a private blockchain or enterprise blockchain.
* I’ll prefer using proof of Trusted Node algorithm to expedite the expectations and bring trust between Vendors and clients. Nodes will be provided to customers with solution to run a private blockchain, customers will act as a trusted node and will be able to controls access to their data. From this solution perspective, both Clients and Vendors are customers and will be running nodes in their environment. This will provide more ownership and controls to customers and at the same time reduces operational cost of running blockchain nodes in my environment.
* No, I do not have a developer. I’m a solution architect and a developer, thinking to develop prototype by myself and later expand team. My plan is not to use open source code to reduce zero day security risk. Since open source code is publically available therefore a malicious attacker will look for bugs to exploit the application. I would like to create my own private blockchain and limit public exposure.

**Network layer**

* Who needs to run a node? Who has read access? Who has write access?
* What are the technology integration requirements?
* How significant are the resource (calculation) requirements at a given node?
* What are the data storage requirements regarding network capability (e.g. Storj), archiving and regulation?

(Max. 250 words)

Start writing here:

* Product customers will be responsible to run the node. In this case vendors and clients will be running the node, node (hardware) will be provided as part of the subscription or licensing model. Vendor will have read / write access to their data and Clients will have read only access to Vendor data and vendor will control access to their data.
* Below are the technology integration requirements;
  1. Internet connection to connect different nodes running in the customer’s environment.
  2. Integration with customers Identity and Access Management
  3. Support Single Sign-On
  4. Customer will be required to install Nodes in the DMZ environment to allow Clients access the data.
* Resource requirement at a given node is not very importance because I’m thinking to use proof of trust as consensus algorithm. I will provide node as a black box to my customers, configuration setting and management of node will be product owner responsibility. Node synchronization will able to responsibility of the product owner and will be part of support contract.
* Customers will store their data therefore will not require a centralized data storage. Data regulation requirements depending on the data protection laws, like GDPR for EMEA region, FTC Act and US privacy laws generally provide regulation. Data access is provided by data owner, application can provide geo location of the source accessing the information. Customers will have more control of their data. Since read only access is provided and data not sent to the Clients, GDPR will not be applicable.

**Application layer**

* Who is going to use the application? What are the implications for user experience and design?
* What is the existing organisational structure, and what behavioural patterns do users have today? How does this product or service fit into their existing workflow?
* Are there any behavioural or organisational changes necessary to implement this use case?

(Max. 250 words)

Start writing here:

* The US Sarbanes-Oxley Act and the US Health Insurance Portability and Accountability Act (HIPAA), require enterprise to conduct periodic risk assessment. The PCI DSS also requires organizations to perform a formal risk assessment at least annually. Organization which are required to be PCI DSS compliant, US Sarbanes-Oxley Act compliance, or HIPAA compliance will be utilizing this application.

I’m expecting customers to provide an interface to upload confidential data to be shared with their clients. Customer will also get access to a webpage to create customize questions for their Vendors. Vendor will be able to provide responses allow read only access to their data.

* As of today, Security Risk Assessment process is partially automated. Organizations utilize third party tool to collect assessment responses but confidential or priority information is shared over email. The data is not centrally located therefore hard to manage and assessment takes more time due to resistance is sharing confidential data.

This product will act as one plane of glass for all the assessments and data associated with that assessment. Data available in one repository is a big advantage, Organization would be able to view list of active vendors and categorize them based on high, medium, or a low security risk associated with the vendor.

* Yes, Organization required to trust, understand, and accept Blockchain technology. The mechanism of encrypting the data for safety, available, and centralized data store in a decentralized network need to be understood.