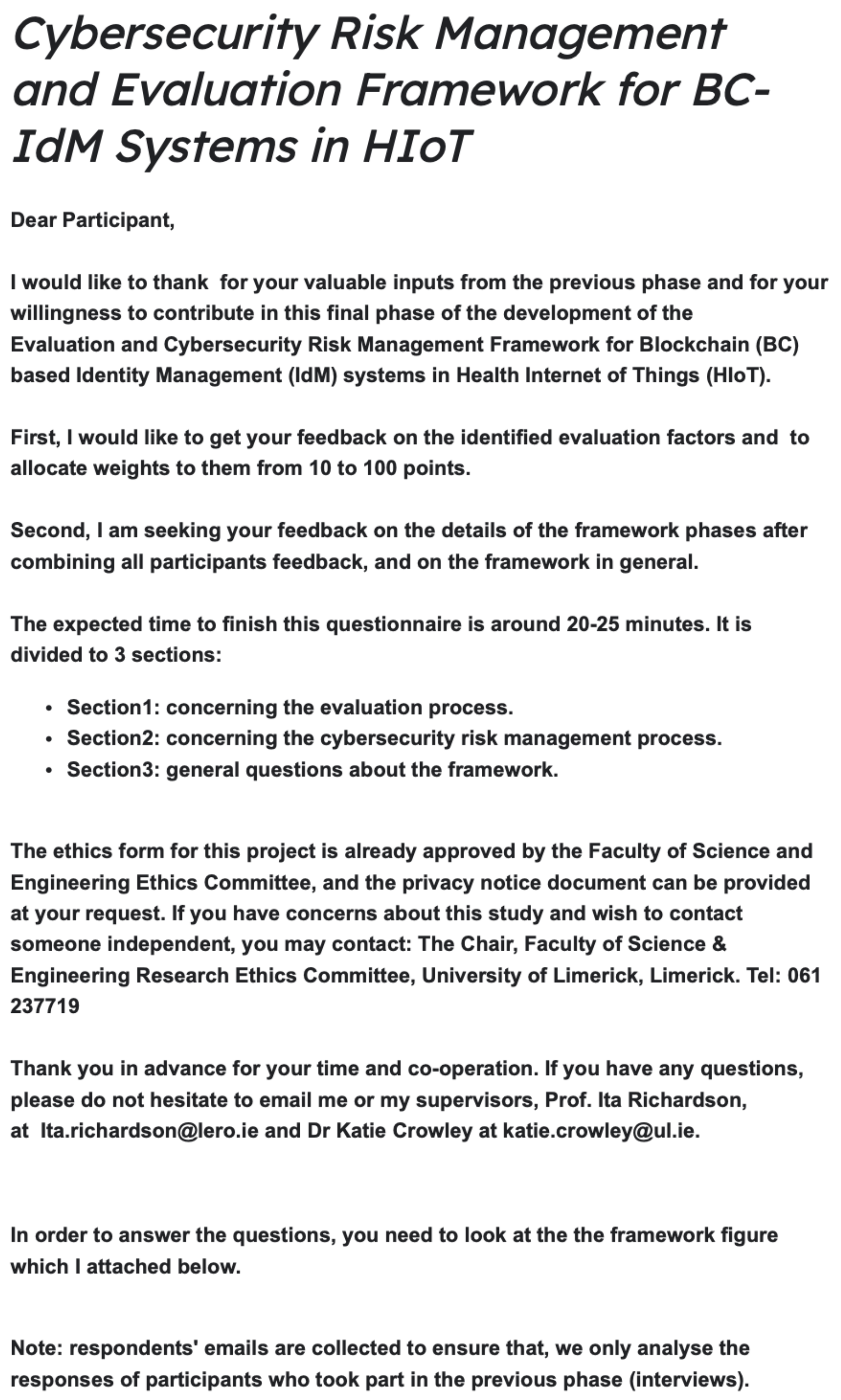
Questionnaire 1



Cybersecurity Risk Management and Evaluation Framework for BC-IdM Systems in HIoT

Dear Participant,

I would like to thank for your valuable inputs from the previous phase and for your willingness to contribute in this final phase of the development of the Evaluation and Cybersecurity Risk Management Framework for Blockchain (BC) based Identity Management (IdM) systems in Health Internet of Things (HIoT).

First, I would like to get your feedback on the identified evaluation factors and to allocate weights to them from 10 to 100 points.

Second, I am seeking your feedback on the details of the framework phases after combining all participants feedback, and on the framework in general.

The expected time to finish this questionnaire is around 20-25 minutes. It is divided to 3 sections:

- **Section1: concerning the evaluation process.**
- **Section2: concerning the cybersecurity risk management process.**
- **Section3: general questions about the framework.**

The ethics form for this project is already approved by the Faculty of Science and Engineering Ethics Committee, and the privacy notice document can be provided at your request. If you have concerns about this study and wish to contact someone independent, you may contact: The Chair, Faculty of Science & Engineering Research Ethics Committee, University of Limerick, Limerick. Tel: 061 237719

Thank you in advance for your time and co-operation. If you have any questions, please do not hesitate to email me or my supervisors, Prof. Ita Richardson, at Ita.richardson@lero.ie and Dr Katie Crowley at katie.crowley@ul.ie.

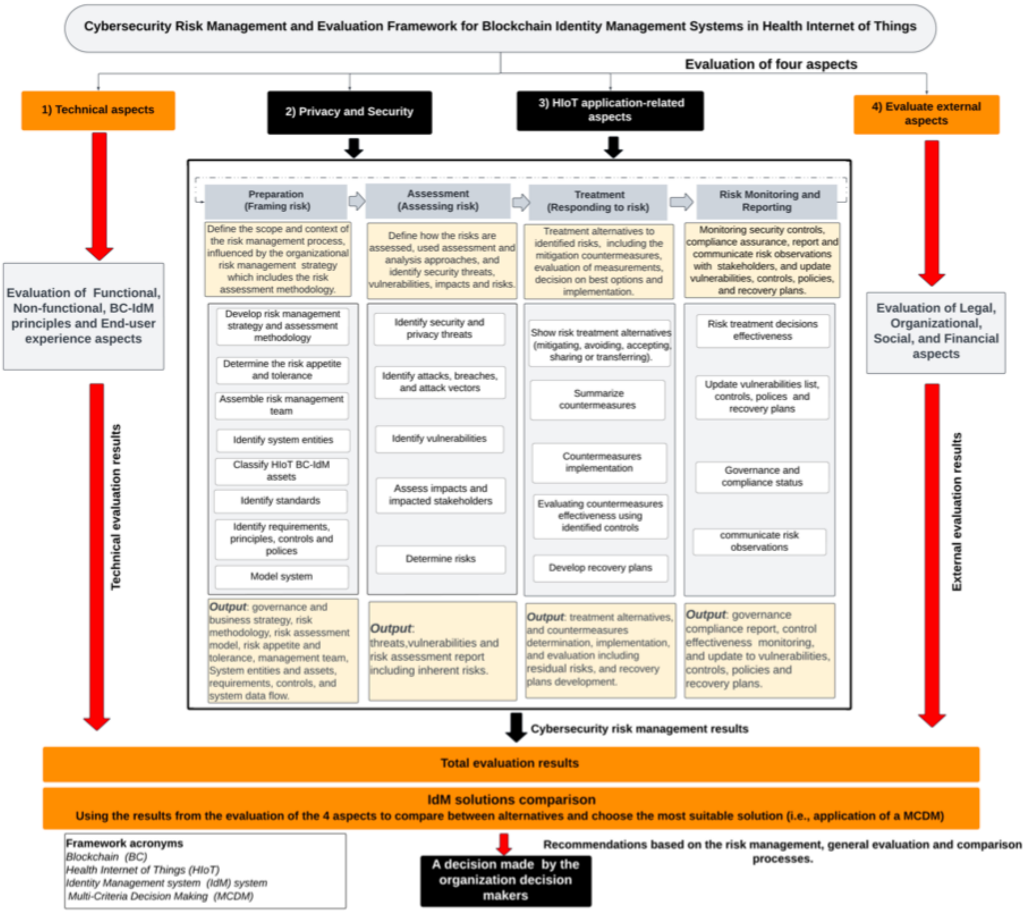
In order to answer the questions, you need to look at the the framework figure which I attached below.

Note: respondents' emails are collected to ensure that, we only analyse the responses of participants who took part in the previous phase (interviews).

