CLUSIL

Working-Group *Information Security Management* (ISM)

Benchmark of Information Security Controls

Questionnaire

General information

Version:	2016-06-03
State:	Final
Project:	CLUSIL Benchmark
Author:	Cédric MAUNY + CLUSIL Benchmark taskforce
Date:	
Distribution:	CLUSIL Benchmark taskforce ; CLUSIL Board ; CLUSIL Members

Distribution list

Recipient	Date	Channel	Reason*
Members of the CLUSIL WG ISM *Benchmark taskforce*	2016-05-27	e-mail	I
CLUSIL Board	2016-06-03	e-mail	V
Members of the CLUSIL	2016-05-31	website	I

***** A: action / V: validation / C: comments / I: information

History

Version	Date	Author (αβ order)	Modifications
0.9.0	2015-10-15	Cédric MAUNY	Consolidation of the questions gathered and developed in the Excel sheet *CLUSIL - List of Questions - Fine Tuning - v20150921* To work on the wording of the questions To prepare the dissemination / collection strategy of answers
0.9.1	2015-12-12	Michael SIM	Review of the wording of the questions (track changes)
0.9.2	2015-12-17	Cédric MAUNY	Update of the document (track changes)
0.9.3	2016-01-04	Cédric MAUNY Eric TIERLING	Review of the question
1.0	2016-01-21	Cédric MAUNY	Final review post CLUSIL EoY 2015 of 2016-01-19
1.1	2016-04-05	Cédric MAUNY	Comments from Cédric MULLER, Jérémy THIMONT, Jean-François MAIRLOT and Michael SIM are taken into account into this version
1.2	2016-04-06	Jürgen BLUM Cédric MAUNY	Some changes
1.3	2016-04-18	Gilles KOZIEL Cédric MAUNY Steve MULLER Eric TIERLING	Integration of proposal of changes
1.4	2016-04-19	Werner ANSORGE Gilles KOZIEL Cédric MAUNY Steve MULLER	Update of the questionnaire further to the WG ISM meeting of 2016-04-18
2.0	2016-05-27	Cédric MAUNY	Finalisation for publication
2.1	2016-06-03	Jean GOETZINGER Cédric MAUNY	Approval by the President of the CLUSIL Integration of comments (questions, Exec Summary, …)

Validation

Name	Role	Responsibility	Date	Signature
CLUSIL Board	Owner of the document	Validation before publication Approval for publication	2016-06-03	Once published on the website of CLUSIL

Member of the CLUSIL WG ISM Benchmark taskforce: benchmark@clusil.lu

Contributors for year 2014

1. Werner ANSORGE
2. Olivier ANTOINE
3. Christophe AJDONIK
4. Émelyne BAUDRIER
5. Jürgen BLUM
6. Alexandre CASTAING
7. Guy ISLER
8. Yann FAGUER
9. Olivier LEONARD
10. Daniel MARNACH
11. Cédric MAUNY
12. Olivier MONTEE
13. Christophe RUPPERT
14. Guillaume SCHAFF
15. Michael SIM
16. Raphaël TABAN
17. Eric TIERLING

Contributors for year 2015

1. Roland BAULER
2. Kamal BENLAFQUIH
3. Jürgen BLUM
4. Adriana CULTRONE
5. Mélanie GAGNON
6. Clément GORLT
7. Cédric MAUNY
8. Steve MULLER
9. Olivier MONTÉE
10. Flavien ROUZAUD
11. Michael SIM
12. Eric TIERLING

Contributors for year 2016[1]

1. Jürgen BLUM
2. Mélanie GAGNON
3. Gilles KOZIEL
4. Jean-Francois MAIRLOT
5. Cédric MAUNY
6. Cédric MULLER
7. Steve MULLER
8. Michael SIM
9. Eric TIERLING
10. Jeremy THIMONT

[1] By the date of the publication of the questionnaire

Executive Summary

This document is the "*Benchmark of Information Security Controls*" of the CLUSIL.

The project was announced during the end-of-year event 2013 of the CLUSIL as upcoming deliverable of the working-group *Information Security Management*. The main goal was to create a questionnaire of security related controls for the community of information security experts. The project is focused on the Luxembourg information security landscape and aims at assessing questions that are not asked in other benchmarks or surveys.

