Review of the current situation

Key questions for suppliers

# To be filled in by the internal IT/OT department:

|  |  |
| --- | --- |
| Supplier number: |  |
| Contact (name): |  |
| Branch: |  |
| Operating in the following branches: |  |
| Questionnaire No: |  |

# To be filled in by the supplier:

|  |  |
| --- | --- |
| Supplier name: |  |
| Service provided by the supplier: |  |
| Job title: |  |
| Date: |  |
| Signature: |  |

# IT security

| 1.1 | Does your company have a valid IT security certificate that is recognised in your industry (e.g. ISO27001 / CoBit / BSI)? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'yes', please specify which certificate: |  |
| 1.2 | How is IT security organised in your company? Describe the positions in your company that deal with IT and specify the people responsible (e.g. CISO, IT Security Officer, CTO). |  |
| 1.3 | Do you do vulnerability management? | Yes ☐  No ☐  I don’t know ☐ |
| 1.4 | If your company were to discover a vulnerability, how and how quickly would you notify us? |  |
| 1.5 | If your company were to experience an internal IT security incident, how and how quickly would you notify us? |  |

# Data security

| 2.1 | Does the way you process data comply with the requirements set out in existing data protection legislation (e.g. Data Protection Act)? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'no', please explain why: |  |
| 2.2 | Do you have a chart that shows how sensitive data is entered into your systems and where it is stored? | Yes ☐  No ☐  I don’t know ☐ |
|  | If your answer is 'no': Would your company be willing to create such a chart? | Yes ☐  No ☐  I don’t know ☐ |

| 2.3 | Does your organisation encrypt sensitive data in transit between systems and at rest in online storage and back-ups? And are your encryption methods up to date, properly maintained and compliant with industry standards? | | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- | --- |
| 2.4 | Does your organisation have a standard process in place for the permanent deletion of data? | | Yes ☐  No ☐  I don’t know ☐ |
| 2.5 | | Do you provide us with IT or OT products that run on our (critical) systems? | Yes ☐  No ☐  I don’t know ☐ |
|  | | Please describe the IT/OT products. |  |

# Computer systems

| 3.1 | Does your company operate its own systems for the services it provides to us? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'no' and the systems you use are provided by third-party providers: who is the provider? |  |
| 3.2 | Are the systems equipped with an up-to-date EDR/XDR solution, and are incidents detected by these advanced antivirus solutions actively managed within your organisation or reviewed by an outsourced SOC? | Yes ☐  No ☐  I don’t know ☐ |
| 3.3 | How quickly could these systems be restored to normal operation after a service interruption or cyber incident? |  |

# Access to computer systems, other devices, workload programs

| 4.1 | Are the systems described above accessed only with personalised user accounts? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
| 4.2 | Are the user accounts your employees use to perform their normal day-to-day work different from the user accounts they use to access our organisation's systems or systems containing our organisation's data? | Yes ☐  No ☐  I don’t know ☐ |
| 4.3 | Do you follow the principle of least privilege in your organisation? | Yes ☐  No ☐  I don’t know ☐ |
| 4.4 | Do you ensure that user accounts with higher permissions do not have this level of permission permanently? | Yes ☐  No ☐  I don’t know ☐ |
| 4.5 | If you use service accounts to provide services, have you ensured that the credentials are stored securely and are not accessible to unauthorised employees? | Yes ☐  No ☐  I don’t know ☐ |
| 4.6 | Is access to systems that contain/process our organisation's data protected by MFA when accessed remotely (via VPN, inter-site access or similar)? | Yes ☐  No ☐  I don’t know ☐ |
| 4.7 | Are all accesses to these systems logged, stored and available for review by our organisation's IT security personnel upon request? | Yes ☐  No ☐  I don’t know ☐ |
| 4.8 | Do you have a detailed password policy in writing? | Yes ☐  No ☐  I don’t know ☐ |

# Awareness

| 5.1 | Have employees been made aware of IT security issues (at the very least the threat of phishing) and have they received the appropriate training? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
| 5.2 | Can the training programme be made available for our organisation's IT Security staff to review? | Yes ☐  No ☐  I don’t know ☐ |