1. Email *

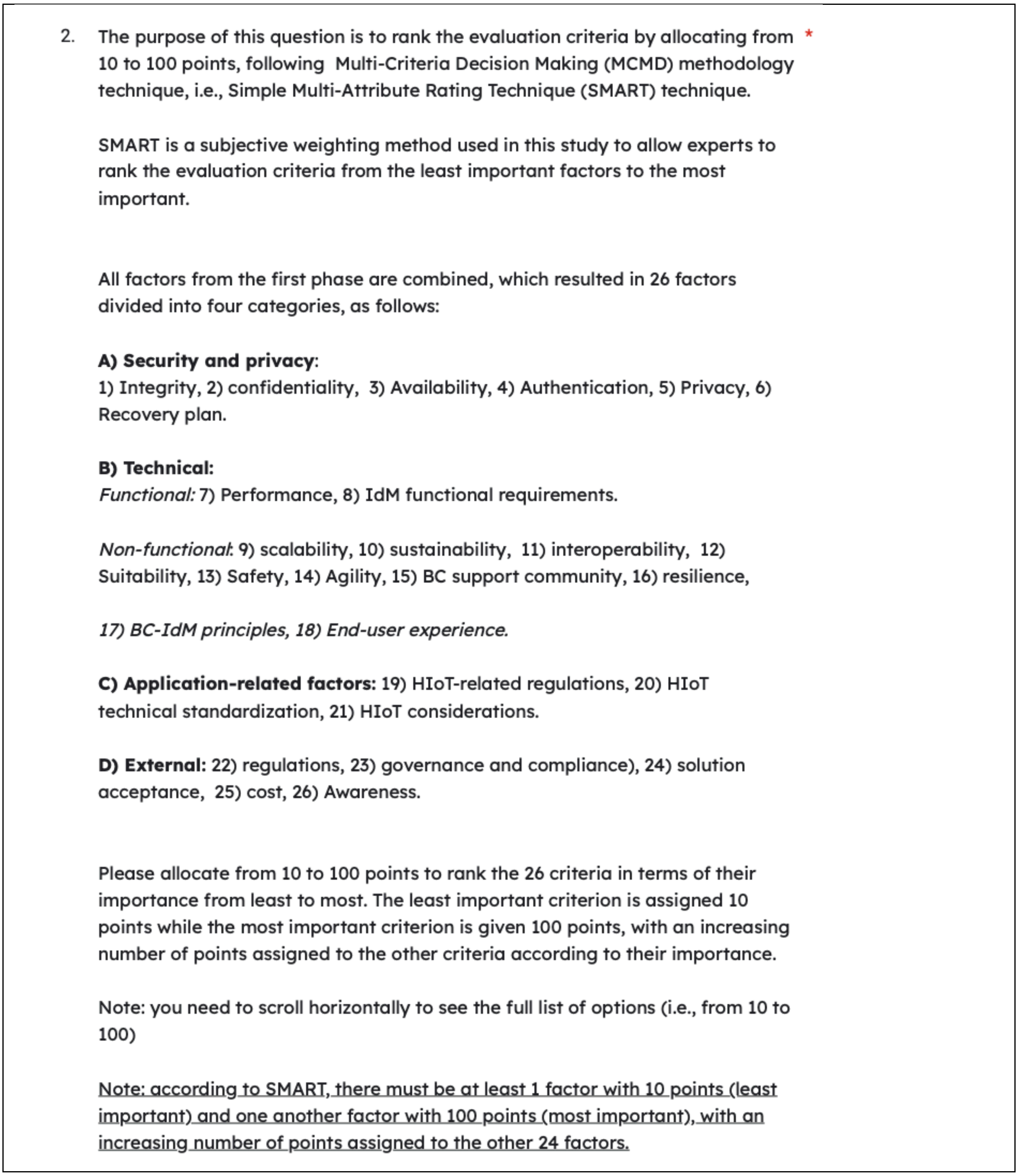
____

Cybersecurity Risk Management and Evaluation Framework for BC-IdM Systems in HIoT


Cybersecurity Risk Management and Evaluation Framework for Blockchain Identity Management Systems in Health Internet of Things
Evaluation of four aspects
1) Technical aspects
2) Privacy and Security
3) HIoT application-related aspects
4) Evaluate external aspects
Evaluation of Functional, Non-functional, BC-IdM principles and End-user experience aspects
Technical evaluation results
Evaluation of Legal, Organizational, Social, and Financial aspects
External evaluation results
Preparation (Framing risk)
Assessment (Assessing risk)
Treatment (Responding to risk)
Risk Monitoring and Reporting
Define the scope and context of the risk management process, influenced by the organizational risk management strategy which includes the risk assessment methodology.
Define how the risks are assessed, used assessment and analysis approaches, and identify security threats, vulnerabilities, impacts and risks.
Treatment alternatives to identified risks, including the mitigation countermeasures, evaluation of measurements, decision on best options and implementation.
Monitoring security controls, compliance assurance, report and communicate risk observations with stakeholders, and update vulnerabilities, controls, policies, and recovery plans.
Develop risk management strategy and assessment methodology
Determine the risk appetite and tolerance
Assemble risk management team
Identify system entities
Classify HIoT BC-IdM assets
Identify standards
Identify requirements, principles, controls and polices
Model system
Identify security and privacy threats
Identify attacks, breaches, and attack vectors
Identify vulnerabilities
Assess impacts and impacted stakeholders
Determine risks
Show risk treatment alternatives (mitigating, avoiding, accepting, sharing or transferring).
Summarize countermeasures
Countermeasures implementation
Evaluating countermeasures effectiveness using identified controls
Develop recovery plans
Risk treatment decisions effectiveness
Update vulnerabilities list, controls, polices and recovery plans
Governance and compliance status
communicate risk observations
Output: governance and business strategy, risk methodology, risk assessment model, risk appetite and tolerance, management team, System entities and assets, requirements, controls, and system data flow.
Output: threats,vulnerabilities and risk assessment report including inherent risks.
Output: treatment alternatives, and countermeasures determination, implementation, and evaluation including residual risks, and recovery plans development.
Output: governance compliance report, control effectiveness monitoring, and update to vulnerabilities, controls, policies and recovery plans.
Cybersecurity risk management results
Total evaluation results
IdM solutions comparison
Using the results from the evaluation of the 4 aspects to compare between alternatives and choose the most suitable solution (i.e., application of a MCDM)
Framework acronyms
Blockchain (BC)
Health Internet of Things (HIoT)
Identity Management system (IdM) system
Multi-Criteria Decision Making (MCDM)
A decision made by the organization decision makers
Recommendations based on the risk management, general evaluation and comparison processes.

Evaluation Factors Question

Please answer the following question concerning the evaluation factors of BC-IdM systems in HIoT.



2. The purpose of this question is to rank the evaluation criteria by allocating from 10 to 100 points, following Multi-Criteria Decision Making (MCMD) methodology technique, i.e., Simple Multi-Attribute Rating Technique (SMART) technique. *

SMART is a subjective weighting method used in this study to allow experts to rank the evaluation criteria from the least important factors to the most important.

All factors from the first phase are combined, which resulted in 26 factors divided into four categories, as follows:

A) Security and privacy:
1) Integrity, 2) confidentiality, 3) Availability, 4) Authentication, 5) Privacy, 6) Recovery plan.

B) Technical:
Functional: 7) Performance, 8) IdM functional requirements.

Non-functional: 9) scalability, 10) sustainability, 11) interoperability, 12) Suitability, 13) Safety, 14) Agility, 15) BC support community, 16) resilience,

17) BC-IdM principles, 18) End-user experience.

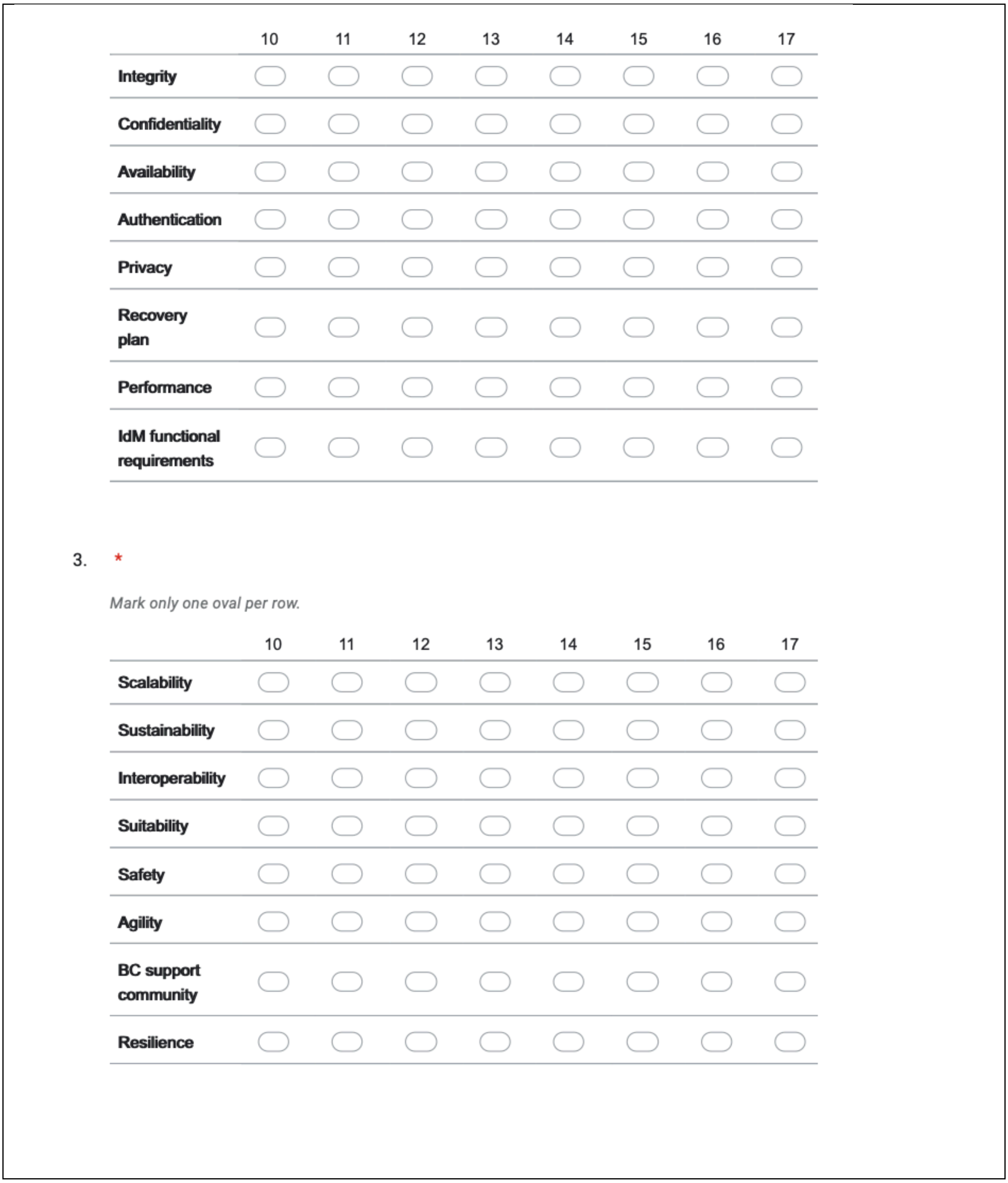
C) Application-related factors: 19) HIoT-related regulations, 20) HIoT technical standardization, 21) HIoT considerations.

D) External: 22) regulations, 23) governance and compliance), 24) solution acceptance, 25) cost, 26) Awareness.

Please allocate from 10 to 100 points to rank the 26 criteria in terms of their importance from least to most. The least important criterion is assigned 10 points while the most important criterion is given 100 points, with an increasing number of points assigned to the other criteria according to their importance.

Note: you need to scroll horizontally to see the full list of options (i.e., from 10 to 100)

Note: according to SMART, there must be at least 1 factor with 10 points (least important) and one another factor with 100 points (most important), with an increasing number of points assigned to the other 24 factors.