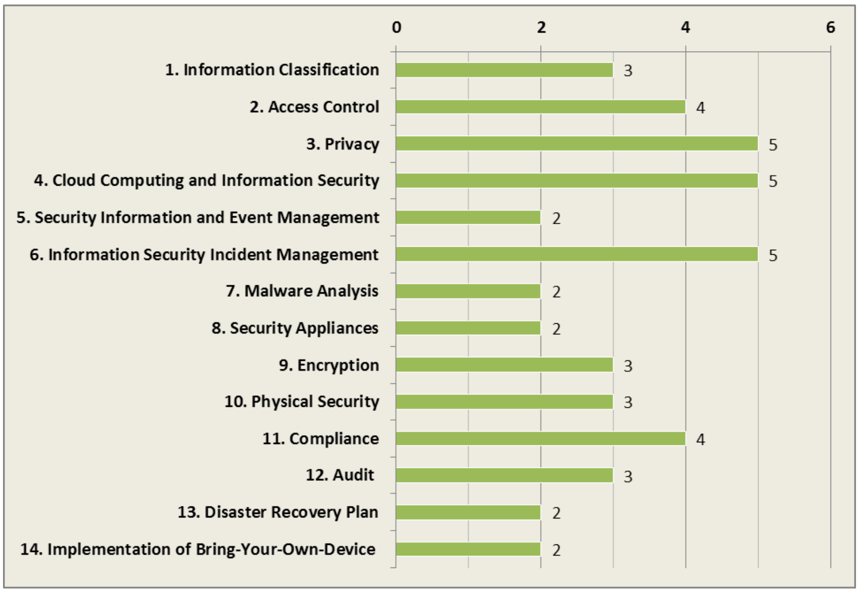
A total of 57 questions have been drafted, some of them may trigger to answer additional questions according to your answers; as such a total of 67 potential questions could be reached. The set of questions is distributed into 14 categories (45 technical questions, generic questions excluded) as depicted in the following tables and figures.

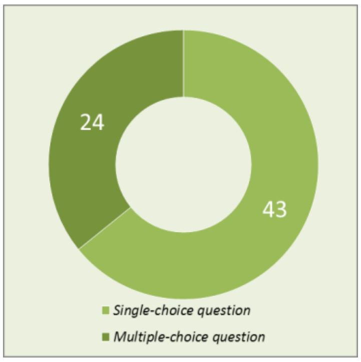
This document represents the final version of the questionnaire prepared by the Benchmark Taskforce after several months of meetings, e-mail exchanges, fruitful comments and interesting discussions, as approved by the Board of CLUSIL.

Overview on the set of questions

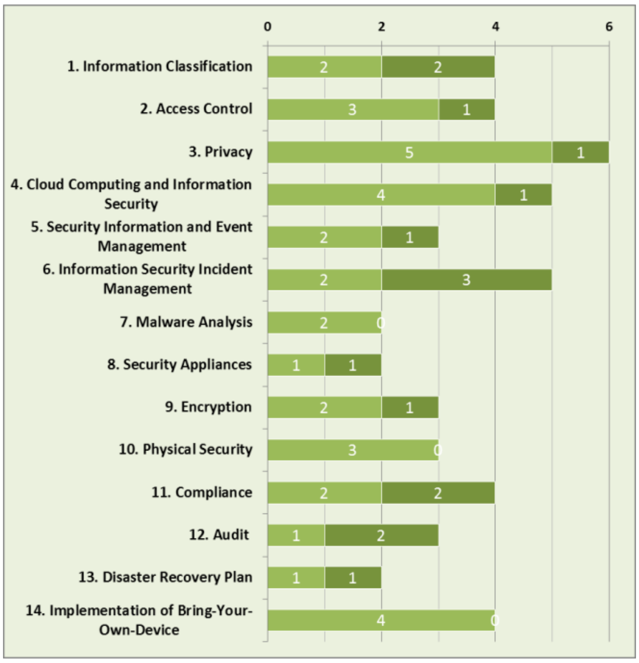
57 questions distributed over 15 categories:

0. Generic questions	12
1. Information Classification	3
2. Access Control	4
3. Privacy	5
4. Cloud Computing and Information Security	5
5. Security Information and Event Management	2
6. Information Security Incident Management	5
7. Malware Analysis	2
8. Security Appliances	2
9. Encryption	3
10. Physical Security	3
11. Compliance	4
12. Audit	3
13. Disaster Recovery Plan	2
14. Implementation of Bring-Your-Own-Device	2
TOTAL	*57*





	Single-choice question	Multiple-choice question
0. Generic questions	9	8
1. Information Classification	2	2
2. Access Control	3	1
3. Privacy	5	1
4. Cloud Computing and Information Security	4	1
5. Security Information and Event Management	2	1
6. Information Security Incident Management	2	3
7. Malware Analysis	2	0
8. Security Appliances	1	1
9. Encryption	2	1
10. Physical Security	3	0
11. Compliance	2	2
12. Audit	1	2
13. Disaster Recovery Plan	1	1
14. Implementation of Bring-Your-Own-Device	4	0
TOTAL	*43*	*24*



Presentation of the CLUSIL Benchmark for Information Security Controls / FAQ

Who is the target audience?

Target audience is (Chief) Information Security Officer ((C)ISO), Responsable de la Sécurité des Systèmes d'Information (RSSI), IT Manager, … anyone who has the information security within his scope inside its company

How to enter the answers?

The questionnaire can be printed out and send out using the restricted area of the CLUSIL website.

Improvement will consist in publishing the questionnaire as online survey (to come)

What is the scope of the questionnaire?

Unless specified, every questions apply to the entity located in Luxembourg.

What are the different types of questions?

There are two types of questions

□ Multiple-choice question

○ Single-choice question

How privacy and anonymity are ensured?

Privacy and anonymity of the respondent is the critical success factor of such survey and CLUSIL considers privacy and anonymity of the respondents as his highest priority. The questionnaire will be anonymously uploaded within the restricted area of the CLUSIL. Once uploaded, the filled out form will be anonymously posted to a specific mailing-list of the CLUSIL for analysis. Anonymity is preserved at all circumstances. No logs of the uploading activity will be kept.

How long to fill-out the form?

Beta-testers were able to fill-out the form in less than 30 minutes.

Is there any sequence order and mandatory questions?

It is not mandatory to follow the sequence of categories of questions. Categories of questions are independent and can be answered in any order. Sequence of questions inside a same category may be relevant to follow.

Not question is mandatory. There is no obligation to answer to every questions. However, for the completeness of the survey and scientific approach of the study, it is preferable to answer to each of them and respondents are requested to fill out all the questions.

Table of Contents

Acronyms

APT	Advanced Persistent Threat
BCP	Business Continuity Plan
BIA	Business Impact Analysis / Assessment
BYOD	Bring-Your-Own-Device
CERT[2]	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLUSIL	CLUb de la Sécurité de l’Information - Luxembourg
CMMI	Capability Maturity Model Integration
CNPD	Commission Nationale de Protection des Données
CSIRT	Computer Security Incident Response Team
CSSF	Commission de Surveillance du Secteur Financier
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DPO	Data Protection Officer
DRM	Digital Rights Management
DRP	Disaster Recovery Plan
EU	European Union
IDS	Intrusion Detection System
ILR	Institut Luxembourgeois de Régulation
IPS	Intrusion Prevention System
ISO[2]	*International Standardization Organisation*
ISO	Information Security Officer
ISP	Internet Service Provider
LAN	Local Area Network
MAN	Metropolitan Area Network
MDM	Mobile Device Management
MTD	Maximum tolerated Downtime
NGIPS	Next-Generation Intrusion Prevention System
PCI-DSS	Payment Card Industry – Data Security Standard
PIA	Privacy Impact Assessment
PSDC	Prestataire de Service de Dématérialisation et de Conservation
PSF	Professionnel du Secteur Financier
RSSI	Responsable de la Sécurité des Systèmes d’Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SOC	Security Operations Centre
WAN	Wide Area Network

[2] Generally not to be considered as an acronym in that meaning

0. Generic questions

0.1. What is your primary business sector of activity? [multiple-choice]

□ Banking
□ Insurance
□ Industry
□ Support-PSF
□ Health
□ Governmental (included EU and other Institutions)
□ Service provider
□ ICT
□ Advisory
□ Other (please specify: ____________________)

