# Appendix A

Table A1. Summary of the retained risk factors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Group** | **Original # in [15]** | **New #** | **Risk factor** | **Scales** |
| Overall project information | 1.4 | 1.1 | What is the project duration? | [<= 3 months, 3 – 6 months, 6 – 12 months, 12 – 24 months, > 24 months] |
| 1.6 | 1.2 | What is the project type? | [Transportation Infrastructure Projects, Government Projects, Healthcare Projects, Large-Scale Commercial Projects, Residential Projects, Other types] |
| 1.7 | 1.3 | Whether there is a dedicated cybersecurity legal team for the project? | [Yes, No, Unsure] |
| 3.1 | 1.4 | What is the scale of your company? | [<= 30, 31 – 60, 61 – 100, 101 – 150, > 150] |
| 3.2 | 1.5 | What is the phase of the construction project when your company is involved? | [Planning and Bidding phase, Design phase, Construction phase, Maintenance & Operation phase, Demolition phase] |
| Project structure | 2.2  (2.2.1 – 2.2.3) | 2.1 (2.1.1 – 2.1.3) | What is the number of sub-teams at different layers of the project?  (The number of sub-teams at different layers of a project indicates the project’s structural complexity and associated cyber risks. Outer-layer sub-teams, often smaller with fewer cybersecurity resources, are generally more vulnerable, while inner-layer teams are typically larger, better equipped, and more security-conscious. Understanding the distribution of sub-teams across layers is crucial for implementing effective, targeted risk management strategies.) | Eight layers, each layer’s scales are: [<= 10, 11 – 20, 21 – 30, 31 – 40, > 40, N/A], “N/A” means this layer is not existent |
| 2.4 | 2.2 | What is the percentage of teams overlapping in different projects?  (The percentage of teams overlapping in different projects refers to the proportion of teams engaged simultaneously in multiple initiatives. This overlap can elevate cyber risks due to shared resources and personnel, which may introduce security gaps and dependencies. Increased team overlap heightens the likelihood of breaches and necessitates robust management strategies to address these vulnerabilities effectively.) | [<= 20%, 21% - 40%, 41% - 60%, 61% - 80%, 81% - 100%] |
| IT factors | 3.3 | 3.1 | Is there a dedicated IT team for the project? | [Yes, No, Unsure] |
| 3.6 | 3.2 | What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project? | [<= 20%, 21% - 40%, 41% - 60%, 61% - 80%, 81% - 100%] |
| 3.7 | 3.3 | What is the network type used for the project: Public or Private?   (Choosing between a public or private network impacts a project’s cybersecurity. Public networks can be vulnerable to attacks due to easier access, while private networks offer enhanced security controls but may be costly and complex to manage. Each type requires specific security approaches.) | [Public network, Private network, Both public and private network] |
| 3.8 | 3.4 | What is the percentage of individuals who fail phishing tests after completing mandatory training? | [<= 20%, 21% - 40%, 41% - 60%, 61% - 80%, 81% - 100%] |
| Management and human factors | 5.1 | 4.1 | What is the average level of commitment to corporate governance, ethical practices and cybersecurity policy? | [Level 1, Level 2, Level 3, Level 4, Level 5] |
| 5.3 | 4.2 | Do you allow password reuse for any project-related software, systems, or accounts (e.g., project management tools, email, internal networks, file storage, etc.)? | [Yes, No] |
| 5.4 | 4.3 | Does internet access within your construction project require Multi-Factor Authentication (MFA) or utilize other methods such as biometrics or face recognition? | [Yes, No] |

*Notes: For detailed information about each risk factor, please refer to [15].*