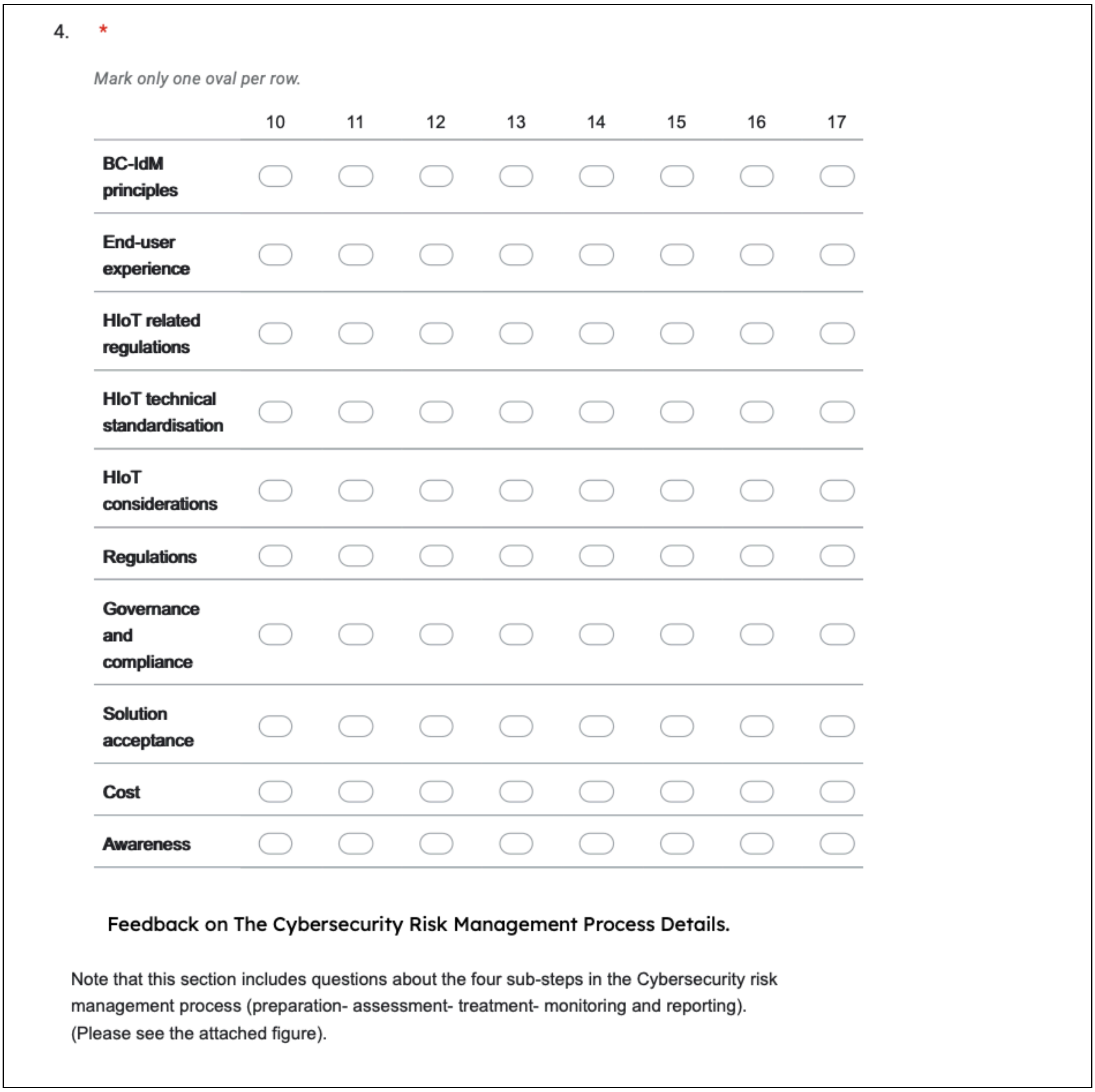


	10	11	12	13	14	15	16	17
Integrity	○	○	○	○	○	○	○	○
Confidentiality	○	○	○	○	○	○	○	○
Availability	○	○	○	○	○	○	○	○
Authentication	○	○	○	○	○	○	○	○
Privacy	○	○	○	○	○	○	○	○
Recovery plan	○	○	○	○	○	○	○	○
Performance	○	○	○	○	○	○	○	○
IdM functional requirements	○	○	○	○	○	○	○	○

3. *

Mark only one oval per row.

	10	11	12	13	14	15	16	17
Scalability	○	○	○	○	○	○	○	○
Sustainability	○	○	○	○	○	○	○	○
Interoperability	○	○	○	○	○	○	○	○
Suitability	○	○	○	○	○	○	○	○
Safety	○	○	○	○	○	○	○	○
Agility	○	○	○	○	○	○	○	○
BC support community	○	○	○	○	○	○	○	○
Resilience	○	○	○	○	○	○	○	○



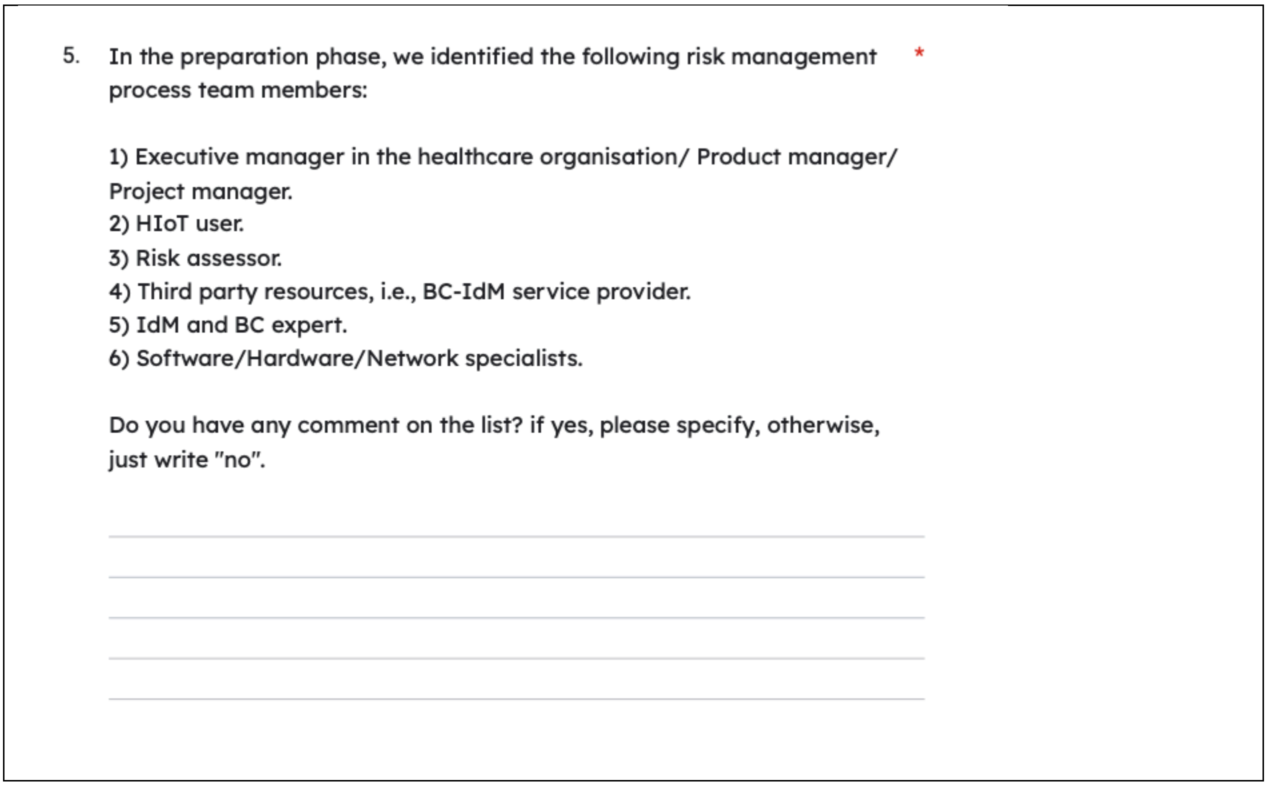
4. *

Mark only one oval per row.

	10	11	12	13	14	15	16	17
BC-IdM principles	○	○	○	○	○	○	○	○
End-user experience	○	○	○	○	○	○	○	○
HIoT related regulations	○	○	○	○	○	○	○	○
HIoT technical standardisation	○	○	○	○	○	○	○	○
HIoT considerations	○	○	○	○	○	○	○	○
Regulations	○	○	○	○	○	○	○	○
Governance and compliance	○	○	○	○	○	○	○	○
Solution acceptance	○	○	○	○	○	○	○	○
Cost	○	○	○	○	○	○	○	○
Awareness	○	○	○	○	○	○	○	○

Feedback on The Cybersecurity Risk Management Process Details.

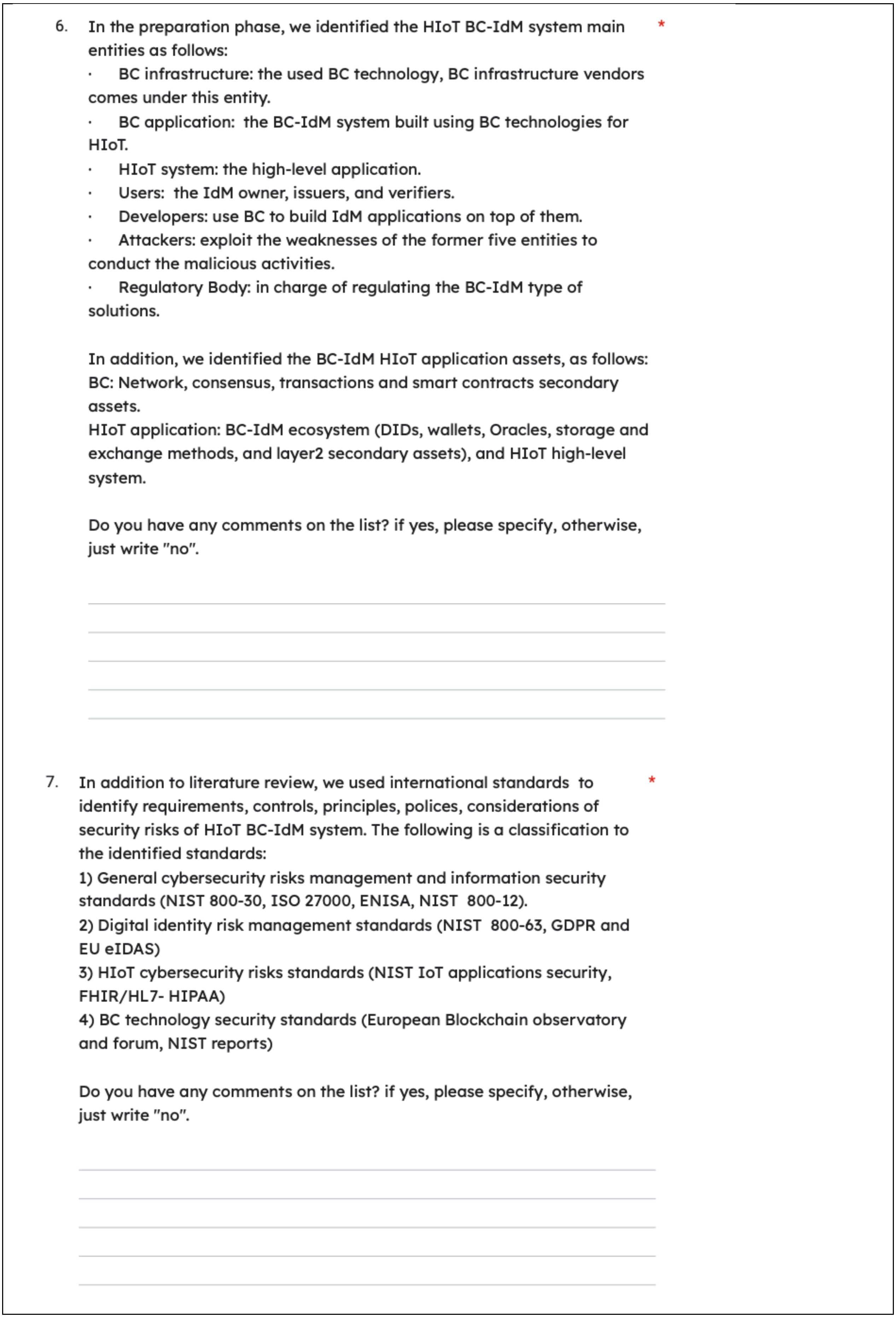
Note that this section includes questions about the four sub-steps in the Cybersecurity risk management process (preparation- assessment- treatment- monitoring and reporting). (Please see the attached figure).