0.2. How large is your company (in Luxembourg)? [single-choice]

○ Less than 10 staff
○ <=50 staff
○ <=100 staff
○ <=250 staff
○ <=500 staff
○ >500 staff

0.3. Is the Luxembourg entity also part of a larger group? [single-choice]

○ Yes, BeNeLux / BeLux group
○ Yes, European group
○ Yes, worldwide group
○ No, we are independent

If yes, what is the total size of the Group? [single-choice]

○ Less than 50 persons
○ >50 persons
○ >250 persons
○ >500 persons
○ >1 000 persons
○ >2 500 persons
○ >5 000 persons
○ >10 000 persons
○ More than 25 000 persons

If yes, how would you designate the Luxembourgish branch? [single-choice]

○ Head office / Headquarter
○ Subsidiary
○ Other (please specify: ____________________)

If yes, what is the level of independence on the Information Security Strategy? [multiple-choice]

□ Information Security Strategy is decided at Group-level and local-level has to take it over / implement it at local-level.
□ Information Security Strategy is decided at local-level.
□ There is a hybrid approach: Some decisions of the Group-level are implemented, supplemented by a strategy decided at the local-level

0.4. What is your primary field of responsibility? [multiple-choice]

□ General Management / Board of Director
□ Financial
□ Information Security
□ Data protection
□ IT department
□ Risk Management
□ Audit department
□ Compliance department
□ Application development
□ Other (please specify: ____________________)

0.5. How large is the Information Security team within the Luxembourgish entity? [single-choice]

○ Less than 2 full-time-equivalent
○ Between 3 and 5 full-time-equivalent
○ Between 6 and 10 full-time-equivalent
○ Between 11 and 25 full-time-equivalent
○ Between 26 and 50 full-time-equivalent
○ More than 50 full-time-equivalent

0.6. How to categorise the staff of Information Security team within the Luxembourgish entity? [multiple-choice]

□ Internal staff under direct contract
□ Full-time job
□ Part-time job
□ Outsourced activity

0.7. What are the legal and regulatory requirements you have to comply with? [multiple-choice]

□ Commission de Surveillance du Secteur Financier
□ Institut Luxembourgeois de Régulation
□ Commissariat aux Assurances
□ Commission Nationale de Protection des Données
□ Group Compliance
□ Other (please specify: ____________________)

0.8. Are you currently following a specific security framework / best practices? [multiple-choice]

□ Yes, ISO/IEC 27001 version 2005
□ Yes, ISO/IEC 27001 version 2013
□ Yes, ISO/IEC 27017[3] version 2015
□ Yes, ISO/IEC 27018[4] version 2014
□ Yes, PCI-DSS
□ Yes, PSDC
□ Yes (please specify: ____________________)
□ No

0.9. Is the entity willing to acquire certified status (or, where applicable, to become at least compliant with)? [multiple-choice]

□ Yes, against ISO/IEC 27001
□ Yes, with ISO/IEC 27017
□ Yes, with ISO/IEC 27018
□ Yes, against PCI-DSS
□ Yes, against PSDC
□ Yes, against other referential (please specify: ____________________)
□ No

If yes, in which timeframe: [single-choice]

○ Less than 1 year
○ Between 1 and 3 years
○ More than 3 years

[3] Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[4] Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

If yes, for which reason [multiple-choice]

□ Requested by customers
□ Requested by head-office / Group
□ To develop activities and creating new market opportunities
□ For regulatory requirements
□ Other (please specify: ____________________)

0.10. How important is your IT environment to achieve company business goals? [single-choice]

○ Vital
○ Important
○ Useful
○ Other (please specify: ____________________)

0.11. How do you self-assess your information security maturity level at global overview? (for instance according to following CMMI-levels) [single-choice]

○ Maturity Level 0 - Not existent

○ Maturity Level 1 – Initial (chaotic)
It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an *ad hoc*, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes[5].

○ Maturity Level 2 – Repeatable
It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress[5].

○ Maturity Level 3 – Defined
It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization[5].

○ Maturity Level 4 - Managed
It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level[5].

○ Maturity Level 5 – Optimizing
It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements[5].