5. In the preparation phase, we identified the following risk management process team members: *

1) Executive manager in the healthcare organisation/ Product manager/ Project manager.
2) HIoT user.
3) Risk assessor.
4) Third party resources, i.e., BC-IdM service provider.
5) IdM and BC expert.
6) Software/Hardware/Network specialists.

Do you have any comment on the list? if yes, please specify, otherwise, just write "no".



6. In the preparation phase, we identified the HIoT BC-IdM system main entities as follows: *

· BC infrastructure: the used BC technology, BC infrastructure vendors comes under this entity.

· BC application: the BC-IdM system built using BC technologies for HIoT.

· HIoT system: the high-level application.

· Users: the IdM owner, issuers, and verifiers.

· Developers: use BC to build IdM applications on top of them.

· Attackers: exploit the weaknesses of the former five entities to conduct the malicious activities.

· Regulatory Body: in charge of regulating the BC-IdM type of solutions.

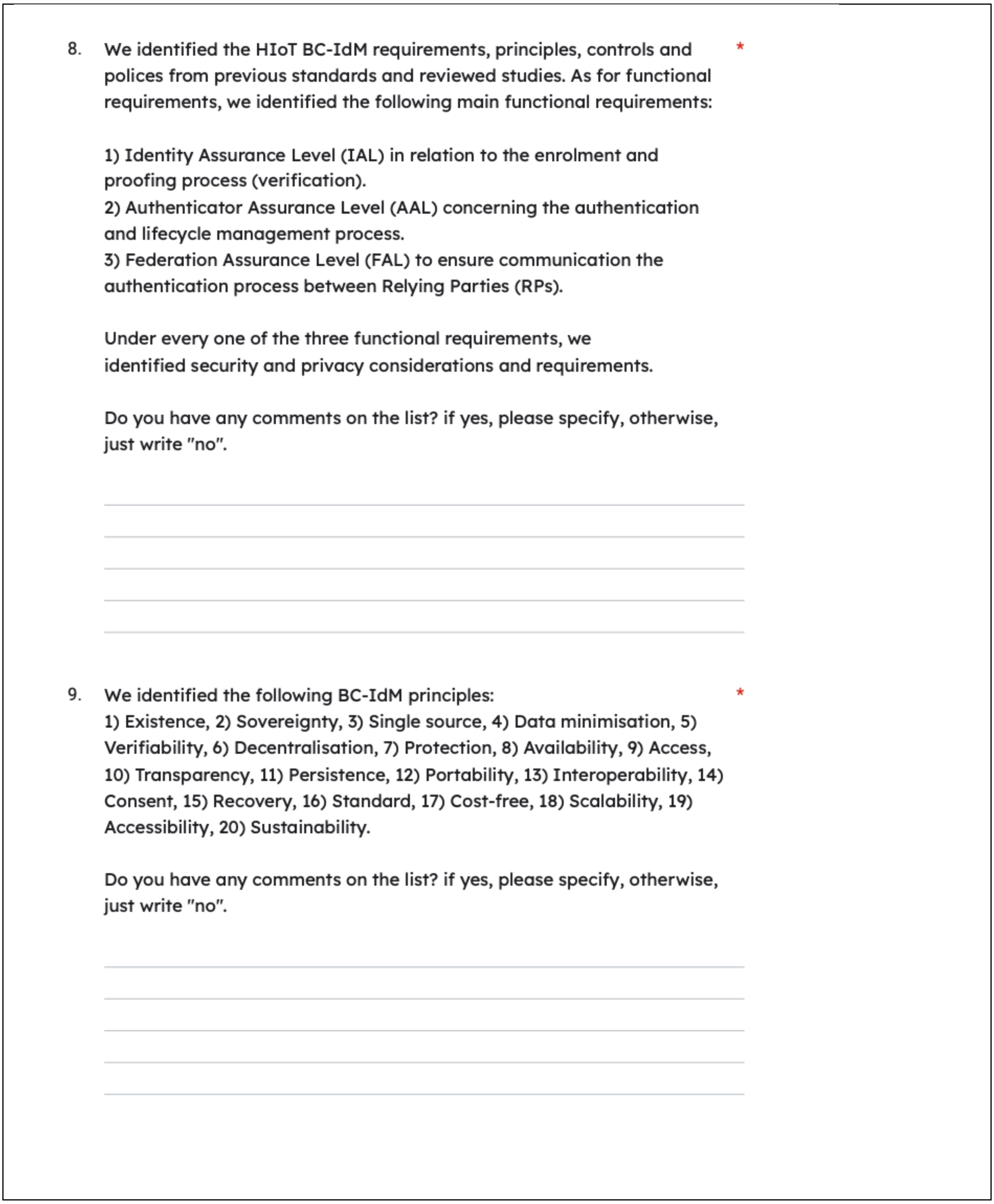
In addition, we identified the BC-IdM HIoT application assets, as follows:
BC: Network, consensus, transactions and smart contracts secondary assets.
HIoT application: BC-IdM ecosystem (DIDs, wallets, Oracles, storage and exchange methods, and layer2 secondary assets), and HIoT high-level system.

Do you have any comments on the list? if yes, please specify, otherwise, just write "no".

7. In addition to literature review, we used international standards to identify requirements, controls, principles, polices, considerations of security risks of HIoT BC-IdM system. The following is a classification to the identified standards: *

1) General cybersecurity risks management and information security standards (NIST 800-30, ISO 27000, ENISA, NIST 800-12).
2) Digital identity risk management standards (NIST 800-63, GDPR and EU eIDAS)
3) HIoT cybersecurity risks standards (NIST IoT applications security, FHIR/HL7- HIPAA)
4) BC technology security standards (European Blockchain observatory and forum, NIST reports)

Do you have any comments on the list? if yes, please specify, otherwise, just write "no".



8. We identified the HIoT BC-IdM requirements, principles, controls and polices from previous standards and reviewed studies. As for functional requirements, we identified the following main functional requirements: *

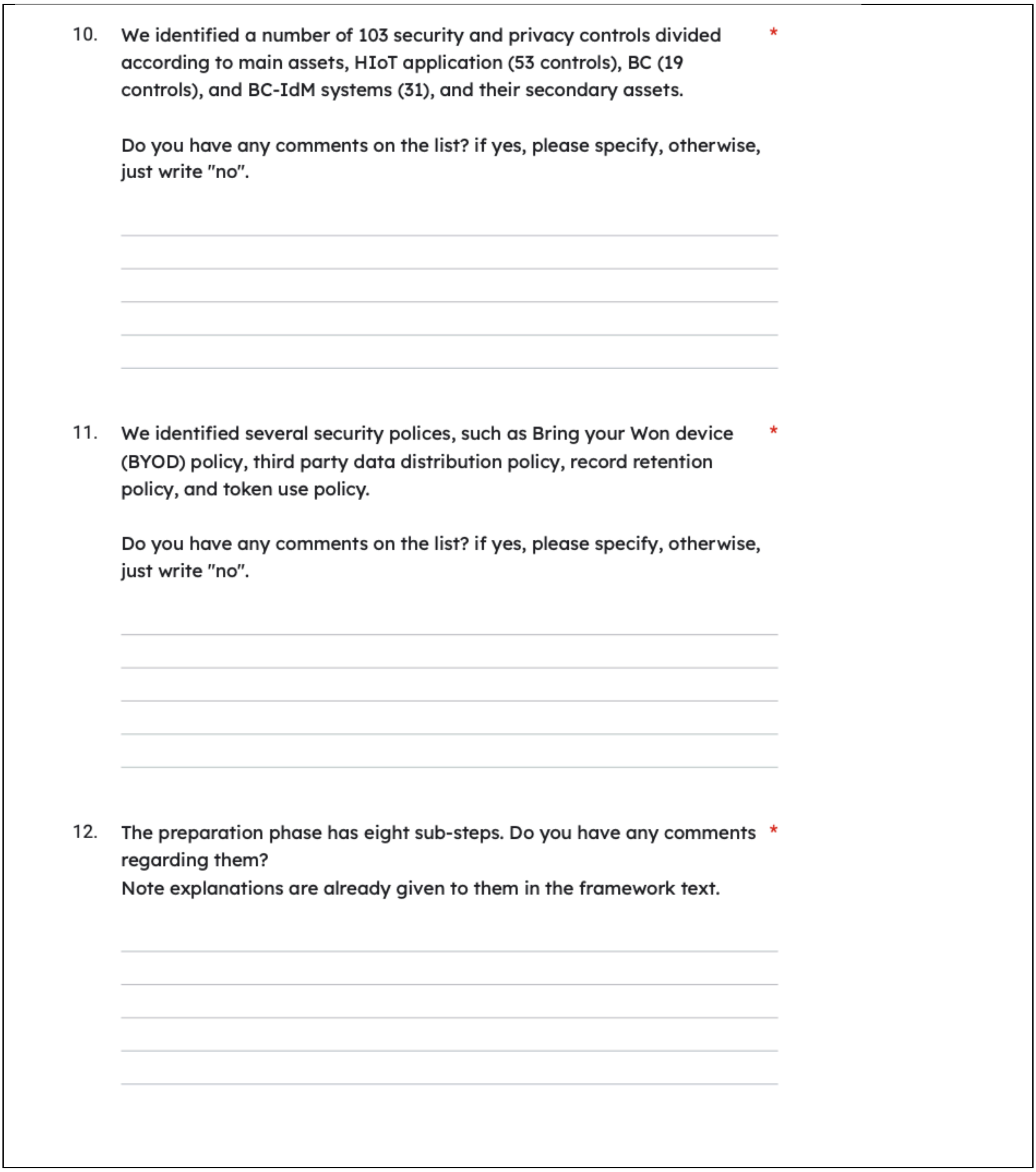
   1) Identity Assurance Level (IAL) in relation to the enrolment and proofing process (verification).
   2) Authenticator Assurance Level (AAL) concerning the authentication and lifecycle management process.
   3) Federation Assurance Level (FAL) to ensure communication the authentication process between Relying Parties (RPs).

   Under every one of the three functional requirements, we identified security and privacy considerations and requirements.

   Do you have any comments on the list? if yes, please specify, otherwise, just write "no".

9. We identified the following BC-IdM principles: *
   1) Existence, 2) Sovereignty, 3) Single source, 4) Data minimisation, 5) Verifiability, 6) Decentralisation, 7) Protection, 8) Availability, 9) Access, 10) Transparency, 11) Persistence, 12) Portability, 13) Interoperability, 14) Consent, 15) Recovery, 16) Standard, 17) Cost-free, 18) Scalability, 19) Accessibility, 20) Sustainability.

   Do you have any comments on the list? if yes, please specify, otherwise, just write "no".



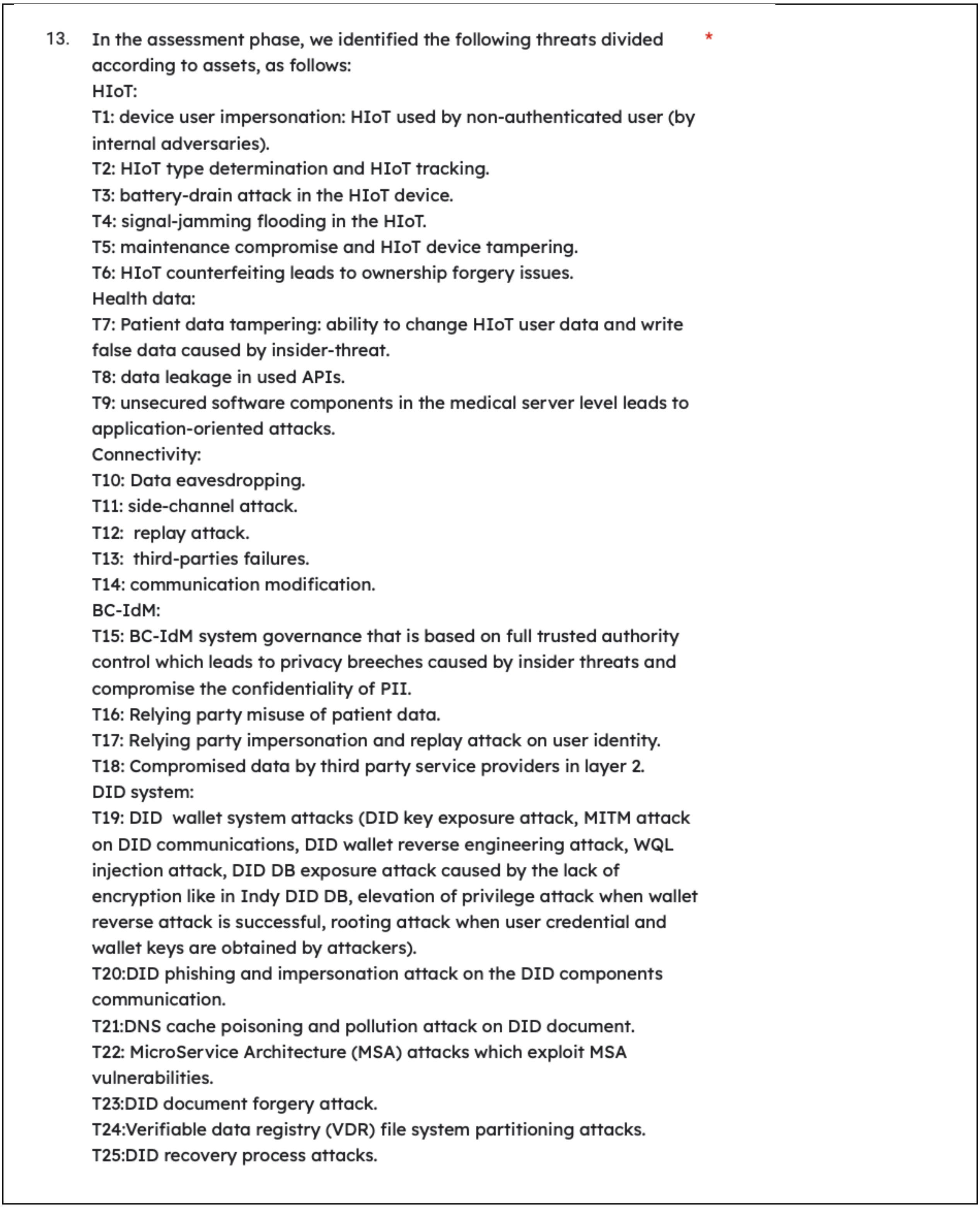
10. We identified a number of 103 security and privacy controls divided according to main assets, HIoT application (53 controls), BC (19 controls), and BC-IdM systems (31), and their secondary assets. *

    Do you have any comments on the list? if yes, please specify, otherwise, just write "no".

11. We identified several security polices, such as Bring your Won device (BYOD) policy, third party data distribution policy, record retention policy, and token use policy. *

    Do you have any comments on the list? if yes, please specify, otherwise, just write "no".

12. The preparation phase has eight sub-steps. Do you have any comments regarding them? *
    Note explanations are already given to them in the framework text.



13. In the assessment phase, we identified the following threats divided according to assets, as follows: *

HIoT:

T1: device user impersonation: HIoT used by non-authenticated user (by internal adversaries).

T2: HIoT type determination and HIoT tracking.

T3: battery-drain attack in the HIoT device.

T4: signal-jamming flooding in the HIoT.

T5: maintenance compromise and HIoT device tampering.

T6: HIoT counterfeiting leads to ownership forgery issues.

Health data:

T7: Patient data tampering: ability to change HIoT user data and write false data caused by insider-threat.

T8: data leakage in used APIs.

T9: unsecured software components in the medical server level leads to application-oriented attacks.

Connectivity:

T10: Data eavesdropping.

T11: side-channel attack.

T12: replay attack.

T13: third-parties failures.

T14: communication modification.

BC-IdM:

T15: BC-IdM system governance that is based on full trusted authority control which leads to privacy breeches caused by insider threats and compromise the confidentiality of PII.

T16: Relying party misuse of patient data.

T17: Relying party impersonation and replay attack on user identity.

T18: Compromised data by third party service providers in layer 2.

DID system:

T19: DID wallet system attacks (DID key exposure attack, MITM attack on DID communications, DID wallet reverse engineering attack, WQL injection attack, DID DB exposure attack caused by the lack of encryption like in Indy DID DB, elevation of privilege attack when wallet reverse attack is successful, rooting attack when user credential and wallet keys are obtained by attackers).

T20:DID phishing and impersonation attack on the DID components communication.

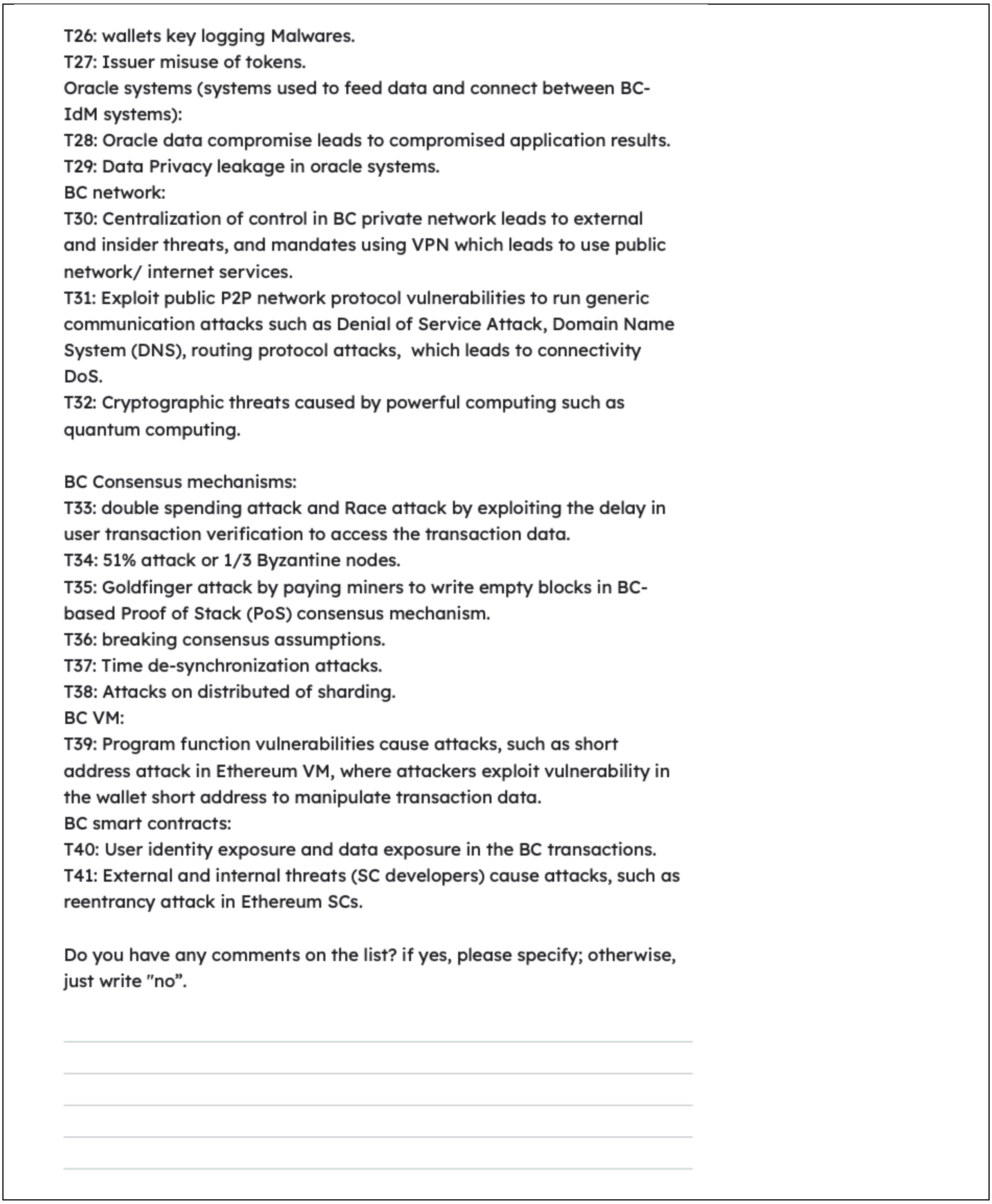
T21:DNS cache poisoning and pollution attack on DID document.