[5] https://en.wikipedia.org/wiki/Capability_Maturity_Model

0.12. What is the expected evolution of your information security investments for 2017 compared to 2016? [single-choice]

	Major decrease (more than 10%)	Decrease (less than 10%)	Stable	Increase (less than 10%)	Major increase (more than 10%)	Information security budget is not managed by my Department but managed by another Department
Financial (budget €)	❍	❍	❍	❍	❍	______________
Human (FTE)	❍	❍	❍	❍	❍	______________
Technologies	❍	❍	❍	❍	❍	______________
Operations	❍	❍	❍	❍	❍	______________
Threats	❍	❍	❍	❍	❍	______________
Outsourcing	❍	❍	❍	❍	❍	______________

1. Information classification

1.1. Do you have an information security policy? [multiple-choice]

- □ Yes, it is formally defined and communicated to all employees
- □ Yes, it is formally defined and communicated to third-parties
- □ The information security is defined but not (yet) formally published / endorsed by the upper-management
- □ No security policy is defined but this is planned within (please specify: ____________________) months / years

1.2. Have you classified your data and if so for which purpose? [multiple-choice]

- □ To reinforce information security
- □ To determine the security needs according to ISO/IEC 27001
- □ To determine the total value of our assets
- □ To identify data related to privacy
- □ In the context of BCP/DRP
- □ Other (please specify: ____________________)
- □ No classification is implemented

If no classification is implemented yet, are you planning to do so within the following timeframe? [single-choice]

- ○ Less than 1 year
- ○ Between 1 and 3 years
- ○ More than 3 years
- ○ I do not know

1.3. How frequently is the data classification(s) process reviewed? [single-choice]

- ○ On-going compliance / on a continuous approach
- ○ Annually
- ○ Every 3 years
- ○ Other (please specify: ____________________)

2. Access Control

2.1. What type of credentials do you use? [single-choice]

	For critical accesses	**For regular accesses**
Something you know (passwords, …)	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years
Something you have (tokens, smart cards, mobile devices)	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years
Something you are (biometric)	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years	○ Mandatory ○ Optional ○ Not available ○ We are going to run such a project within (please specify: ___________) months / years

2.2. Do you have a password policy in place to ensure minimum password strength (e.g. minimum complexity, frequency of change, etc.)? [single-choice]

○ Yes, it is implemented, enforced and audited for all systems on a given frequency (please specify: ____________________)
○ Yes, it is implemented on the systems and enforced
○ Yes, but it is more a guidelines in the sense of good-practices
○ No
○ I do not know

2.3. Are you monitoring account usage? [single-choice]

○ Yes, this is implemented and reports are regularly reviewed (please specify the frequency: ____________________)
○ No, but this is a project (please specify the timeframe: ____________________)
○ No, not at all

2.4. What happens after too many false login attempts on regular accounts? [multiple-choice]

- □ Lockout time
- □ Manual activation by administrator
- □ Automatic re-activation after a predefined time (please specify the duration: ____________________)
- □ Reactivation by user through out-of-band communication means
- □ Alarm triggered by a SIEM
- □ Alarm triggered by a SIEM and investigated on demand
- □ Alarm triggered by a SIEM and systematically investigated
- □ Nothing / undefined
- □ Other (please specify: ____________________)

3. Privacy

3.1. Who is in charge of personal data protection? [multiple-choice]

□ Data Protection Officer
□ (Chief) Information Security Officer
□ Chief Information Officer
□ Board of Directors
□ Compliance unit
□ Nobody
□ Other (please specify: ____________________)

3.2. Are you using external providers to store personal data outside of your enterprise (not on-premises)? [single-choice]

○ Yes
○ No
○ I do not know

If yes, where is it located? [single-choice]

○ In Luxembourg
○ Within the EU
○ Outside of the EU
○ I do not know

3.3. Is your Data Protection Officer working independently or does his/her function belong to another unit such as compliance or legal? [single-choice]

○ Independent role
○ Part of Compliance unit
○ Part of Legal unit
○ We do not have a Data Protection / Privacy Officer
○ Other (please specify: ____________________)

3.4. Do you know about the new EU Regulation on Privacy, the General Data Protection Regulation (GDPR)? [single-choice]

○ Yes, I am well informed
○ Yes, but I am not sufficiently informed yet
○ I know of this Regulation but I consider this as not applicable to my business
○ No, not much
○ No, but I wait until the legislation is enacted

3.5. Do you feel concerned by the upcoming EU Regulation on Privacy? [single-choice]

○ Yes, totally
○ Yes, but this is out of my scope of responsibilities
○ No, not at all
○ I do not know

4. Cloud Computing and information security

4.1. Is your company using Cloud services for business purpose (including shadow IT)? *(several Cloud Services Provider may be used, please check all as appropriate)* [multiple-choice]

- □ Yes and the Cloud service provider is located in Luxembourg.
- □ Yes and the Cloud service provider is located within the EU.
- □ Yes and the Cloud service provider is located in a non-EU country.
- □ Yes, but I do not know where the Cloud service provider stores our business data.
- □ Yes, although it is forbidden by internal policies
- □ No, this is forbidden by internal policies.
- □ No, not at all.
- □ I do not know.

4.2. Do you trust Cloud computing from a security perspective? (note: question about privacy is addressed just below) [single-choice]

- ○ Yes, but only if the Cloud service provider is located in Luxembourg.
- ○ Yes, even if the Cloud service provider is located outside of Luxembourg.
- ○ Yes, but only if the Cloud service provider complies with ISO/IEC 27017[6].
- ○ Yes, but only if the Cloud service provider is a PSF.
- ○ It depends (please specify: ____________________).
- ○ No, not at all.

4.3. Do you trust Cloud computing from a privacy perspective? [single-choice]

- ○ Yes, but only if the Cloud service provider is located in Luxembourg.
- ○ Yes, even if the Cloud service provider is located outside of Luxembourg.
- ○ Yes, but only if the Cloud service provider complies with ISO/IEC 27018[7].
- ○ It depends (please specify: ____________________).
- ○ No, not at all.

[6] Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[7] Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

4.4. Is your company using Cloud services for security purposes: “Security-as-a-Service? [single-choice]

○ Yes, for all security mechanisms and solutions (such as anti-malware, APT, vulnerability scans, Cloud-based firewalls, …)
○ Yes, for some security mechanisms and solutions (such as anti-virus, Cloud-based firewalls, SIEM-as-a-Service, etc.)
○ No, but it is planned (please specify the timeframe: ____________________)
○ It depends (please specify: ____________________).
○ No, not at all.

4.5. What about you as an individual (not as a company): are you using Cloud services? [single-choice]

○ Yes and the Cloud service provider is located in Luxembourg.
○ Yes and the Cloud service provider is located within the EU.
○ Yes and the Cloud service provider is located in a non-EU country.
○ Yes, but I do not know where the Cloud service provider stores our business data.
○ Yes, although it is forbidden by internal policies
○ No, this is forbidden by internal policies.
○ No, not at all.
○ I do not know.

5. Security Information and Event Management (SIEM)

5.1. Is security event monitoring performed within your company? [single-choice]

○ Local Team / Local SOC
○ Outsourced to external entity within the Group
○ Outsourced to external entity outside of the Group
○ No security event monitoring today but there is a plan to have it
○ No security event monitoring plan

If security event monitoring is performed, how is it performed? [single-choice]

○ On a 24/7 basis with permanent resources
○ On a 24/7 basis with on-call services (from a single location)
○ On a 5 days a week / 8 hours per day basis (normal business hours)
○ On a 5 days a week / 12 hours per day basis (extended hours)

5.2. What are the key criteria influencing your strategy for security event monitoring? [multiple-choice]

□ Customer expectations
□ Visibility on current security posture
□ Legal and regulatory constraints
□ Operational constraints
□ Financial constraints
□ Business continuity constraints (RTO, RPO, MTD)
□ Alignment with business objectives
□ As part of the risk mitigation plans for given risk(s)
□ Other (please specify: ___________________)

6. Information Security Incident Management

6.1. Is cybercrime a concern for your organisation / personnel? [single-choice]

○ Highest priority and risk
○ One of the highest priority and risk
○ No specific consideration

6.2. Have you ever faced major / serious security incidents within the past 12 months? (such as but not limited to Advanced Persistent Threats / APT) [single-choice]

○ Yes, more than 10 times
○ Yes, between 5 and 10 times
○ Yes, less than 5 times
○ Nothing has been detected
○ No, not at all

6.3. Have you already established a communication strategy in case of an incident? [multiple-choice]

□ Yes, for external communication (e.g. to press)
□ Yes, for internal communication (e.g. to employees)
□ No, but external communication is under development
□ No, but internal communication is under development
□ No, no communication at all
□ I do not know

6.4. Do you have a security incident response plan in case of an incident? [multiple-choice]

□ Yes
□ Yes, for incidents triggered by human reporting mechanisms
□ Yes, for incidents triggered by SIEM
□ Yes, for incidents triggered by IDS / IPS
□ Yes, for incidents triggered by other solutions (anti-virus, firewall logs, …)
□ The strategy is based upon the criticality of the incident
□ No

6.5. Are you maintaining a regular relationship with a CERT/CSIRT? [multiple-choice]

- ❑ Yes, CERT/CSIRT activities are internally managed in Luxembourg
- ❑ Yes, CERT/CSIRT activities are internally managed within the Group
- ❑ Yes, CERT/CSIRT activities are outsourced to a third party / expert in Luxembourg
- ❑ Yes, CERT/CSIRT activities are outsourced to a third party / expert in foreign country
- ❑ Some activities are shared with others in my economic sector
- ❑ No, but it is planned (please specify the timeframe: ____________________)
- ❑ Not, not at all

7. Malware analysis

7.1. Are malware analysis and digital forensics activities part of your security strategy? [single-choice]

○ Yes, fully
○ Yes, but only partially
○ No
○ Not currently, but this is planned (please specify in which timeframe: ____________________)

7.2. How are malware analysis and digital forensics activities performed within your company? [single-choice]

○ Local Team
○ Outsourced to external entity within the Group
○ Outsourced to external entity out of the Group
○ Automatically performed by security appliances and software on endpoints
○ No malware analysis is performed

8. Security Appliances

8.1. What are your existing security appliance solutions and which zones are protected? (Please check the corresponding matches) [multiple-choice]

	DMZ	LAN / MAN	ISP / WAN	Datacenter	Other (please specify: ____________)
Firewall	❑	❑	❑	❑	____________
IPS/NGIPS	❑	❑	❑	❑	____________
Proxy Web	❑	❑	❑	❑	____________
Reverse Proxy	❑	❑	❑	❑	____________
Email Security	❑	❑	❑	❑	____________
(Web) Application firewalls	❑	❑	❑	❑	____________
APT / anti-malware appliances	❑	❑	❑	❑	____________
Load-Balancers	❑	❑	❑	❑	____________
(Anti) DDos	❑	❑	❑	❑	____________
Data Loss Prevention (DLP)	❑	❑	❑	❑	____________
Security Incident and Event Management (SIEM)	❑	❑	❑	❑	____________
Honeypot	❑	❑	❑	❑	____________
Other (please specify: ____________)	____________	____________	____________	____________	____________

8.2. Have you implemented an IT solution for DLP? [single-choice]

○ Yes this is in place (please specify since when: ____________________)
○ No but this is in project (please specify the timeframe : ____________________)
○ No not at all

9. Encryption

9.1. Are you encrypting data on your internal network? [single-choice]

○ Yes, all data regardless of the content
○ Yes, but only some sensitive data is encrypted
○ Yes, but limited to passwords that are sent over the LAN during login
○ No, the internal network is already sufficiently protected by other means
○ I do not know

9.2. Are you electronically signing your company’s emails? [single-choice]

○ Yes, systematically, even when communicating with external entities
○ Yes, systematically, but only within the company or group
○ Yes, but only sporadically. Decision is left to the end-user
○ No
○ I don't know

9.3. How are you using encryption? [multiple-choice]

□ For stored data
□ For exchanged data over the LAN
□ For e-mail
□ For Digital Rights Management (DRM) purposes
□ For data in transit
□ For data at rest (fileserver, …)
□ For archived data at rest (backup, …)
□ We do not use encryption
□ Other (please specify: ____________________)

10. Physical Security

10.1. Have you referenced the requirements for physical security into contracts and regulations? [single-choice]

○ Yes
○ No
○ I am not managing this part of information security
○ I do not know

10.2. How frequently do you review physical access rights to restricted physical areas? [single-choice]

○ Yes, annually
○ Yes, quarterly
○ Yes, but with another frequency (please specify the frequency: ____________________)
○ No

10.3. Do you regularly assess protection devices (such as fire extinguishers, alarms and back-office configurations, etc.) and formally document the outcome of the reviews? [single-choice]

○ Yes, checked by internal staff
○ Yes, checked by third party
○ No
○ I am not managing this part of information security

11. Compliance

11.1. Taking accepted national and European laws and regulations, how do you assess the workload to comply with regulations impacting your company in terms of man-hours attributed to the management of information security? [single-choice]

○ Major impact
○ Controllable impact
○ Negligible impact
○ No impact

11.2. What types of risk assessment / impact analysis methods are you currently leading? [multiple-choice]

□ PIA
□ Information security
□ BIA
□ Other (please specify: ____________________)
□ None of them

11.3. What types of risk assessment do you plan to perform within 2 years? [multiple-choice]

□ PIA
□ Information security
□ BIA
□ Other (please specify: ____________________)
□ None of them

11.4. Do you have audit and/or compliance personnel specialized in information security related topics? [single-choice]

○ Yes, in both audit and compliance departments
○ Only in audit department
○ Only in compliance department
○ None of them
○ This is outsourced to another entity internal of the Group
○ This is outsourced to a third-party
○ Other strategy (please specify: ____________________)

12. Audit

12.1. What types of security audits have been performed? [multiple-choice]

	Vulnerability scan (automatic security audits relying on tools such as Nessus or Qualys)	**Penetration testing** (manual security audits also known as Ethical Hacking)	**Compromise assessments**
External network	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Internal network	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Application (web / mobile / API)	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
WiFi	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
VoIP	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Remote Access (Citrix)	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Email infrastructure	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Denial-of-Service	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Source Code Review	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months
Other (please specify: ____________)	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months	□ during the last 12 months □ planned for the next 12 months

12.2. What types of social engineering tests have been performed? [multiple-choice]

	During the last 12 months	**Planned for the next 12 months**
Social engineering by phone	❑	❑
Social engineering face-to-face	❑	❑
Physical intrusion (red-team)	❑	❑
Email phishing test	❑	❑
Other (please specify: ____________________)	❑	❑

12.3. How frequently are security awareness campaigns conducted? [single-choice]

❍ Only at the time of the recruitment
❍ Regular basis for all of the employees (please specify the frequency: ____________________)
❍ Regular basis for part of the employees (please specify the frequency: ____________________)
❍ Rarely, No systematic trainings but regular one-way communications
❍ Never

13. Disaster Recovery Plan

13.1. Is your data synchronized between the production site and the recovery site? [single-choice]

○ Yes, all of the data
○ Yes, but only for some of the data (for instance the most critical data)
○ I do not know
○ No

13.2. How is it done? [multiple-choice]

□ In real-time
□ In near real-time
□ Once per day
□ Other (please specify: ____________________)

14. Implementation of Bring-Your-Own-Device

14.1. Do you allow BYOD practices within your company? [single-choice]

○ Yes, totally
○ Yes, with limitation (specify which ones below)
○ No, not at all
○ No, but this planned (please specify the timeframe: ____________________)
○ I do not know

If <Yes, with limitation> how do you manage the risk? [single-choice]

○ With in-house solution such as MDM
○ With outsourced solution such as MDM
○ The risk is accepted without insight and detailed knowledge
○ Other (please specify: ____________________)

If <No> why not? [single-choice]

○ Corporate users are provided with corporate devices
○ The cost of Risk outweigh the benefits
○ Data protection requirements are too high to allow this practice
○ No technical solutions currently provide sufficient control to implement this strategy
○ Other (please specify: ____________________)

14.2. Have you implemented / authorized BYOD but you finally decided to reverse this decision and forbid it? [single-choice]

○ Yes, we forbid BYOD (please specify the duration: ____________________) after having authorized it
○ No, BYOD is in place (please specify since when: ____________________) and still allowed
○ No we do not allow BYOD

end of the questionnaire