T22: MicroService Architecture (MSA) attacks which exploit MSA vulnerabilities.

T23:DID document forgery attack.

T24:Verifiable data registry (VDR) file system partitioning attacks.

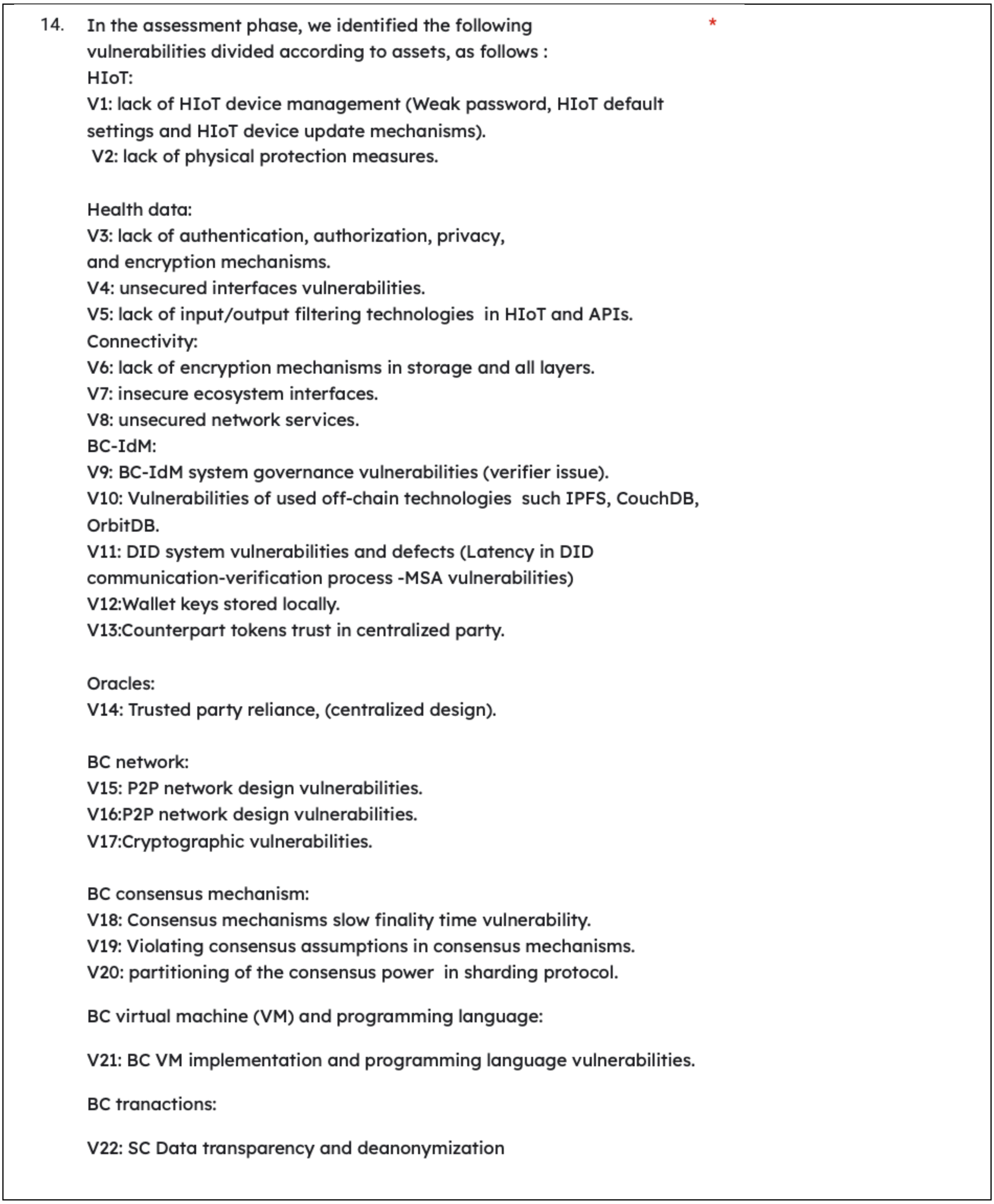
T25:DID recovery process attacks.



T26: wallets key logging Malwares.
T27: Issuer misuse of tokens.
Oracle systems (systems used to feed data and connect between BC-IdM systems):
T28: Oracle data compromise leads to compromised application results.
T29: Data Privacy leakage in oracle systems.
BC network:
T30: Centralization of control in BC private network leads to external and insider threats, and mandates using VPN which leads to use public network/ internet services.
T31: Exploit public P2P network protocol vulnerabilities to run generic communication attacks such as Denial of Service Attack, Domain Name System (DNS), routing protocol attacks, which leads to connectivity DoS.
T32: Cryptographic threats caused by powerful computing such as quantum computing.

BC Consensus mechanisms:
T33: double spending attack and Race attack by exploiting the delay in user transaction verification to access the transaction data.
T34: 51% attack or 1/3 Byzantine nodes.
T35: Goldfinger attack by paying miners to write empty blocks in BC-based Proof of Stack (PoS) consensus mechanism.
T36: breaking consensus assumptions.
T37: Time de-synchronization attacks.
T38: Attacks on distributed of sharding.
BC VM:
T39: Program function vulnerabilities cause attacks, such as short address attack in Ethereum VM, where attackers exploit vulnerability in the wallet short address to manipulate transaction data.
BC smart contracts:
T40: User identity exposure and data exposure in the BC transactions.
T41: External and internal threats (SC developers) cause attacks, such as reentrancy attack in Ethereum SCs.

Do you have any comments on the list? if yes, please specify; otherwise, just write "no".



14. In the assessment phase, we identified the following vulnerabilities divided according to assets, as follows : *

HIoT:
V1: lack of HIoT device management (Weak password, HIoT default settings and HIoT device update mechanisms).
V2: lack of physical protection measures.

Health data:
V3: lack of authentication, authorization, privacy, and encryption mechanisms.
V4: unsecured interfaces vulnerabilities.
V5: lack of input/output filtering technologies in HIoT and APIs.

Connectivity:
V6: lack of encryption mechanisms in storage and all layers.
V7: insecure ecosystem interfaces.
V8: unsecured network services.

BC-IdM:
V9: BC-IdM system governance vulnerabilities (verifier issue).
V10: Vulnerabilities of used off-chain technologies such IPFS, CouchDB, OrbitDB.
V11: DID system vulnerabilities and defects (Latency in DID communication-verification process -MSA vulnerabilities)
V12:Wallet keys stored locally.
V13:Counterpart tokens trust in centralized party.

Oracles:
V14: Trusted party reliance, (centralized design).

BC network:
V15: P2P network design vulnerabilities.
V16:P2P network design vulnerabilities.
V17:Cryptographic vulnerabilities.

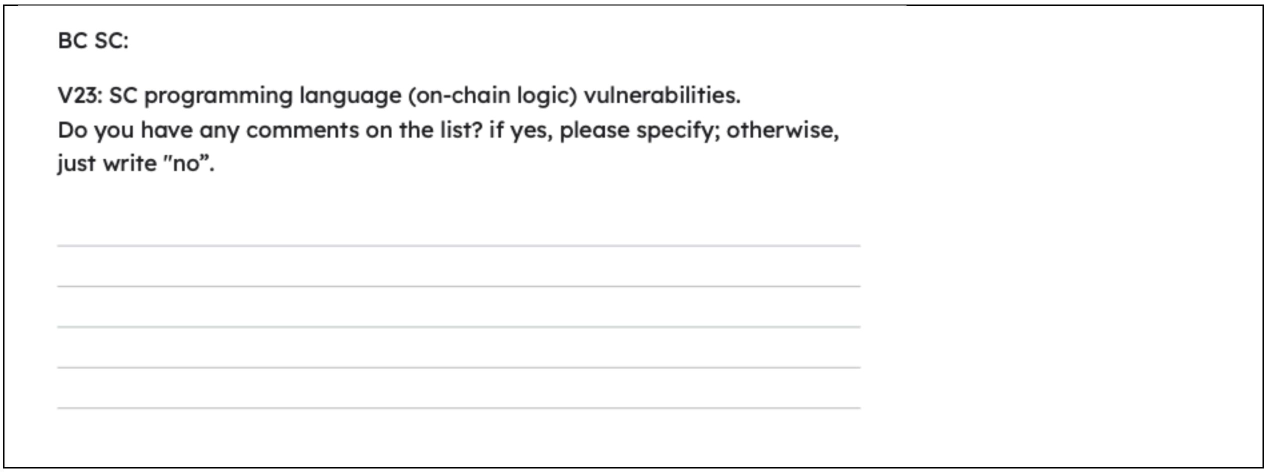
BC consensus mechanism:
V18: Consensus mechanisms slow finality time vulnerability.
V19: Violating consensus assumptions in consensus mechanisms.
V20: partitioning of the consensus power in sharding protocol.

BC virtual machine (VM) and programming language:

V21: BC VM implementation and programming language vulnerabilities.

BC tranactions:

V22: SC Data transparency and deanonymization



BC SC:

V23: SC programming language (on-chain logic) vulnerabilities.
Do you have any comments on the list? if yes, please specify; otherwise, just write "no”.

15. In the assessment phase, we identified the following countermeasures, divided according to assets, as follows: *

HIoT device
C1: Using proxy data protection.

C2: Protect host and device security using authentication, and authorization..

C3: using proof-of-ownership Physical Unclonable Function (PUF) based AuthN mechanisms.

Health Data:
C4: Using multi-factor authentication, authorization, and ABE key management mechanisms.
C5: Using logging systems and Using APIs secure protocols such as OAuth & OpenID Connect.

C6: Using input/output filtering technologies with protocols.

C7: Testing software against vulnerabilities and using firewalls and intrusion detection technologies.

Connectivity:

C8:Third-Party data distribution policy and monitoring and review of third-party services.

BC-IdM:

C9: Selecting trusted verifier carefully.

C10: Minimizing personal presentation.

C11: decoupling user with identifiers by using pseudonymous identifiers.

C12: Using Zero-knowledge proofs mechanisms.

C13:Using challenge-response protocols to check private keys.

C14: Security audit to the used off-chain technologies.

C15:To counter DIDs wallet attacks, key exposure vulnerability can be controlled by using DID systems Software data and data diode mechanisms.

C16: MITM can be counter by using certificate pining.

C17: Login auditing is used to prevent WQL injection attacks.

C18: Checking the authenticity of DID responses to prevent fishing consequences.

C19: Using encryption mechanisms with DID data and wallet recovery.

C20: Security audit to MicroService Architecture (MSA) inherited vulnerabilities.

C21: Using multi-factor authentication and HW wallet to counter local stored keys.

C22:Using reputation decentralized systems to improve trust.

C23: Checking oracles for security vulnerabilities and use mitigation solutions.

BC network:
C24: Update system and monitor network users regularly using intrusion detection systems.

C25: Using mechanisms decreases trust (Multiple-factor authentication) and following best practices to mitigate insider threats.

C26: using DNS Security mechanisms.

C27: Use whitelist nodes for peering process.

C28: Use secure consensus mechanisms.

C29: Using quantum computing-safe cryptographic mechanisms.

BC Consensus mechanisms:

C30: Using fast finality consensus mechanisms to tackle double spending.

C31: Using incentive mechanisms to tackle 51 % attack

C32: Using whitelist of trusted peers and timestamping mechanisms to tackle de-synchronization attacks.

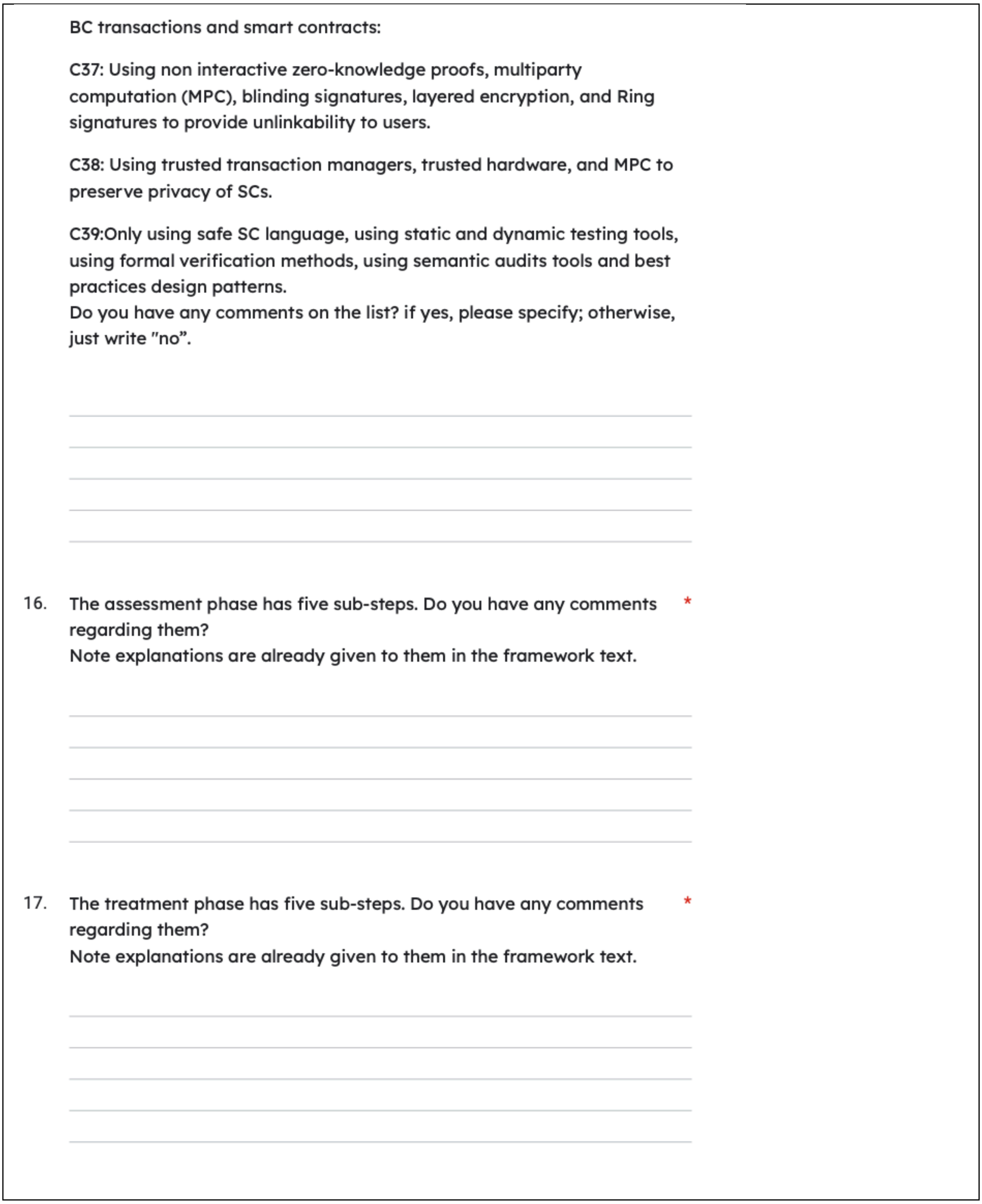
C33: Using asynchronous protocols to tackle breaking consensus assumptions issue.

C34: Distribute node participating in sharing process randomly.

BC VM:

C35: Only using safe VM and languages.

C36: using bugs testing and audit tools.



BC transactions and smart contracts:

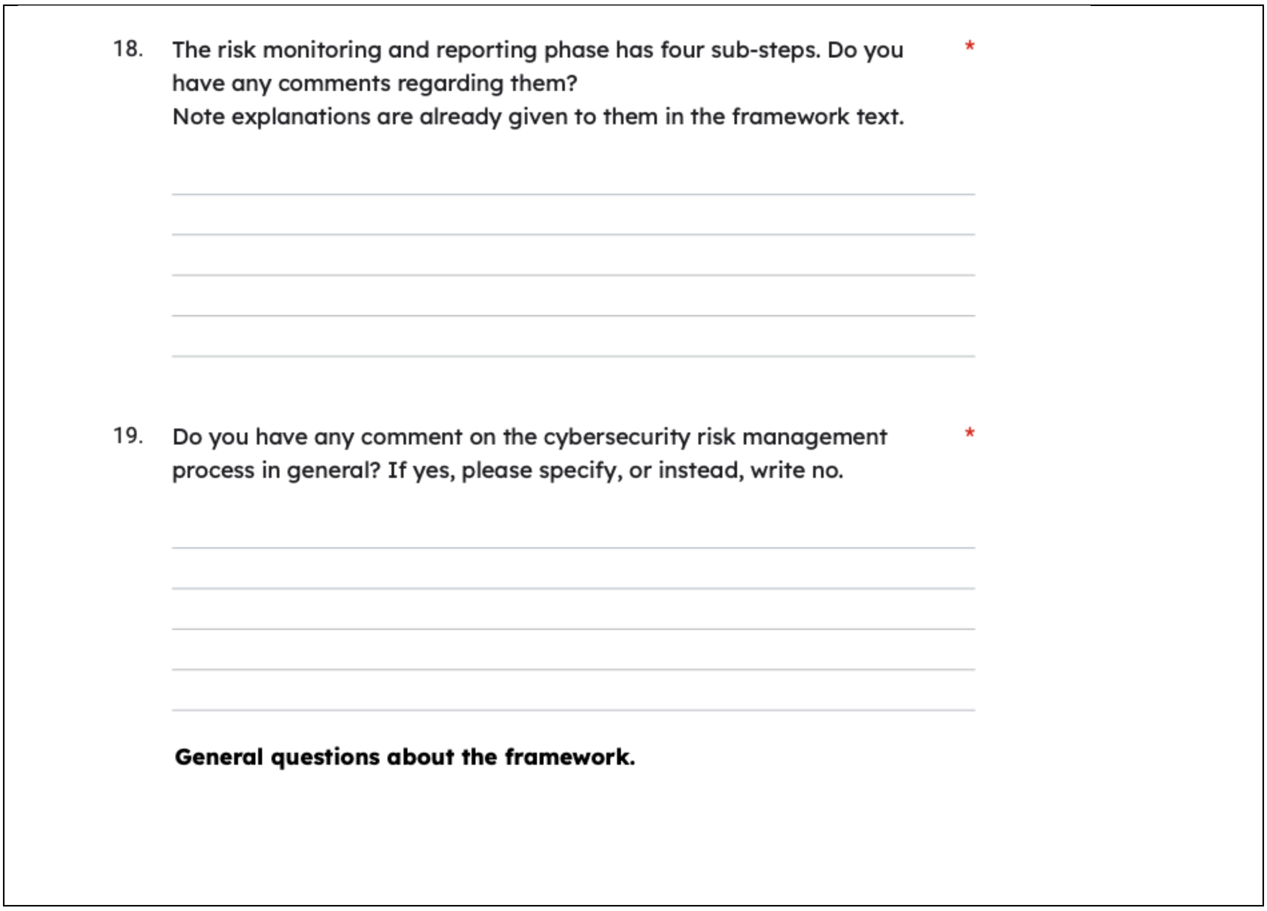
C37: Using non interactive zero-knowledge proofs, multiparty computation (MPC), blinding signatures, layered encryption, and Ring signatures to provide unlinkability to users.

C38: Using trusted transaction managers, trusted hardware, and MPC to preserve privacy of SCs.

C39:Only using safe SC language, using static and dynamic testing tools, using formal verification methods, using semantic audits tools and best practices design patterns.
Do you have any comments on the list? if yes, please specify; otherwise, just write "no".

16. The assessment phase has five sub-steps. Do you have any comments regarding them? *
Note explanations are already given to them in the framework text.

17. The treatment phase has five sub-steps. Do you have any comments regarding them? *
Note explanations are already given to them in the framework text.



18. The risk monitoring and reporting phase has four sub-steps. Do you have any comments regarding them? *
Note explanations are already given to them in the framework text.

19. Do you have any comment on the cybersecurity risk management process in general? If yes, please specify, or instead, write no. *

General questions about the framework.

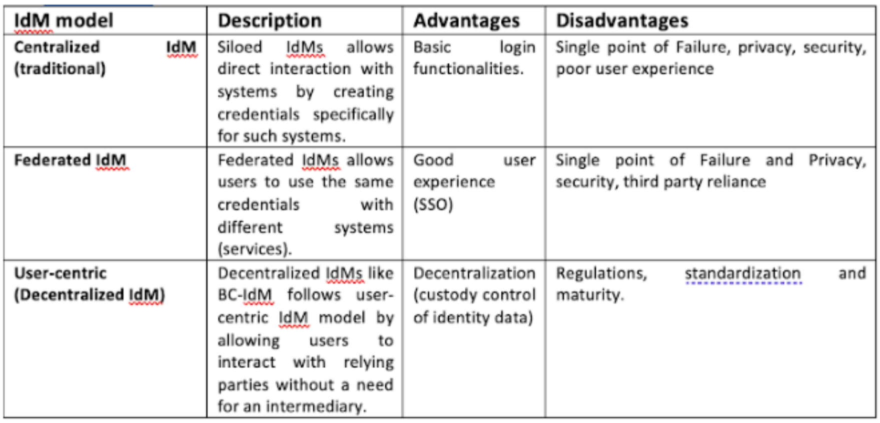
20. After finishing the evaluation process in all four aspects, 1) security and privacy (considered in this work), application-related factors(considered in this work), technical aspects (open research problem/ future work), external factors (open research problem/ future work), there is a comparison process of BC-IdM solutions and classical IdM solutions as shown in the attached framework. *

We identified the following IdM models and BC-IdM solutions to be added in the comparison process (alternatives)., as follows:

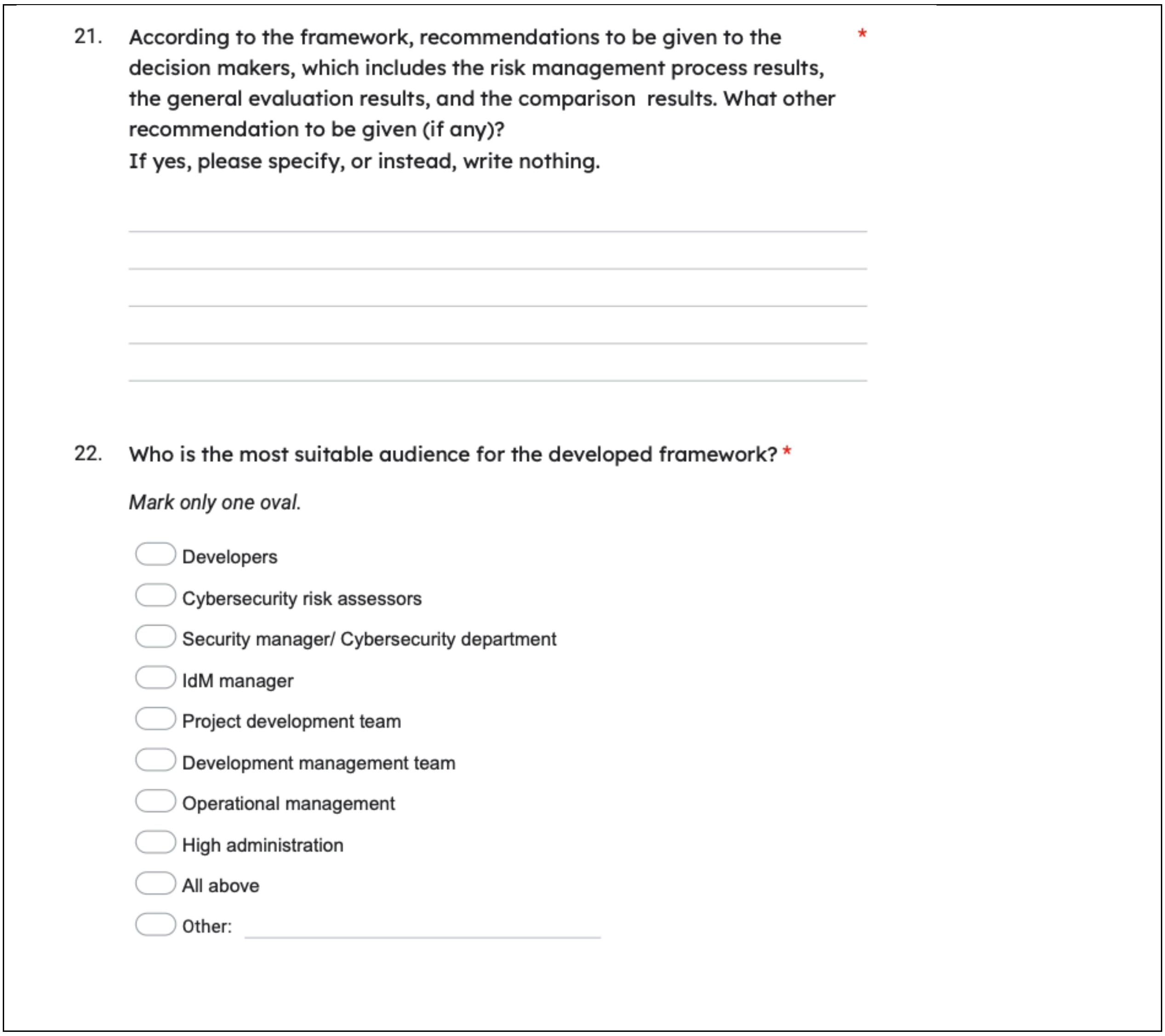
IdM system models (shown in the table below):

BC (we made a list of 10 BC technologies includes (Ethereum, Hyperledger Fabric, Bitcoin, Indy, Corda, Quorum, Multichain, IBM Blockchain, NEM, Elements), and compared them according to **Network Type, Consensus mechanism, Cost, Support Community and governance, and Origin).**

Do you have any comments on the alternatives? If yes, please specify, or instead, write no.



IdM model	Description	Advantages	Disadvantages
Centralized IdM (traditional)	Siloed IdMs allows direct interaction with systems by creating credentials specifically for such systems.	Basic login functionalities.	Single point of Failure, privacy, security, poor user experience
Federated IdM	Federated IdMs allows users to use the same credentials with different systems (services).	Good user experience (SSO)	Single point of Failure and Privacy, security, third party reliance
User-centric (Decentralized IdM)	Decentralized IdMs like BC-IdM follows user-centric IdM model by allowing users to interact with relying parties without a need for an intermediary.	Decentralization (custody control of identity data)	Regulations, standardization and maturity.



21. According to the framework, recommendations to be given to the decision makers, which includes the risk management process results, the general evaluation results, and the comparison results. What other recommendation to be given (if any)? *
If yes, please specify, or instead, write nothing.

____

____

____

____

____

22. Who is the most suitable audience for the developed framework? *

Mark only one oval.

○ Developers

○ Cybersecurity risk assessors

○ Security manager/ Cybersecurity department

○ IdM manager

○ Project development team

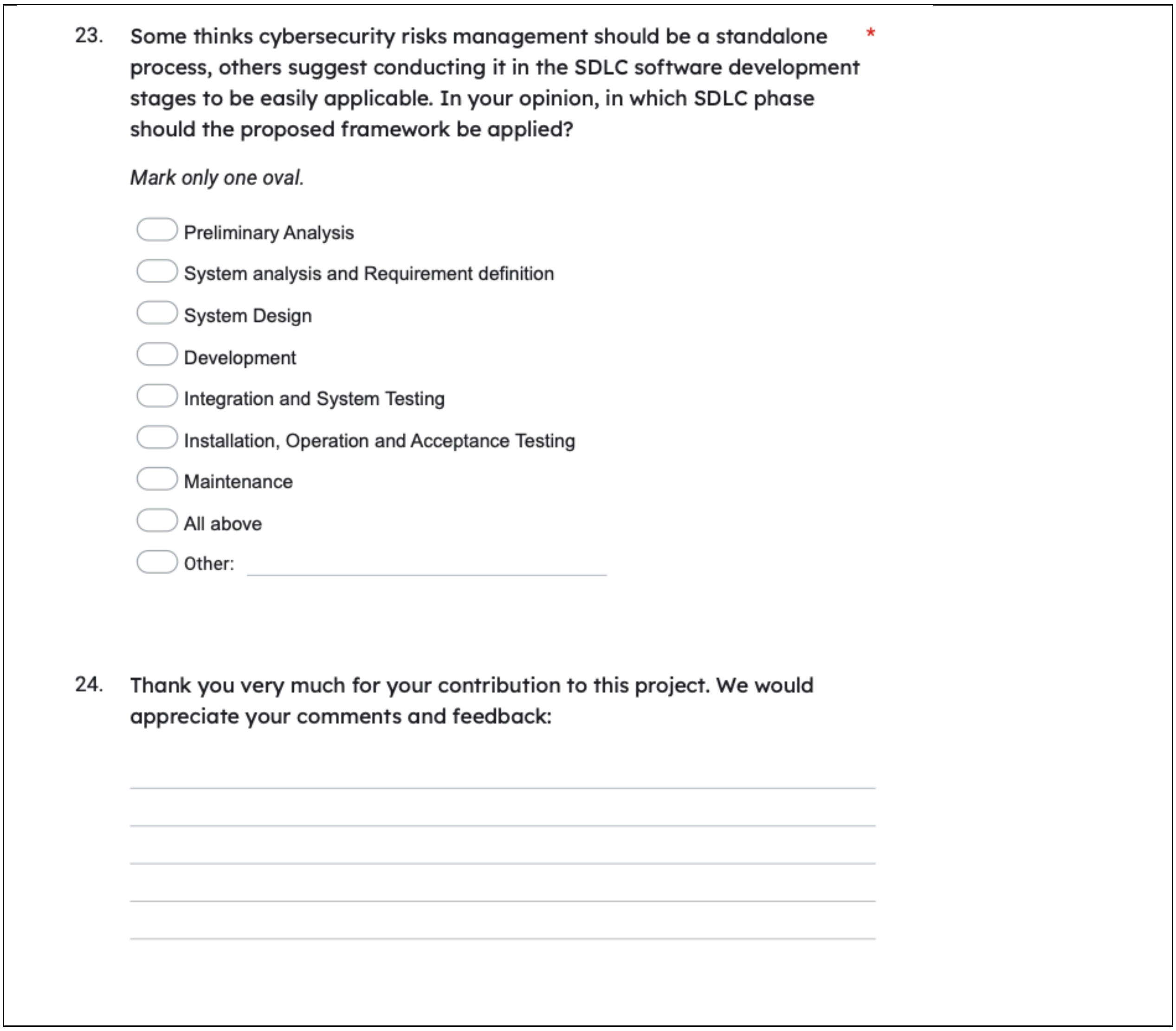
○ Development management team

○ Operational management

○ High administration

○ All above

○ Other: ______________________



23. Some thinks cybersecurity risks management should be a standalone process, others suggest conducting it in the SDLC software development stages to be easily applicable. In your opinion, in which SDLC phase should the proposed framework be applied? *

Mark only one oval.

○ Preliminary Analysis

○ System analysis and Requirement definition

○ System Design

○ Development

○ Integration and System Testing

○ Installation, Operation and Acceptance Testing

○ Maintenance

○ All above

○ Other: ____________________

24. Thank you very much for your contribution to this project. We would appreciate your comments and feedback: