Internal Audit Checklist

A. Name of the internal auditor — add name
Date of assessment — add date

B. Documentation

Internal audit procedure	Created / Reviewed and uploaded in section policies & procedures
Internal auditor role description	Created / Reviewed and uploaded in section policies & procedures
Final report	Final Internal Audit report uploaded in section Internal Audit
Findings documented	Findings copied in sections Internal Audit
Improvements	Improvements created for each finding - section Improvements

C. Before starting the assessment

- Mention as unapplicable controls that are excluded from the scope according to the SoA
- If an Information Security Risk Assessment and/or external audit has been performed the year before, check in Compleye Online Internal Audit if all findings have been addressed and improvements have been closed.

D. Performing the assessment

- Include links to evidence from Compleye Online and/or from other sources in the "Evidence" column
- If evidence is not sufficient, fill in the "Topics for invesigation" column with questions and/or remarks

Review findings from previous internal and external audits to determine if improvements have been addressed and are effective:

- If improvements have been implemented and are effective, notify that the improvement is closed
- If the improvement has not been implemented, notify this in the "Topics for investigation" column
- When all criteria have been reviewed, schedule an investigation meeting with the ISMS team members
- Provide them with the assessment before the investigation meeting so they can already review questions and remarks and give answers/information in the "Investigation notes" column

E. Investigation meeting

Date of investigation meeting — add date & people attending

- During the investigation meeting, review all questions and remarks of the "Topics for investigation" column.
- You can close findings for which the ISMS team can provide sufficient evidence of implementation.
- Concerning findings for which there is no evidence of implementation, classify the finding as non-conformity or concern according to the classification defined in the Internal Audit procedure. If possible, define improvements with the team for these findings.

F. Final report

- After the findings have been finalized and classified, you can list them in the final report together with the
- Once the final report is finalized, you can send it to the ISMS team and management for approval

Disclaimer: this template provides guidelines on how to perform an Internal audit assessment Ch4-10. The criteria listed below are suggestions based on what evidence can be found in Compleye Online - you can add the link to specific section in Compleye Online. If you store evidence in other tooling you can refer to. It is possible for each organization to define new criteria adjusted to the organization's context and their own requirements as defined in their policies and procedures.

Results Internal Audit - Ch 4-10

Chapter	Norm Description		Criteria	Links to evidence	Topics for investigation	Investigation Notes	Classification of Finding (after Investigation)	
							Non-conformity	Opportunity for improvement
4. Context of the Organization	4.1 Organization and context	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	Check in Compleye Online Strategy and Ambition section if the following evidence/information was provided : Company, Product, Customer & Third Parties and Compliance Challenge.					
			Check in the latest Management Review if the following topics were addressed: Change in external and internal topics that are relevant to the ISMS, Feedback from Stakeholders that concerns the availability, integrity and retransmission of information					
			As per above, check if the information provided is not older then 1 year old.					
	4.2 Interested parties and their Requirements	Final Internal Audit report uploaded in section Internal Audit	Check in Compleye Online Interested Parties & Legal Requirements whether the stakeholders and (legal) requirements were defined.					
			As per above, check if this overview is not older than 1 year.					
			Check in Compleye Online if the information in the Global Impact customers/projects was defined.					
			As per above, if this information is available check if this information is not older than one year and approved.					
	4.3 Scope of ISMS	The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a. the external and internal issues referred to in 4.1, b. the requirements referred to in 4.2 c. interfaces and dependencies between activities performed by the organization, and those that are performed by other organization. The scope shall be available as documented information.	Check in Compleye Online ISO Certification or Strategy & Context sections if the ISMS scope was defined and documented.					
			As per above, check if the review of the scope is not older than 1 year .					
	4.4 ISMS	The management shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	Check the Improvement section and verify whether the improvements have the assigned owner and are addressed within the established deadlines.					
			Check if the improvements are included in the Management Review document.					
5. Leadership	5.1 Leadership and Commitment	Top Management shall demonstrate leadership and commitment with respect to the information security management system by: a)Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization. b)Ensuring the integration of the information security management system requirements into the organization's processes. c)Ensuring the integration of the information security management system requirements into the organization's processes. d)Ensuring that the resources needed for the information security management system are available e)Communicating the importance of effective information security management and of conforming to the information security management system requirements f)Ensuring that the information security management system achieves its intended outcomes g)Directing and supporting persons to contribute to the effectiveness of the information security management system h)Promoting continual improvement	Check if the Security Policy and supporting Security Procedures were documented and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					
			Check in Compleye Online section Strategy & Ambition section if the security objectives were defined.					
			Check if the Security Awareness Training refers to the security management procedures and was delivered in the last twelve months.					
	5.2 Policy	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. e) be available as documented information; f) be communicated within the organization; g) be available to interested parties, as appropriate.	Check if the Security Policy and supporting Security Procedures were documented and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					
			Check if the policies and procedures were reviewed less than a year ago.					
			Check if the relevant security metrics were defined in Compleye Online and owners are assigned to each metric					
			Is the CTO involved in the Risk Assessments such as ISRA, High Risk Supplier Assessment.					
			Check if the ISMS team members were involved in defining the improvements during the management review by veryifying if they were present in the evaluation meeting?					
			Check if the Security Policy is given to new employees as part of the onboarding process.					
			Check in information Security Communication Policy - if and how the security policy is made available to interested parties. (e.g. customers)					
	5.3 Roles and Responsibilities	Top Management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibilities and authority for: a)Ensuring that the information security management system confirms to the requirements of this International Standards, and b)Reporting on the performance of the information security management system to top management.	Check if the ISMS Roles were established and the ISMS competencies reviewed and approved by the CEO.					
			Check if the ISMS competencies are reviewed and assigned on the annual basis.					
			Check if the selected competencies for each role are reflected in the job descriptions.					
			Check if the Security Awareness Training introduced the ISMS team members.					
			Check if the Security Awareness Training is provided to the new team members. Documented in HR Policy - and a control in place to check on the awareness training for new team members.					
6.Planning	6,1	**Actions to address risks and opportunities**						
	6.1.1 General	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement the actions into its information security management system	Check in Compleye Online Interested parties and legal requirements section if the ISMS reference field is filled in to evidence how the requirements are addressed in the organization's ISMS.					
			Check if there is an X-Ray in place and if the X Ray is reviewed on a regular basis and any changes are taken into consideration.					
	6.1.2 Information Security Risk Assessment.	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:1) the risk acceptance criteria; and2) criteria for performing information security risk assessments) ensures that repeated information security risk assessments produce	Check if the following risks assessments have taken place on a yearly basis:					
			ISRA					
			Supplier Assessment					
			BCP					

		consistent, valid and comparable results; identifies the information security risks:1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and2) identify the risk owners;d) analyses the information security risks:1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and3) determine the levels of risk;e) evaluates the information security risks:1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and2) prioritize the analyzed risks for risk treatment. The organization shall retain documented information about the information security risk assessment process.	DRP					
			GDPR Assessment					
			Check if there are compliance assessments of potential customers and if the results of those have led to improvements that are recorded in the Improvement section. If there are no customer Assessment, check if commercial contracts with customers comply with the organization's general SLA / T&C documented in the legal section (sample check).					
			Check if all assessment are being evaluated by ISMS Team and approved by MT.					
			Check if the defined improvements are subject to check on effectiveness - by checking 3 random improvements cards that are closed and effectiveness is reported on the cards					
			Check in latest Management Review if the effectiveness of the entire ISMS system is covered.					
	6.1.3 Information security risk treatment	The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results;b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source.c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;e) formulate an information security risk treatment plan; andf) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	Check if the risk treatment procedure includes the selection of risk treatment options, depending on the results of the risk assessment					
			Check if Compleye Online measures and controls section includes the defined controls together with the assigned monitoring frequency and owner.					
			Check if the individuals measures and controls were addressed at the planned intervals.					
			Check if the Statement of Applicability was issued.					
			Check if the controls that are in scope were marked as applicable.					
			Check if the justification for controls exclusion were included in the Statement of Applicability.					
	6.2 Security Objectives	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated	Check in Compleye Online section ISMS Objectives and/or Management Review, if the objectives were defined and are measurable					
			Check if the objectives are measurable as well as aligned with the security policy, results of the risk assessment and requirements listed in the Interested parties section					
			Check in the objectives were addressed in the last Security Awareness Training.					
			Check if the objectives defined are not older than 1 year.					
			Check if it was outlined how the defined security objectives will be achieved (High Level): owner, deadline, what will be done and evaluation of the results					
7. Support	7.1 Resources	The organization shall determine and provide the resources needed for establishment, implementation, maintaince and continual improvement of the information security management.	Check if the ISMS Team was established and the respective roles and responsibilities assigned.					
			Check Compleye Online Leadership and Management section whether the ISMS competencies have been defined and assigned to ISMS team members.					
			Check Compleye Online Leadership and Management section whether the ISMS competencies were reviewed in the last 12 months.					
			Check Compleye Online Leadership and Management section or internal documentation whether the ISMS roles and responsibilities were reflected in the relevant job descriptions.					
	7.2 Competence	The organization shall: a)Determine the necessary competence of person(s) during work under its control that affects its information security performance b)Ensure that these person are competent on the basis of appropriate education, training or experience c)Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d)Retain appropriate documented information as evidence of competence	Is there an activity/control defined on Compleye Online board for checking competences on a regular basis?					
			Check if the selected competencies for each role are reflected in the job descriptions.					
			Check if the Security topics were addressed during the onboarding of new Team members.					
			Is Security Awareness Training an activity for all Team members? Is it documented in the HR policy or Workspace & Equipment Policy?					
			Check if the onboarding pack of new staff includes the information security policy.					
	7.3 Awareness	Persons doing work under the organization's control shall be aware of: a)The information security policy b)Their contribution to the effectiveness o the information security management system, including the benefits of improved information security performance, and c)The implications of not conforming with the information security management system requirements.	Check if the ISMS roles and responsibilities were documented in job descriptions.					
			Check if the disciplinary process has been put in place. This can be verified by checking a. if the employment contract includes the relevant disciplinary clauses b. if the security awareness training makes a reference to disciplinary process c. if the code of conduct policy or any similar policy was implemented and specifies the disciplinary process.					
	7.4 Communication	The organization shall determine the need for internal and external communications relevant to the information security management system including: a)On what to communicate b)When to communicate c)With whom to communicate d)Who shall communicate, and e)the processes by which communicate shall be effected.	Check if the Communication Policy was documented and approved by the CEO and the final approved PDF version saved in Compleye Online security policies and procedures section.					
	7. 5	General documentation						
	7.5.1 General	The organization's information security management system shall include: a)documented information required by this International Standard; and b)documented information determined by the organization as being necessary for the effectiveness of the information security management system.	Check if all ISO27001 Mandatory topics (Chapters 4 to 10) are covered in Compleye Online specifying how they are organized and implemented. For example, using Compleye's template ISO27001 Mandatory topics.					
		a. you need to document (meaning write down) how chap 4-10 is being implemented (or organized).	If labelling is in scope in the SoA, check that labels are available on documentation.					
		b. label all necessary documentation important for effectiveness of the ISMS with blue label.						
	7.5.2 Creating and Updating Documents	When creating and updating documented information the organization shall ensure appropriate: a)Identification and description (e.g. a title, date, author, or reference number) b)format (e.g. language, software version, graphics) and media (e.g paper, electronic); and c)review and approval for suitability and adequacy.	Check in Compleye Online Security Policies and Procedures whether the PDF final version of security policies and procedures were saved.					
			Select a sample of Security Policies and Procedure documents to check if the title , date and owner was adequately referenced.					

	7.5.3 Control of documented information.	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).For the control of documented information, the organization shall address the following activities, as applicable) distribution, access, retrieval and use;d) storage and preservation, including the preservation of legibility;e) control of changes (e.g. version control); andf) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled	Check if the filling directory process (other than Compleye Online) is documented to specify how policies and procedures are saved in a secure and protected manner.					
			Select a sample of Security Policies and Procedure document to check if the latest version of the document was approval by the owner					
			Check if there is a labeling policy (check data classification policy for this) and if this policy is implemented with labels on documentation. If controlled by access management policy - it is out of scope.					
			Check in the Information Security Communication Policy if and how the versioning of policies and communication is documented.					
8. Operation	8.1 Operations planning and control	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	Check if the security meeting occurred on a monthly basis.					
			Check if the improvements were addressed and actioned at the planned intervals.					
			Check if the security controls and measures are addressed and actioned at the planned intervals.					
	8.2 Information security risk assessment	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).The organization shall retain documented information of the results of the information security risk assessments.	Check in Compleye Online Measures and Controls section if an ISRA control has been included.					
			Check if the ISRA was performed and concluded.					
			Check if the ISRA was approved.					
			Check if the Improvements following the ISRA performance were approved and included in Compleye Online Improvement section.					
	8.3 Information security risk treatment	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	Check if the Improvement Procedure is in place.					
			Check if there is a treatment plan established for improvements.					
			Is evidence of the effectiveness of the treatment plan part of the improvement evaluation?					
9. Performance Evaluation	9.1 Monitoring, measurement, analysis and evaluation	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE The methods selected should produce comparable and reproducible results to be considered valid.c) when the monitoring and measuring shall be performed;d) who shall monitor and measure;e) when the results from monitoring and measurement shall be analyzed and evaluated; andf) who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement	Check if the security metrics were established together with the description and acceptable level defined.					
			Check if the security metrices were reviewed and documented on a regular basis.					
			Check if the security controls and measures are defined with the assigned owner and frequency of review.					
			Check if the security controls and measures are addressed and actioned at the planned intervals.					
			Check if the ISRA was performed and concluded.					
			Check if the Improvements following the ISRA performance were approved and included in the Improvement section.					
	9.2 Internal Audit	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to1) the organization's own requirements for its information security management system; and2) the requirements of this International Standard;b) is effectively implemented and maintained. The organization shall:c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;d) define the audit criteria and scope for each audit;e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;f) ensure that the results of the audits are reported to relevant management; andg) retain documented information as evidence of the audit	Check if the internal audit was conducted at planned intervals (annual basis).					
			Check if the last internal audit was performed by someone who is not part of the ISMS team and whose competence to perform the internal audit can be verified.					
			Check if the last Internal Audit considered the last audit results, if applicable.					
			Check if the Internal Audit report following the last internal audit conclusion was submitted to the Management and ISMS Team for review and approval.					
			Check if the meeting with Management and/or ISMS Team occurred following the last internal audit meeting to evaluate the results and define the improvements.					
	9.3 Management Review	Top Management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:a) the status of actions from previous management reviews) changes in external and internal issues that are relevant to the information security management systemics) feedback on the information security performance, including trends in:1) nonconformities and corrective actions;2) monitoring and measurement results;3) audit results; an4) fulfilment of information security objectives;d) feedback from interested parties;e) results of risk assessment and status of risk treatment plan; andf) opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of	Check if Management Review Document was issued.					
			Is the management review performed on time and not older than 1 year?					
			Check if the management decisions were defined and approved.					
			Check if the 13 compulsory topics of the management review report in Compleye Online have been covered.					
			Check that the improvements decided during the management review have been added to the Improvement section					
10 Improvement	10.1 Nonconformity and corrective actions	10.1 Nonconformity and corrective action When a nonconformity occurs, the organization shall:a) react to the nonconformity, and as applicable:1) take action to control and correct it; and2) deal with the consequences;b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:1) reviewing the nonconformity;2) determining the causes of the nonconformity; and3) determining if similar nonconformities exist, or could potentially occur;c) implement any action needed;d) review the effectiveness of any corrective action taken; ande) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:f) the nature of the nonconformities and any subsequent actions taken, andg) the results of any corrective action.	Check if you are able to find the origin of the improvement (e.g. specific assessment, audit or other wise)					
			Check if the root cause, if other areas might be affected and if treatment plan are in place for each improvement					
			Check if owners are assigned and if deadlines and progress are tracked					
			Check if evidence has been provided before the improvement is closed and if the results have been evaluated by an ISMS team member different from the owner of the improvement					
			check if the effectiveness of the result has been determined in the evaluation of the improvement					
			check if there is an incident procedure in place, with a CAPA procedure					
			check if there is a control in place that checks if the Preventive Actions are being monitored.					
	10.2 Continual Improvement	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Check if the security meetings occurred on a monthly basis and if the improvements were discussed and addressed.					

Disclaimer: this template provides guidelines on how to perform an Internal audit assessment. The criteria listed below are suggestions based on what evidence can be found in Compleye Online - you can add the link to specific section in Compleye Online. If you store evidence in other tooling you can refer to. It is possible for each organization to define new criteria adjusted to the organization's context and their own requirements as defined in their policies and procedures.

Results Internal Audit- Annex A

Chapter	Norm Description			Criteria	Links to evidence	Topics for investigation	Investigation Notes	Classification of Finding (after Investigation)	
								Non-conformity	Opportunity for improvement
A.5 Information security policies	A.5.1 Management direction for information security								
	A.5.1.1	Created / Reviewed and uploadee in section policies & procedures	Control A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Check if the Security Policy and supporting Security Procedures are defined and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					
				Check if the security policy and security procedures were provided to the Staff as part of Security Awareness Training.					
				Check if the Security Policy is provided to new staff as part of the onboarding process.					
				Check in information Security Communication Policy - if and how the security policy is made available to interested parties. (e.g. customers)					
	Improvements	Improvements created for each finding - section Improvements	Control The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Check if the security policy and security procedures were reviewed at the planned intervals and if the changes together with the approval are documented in the policy/procedure documents and/or in Compleye Online.					
A.6 Organization of information security	A.6.1 Internal organization								
	A.6.1.1	Information security roles and responsibilities	Control All information security responsibilities shall be defined and allocated.	Check if the ISMS team was established and their roles and responsibilities documented in the relevant jobs descriptions.					
	A.6.1.2	• If an Information Security Risk Assessment and/or external audit has been performed the year before, check in Compleye Online Internal Audit if all findings have been addressed and improvements have been closed.	Control Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Check if the ISMS assigned roles could pose potential conflict of interest.					
	A.6.1.3	Contact with authorities	Control Appropriate contacts with relevant authorities shall be maintained.	Check if the DPO/Privacy Officer job profile/description - as contact person for supervisory authorities is assigned.					
	A.6.1.4	Contact with special interest groups	Control Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Check if the special interest groups together with the contact details were listed in Compleye Online Legal or Strategy & Ambition sections.					
	A.6.1.5	Information security in project management	Control Information security shall be addressed in project management, regardless of the type of the project.	Check if the Information Security aspects are included in the project procedure.					
	A.6.2 Mobile devices and teleworking								
	A.6.2.1	Mobile device policy	Control A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Check if the security measures concerning Mobile device use are listed in the Workspace & Equipment					
				Check if the security measures concerning Mobile device were addressed during the last Security Awareness training.					
	A.6.2.2	Teleworking	Control A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Check if the security measures concerning remote working are listed in the Workspace & Equipment					
				Check if the security measures concerning remote working were addressed during the last Security Awareness training.					
				If the organization is a full remote working company, check if there is a specific policy establishing rules for remote working.					
A.7 Human resource security	A.7.1 Prior to employment								
	A.7.1.1	Screening	Control Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Check if the Team Member Off/On Boarding Procedures were established and documented.					
				Check if the employment screening is in place and if the process was documented.					
	A.7.1.2	Terms and conditions of employment	Control The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Check if the employment contract include the references to responsibilities for information security.					
	A.7.2 During employment								
	A.7.2.1	Management responsibilities.	Control Management shall require all employees and contractors to apply information security in	Check if the information security policies and relevant procedures are provided to new staff as part of the onboarding process.					

			accordance with the established policies and procedures of the organization.	Check if the information security policies and procedures are provided to participants as part of the security awareness training.					
	A.7.2.2	Information security awareness, education and training	Control All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Check if the information security policies procedures were addressed during the last security awareness training.					
	A.7.2.3	Disciplinary process	Control There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Check if the disciplinary process is in place. This should be referenced in the employment contract and/or Code of Conduct Policy/employee					
				Was the Code of Conduct Policy or employee handbook documented and PDF version of the approved document saved in Compleye Online Security Policies and Procedures section.					
				Check if the Security Awareness Training refers to the disciplinary process.					
				Check if the results of the security awareness					
	A.7.3 Termination and change of employment								
	A.7.3.1	Termination or change of employment respon-sibilities	Control Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Check if the employment contract makes a reference to the post termination clauses regarding the information securities related responsibilities.					
A.8 Asset management	A.8.1 Responsibility for assets								
	A.8.1.1	Inventory of assets	Control Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Check if devices and equipment used to process data are listed in Compleye Online asset register.					
	A.8.1.2	Ownership of assets	Control Assets maintained in the inventory shall be owned.	As per above check if the listed assets have the assigned owners.					
	A.8.1.3	Acceptable use of assets	Control Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Check if the rules of handling assets are defined in the Workspace & Equipment Policy.					
	A.8.1.4	Return of assets	Control All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Check if the Team Member On/Off Boarding Procedures specify the equipment handed over and returned. Check if the implementation of the On/Off Boarding Procedures is documented for each employee joining or leaving the company.					
	A.8.2 Information classification								
	A.8.2.1	Classification of information	Control Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Check if the Data Classification Procedure was documented and the final approved PDF version saved in the Security Policies and Procedures section.					
				Check in Compleye Online if data assets are classified in the Data Classification section.					
	A.8.2.2	Labelling of information	Control An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Check if there is a labeling policy and if this policy is implemented with labels on documentation. Check if labels are correctly implemented in the Data					
				Check if the Data Classification and Labelling topic is addressed in the Security Awareness training.					
	A.8.2.3	Handling of assets	Control Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Check if the rules of handling assets are defined in the Workspace & Equipment Policy.					
	A.8.3 Media handling								
	A.8.3.1	Management of removable media	Control Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	If applicable, Check if Workspace & Equipment Policy addresses the management of removable media.					
	A.8.3.2	Disposal of media	Control Media shall be disposed of securely when no longer required, using formal procedures.	If applicable, Check if Workspace & Equipment Policy addresses the disposal of removable media.					
	A.8.3.3	Physical media transfer	Control Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	If applicable, Check if Workspace & Equipment Policy addresses the management of physical media transfer.					
A.9 Access control	A.9.1 Business requirements of access control								
	A.9.1.1	Access control policy	Control An access control policy shall be established, documented and reviewed based on business and information security requirements.	Check if an Access Management Procedure was documented and the final PDF version was saved in Compleye Online Security Policies and Procedures					
				Check if the Access Management Procedure was reviewed in the last 12 months.					
				Check in Compleye Online if the list of applications and tools was listed and the access rights defined.					
				Check if the access overview was reviewed in line					

				Check if external parties have access to applicatiosn or tools and if this was documented in the Access Overview.					
	A.9.1.2	Access to networks and network services	Control Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Check if only the users who are listed in the Access Overview have access to the listed Tool/Application. This could be evidenced by requesting a sample of current access rights overview to a selected Tool/Application.					
				Check if there is a security control for control on access of tools and if being performed accordingly to described procedure					
	A.9.2 User access management								
	A.9.2.1	User registration and de-registration	Control A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Check if the Team Member On/Off Boarding Procedures specify the creation and removal of access rights. Check if the implementation of the On/Off Boarding Procedures is documented for each employee joining or leaving the company.					
				Check if if the Access Management Procedure was documented and the final and approved PDF version is listed in Compleye Online Security Policies and Procedures section.					
	A.9.2.2	User access provisioning	Control A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Check is the security control for Access of Tooling and Application is in place.					
	A.9.2.3	Management of privileged access rights	Control The allocation and use of privileged access rights shall be restricted and controlled.	Check in Compleye Online if admin access rights are assigned for each tool/application. This includes the overview of any privileged access rights, if applicable.					
	A.9.2.4	Management of secret authentication information of users	Control The allocation of secret authentication information shall be controlled through a formal management process.	Check in the access management policy if it is defined how secret authentication information is controlled during access process					
	A.9.2.5	Review of user access rights	Control Asset owners shall review users' access rights at regular intervals.	Check if the Team Members listed as not-active still have access to tools/applications as per Access Overview records.					
				Check if the user access rights were reviewed at planned intervals.					
	A.9.2.6	Removal or adjustment of access rights	Control The access rights of all employees and external party users to information and information	Check if there is a process of removing/adjusting					
				Check if removing access rights is part of the Off Boarding checklist/process.					
	A.9.3 User responsibilities								
	A.9.3.1	Use of secret authentication information	Control Users shall be required to follow the organization's practices in the use of secret authentication information.	Check the Workspace & Equipment Policy for rules to secure passwords.					
				Check in the security awareness training if the topic of user responsibility concerning secret authentication information was covered					
	A.9.4 System and application access control								
	A.9.4.1	Read	Control Access to information and application system functions shall be restricted in accordance with the access control policy.	Check if the principles of privacy by design are implemented in policies and/or controls: - Implement the "need-to-know" and "need-to-do" principles - Limit the collection of personal data to the minimum necessary for the identified purposes. - Ensure the accuracy and quality of personal data necessary for its processing - Ensure the de-Identification and deletion of personal data as soon as the original data is no longer necessary for the identified purpose(s). - Not retain personal data for longer than is necessary for the purposes for which the personal data is processed. - Document policies, procedures and/or mechanisms for the disposal of personal data. - Ensure the security of personal data transmission. - Provide the ability to return, transfer and/or dispose of personal data in a secure manner.					
	A.9.4.2	Secure log-on procedures	Control Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Check if procedures are documented for providing access in a secure way (e.g. encryption of passwords)					
	A.9.4.3	Password management system	Control Password management systems shall be interactive and shall ensure quality passwords.	Check if there is a password management system in place and controlled					
	A.9.4.4	Use of privileged utility programs	Control The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Check if Utility Programs are defined and if rules of use are set on these programs.					
	A.9.4.5	Access control to program source code	Control Access to program source code shall be restricted.	Check if all tooling used in SDLC is listed.					
				Check if access to this tooling is controlled.					
A.10 Cryptography	A.10.1 Cryptographic controls								
	A.10.1.1	Policy on the use of cryptographic controls	Control A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Check if the Cryptography Policy was documented and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					

	A.10.1.2	Key management	Control A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Check if Key management process is defined in the Cryptography Policy.					
				Check if the control for Key Management process was included in Compleye Online Security Controls and Measures section.					
				As per above, check if the control was concluded at planned intervals and the required evidence provided.					
A.11 Physical and environmental security	A.11.1 Secure areas								
	A.11.1.1	Physical security perimeter	Control Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Check if the policy for the secure areas was documented and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					
	A.11.1.2	Physical entry controls	Control Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Check if the policy for the secure areas establishes if the secure areas are locked and if there is a control on who has access.					
	A.11.1.3	Securing offices, rooms and facilities	Control Physical security for offices, rooms and facilities shall be designed and applied.	Check if there is a Physical security policy for offices					
	A.11.1.4	Protecting against external and environmental threats	Control Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Are controls in place for natural disasters, if applicable for secure areas?					
	A.11.1.5	Working in secure areas	Control Procedures for working in secure areas shall be designed and applied.	Are procedures or rules in place for working in secure areas? Are they documented?					
	A.11.1.6	Delivery and loading areas	Control Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	if loading areas are applicable, are there special rules around physical security for delivery services? Are they documented?					
	A.11.2 Equipment								
	A.11.2.1	Equipment siting and protection	Control Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Check if the access managment policy was documented and the final approved PDF version saved in Compleye Online Security Policies and Procedures section.					
	A.11.2.2	Supporting utilities	Control Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	If there are supporting utilities, eg. servers on office site, check if there are controls in place in case of power failure.					
	A.11.2.3	Cabling security	Control Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	E.g. for office networks and servers, are there measures in place to protect them from interception or damage?					
	A.11.2.4	Equipment maintenance	Control Equipment shall be correctly maintained to ensure its continued availability and integrity.	Is there a maintenance program in place for all hardware assets?					
	A.11.2.5	Removal of assets	Control Equipment, information or software shall not be taken off-site without prior authorization.	Is there a procedure in place for removal of hardware? Is the implementation of the procedure documented (certificate for example)?					
	A.11.2.6	Security of equipment and assets off-premises	Control Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Check if the Workspace & Equipment Policy makes a reference to the use of equipment off site.					
				Check if the Security Awareness Training referred to the use of equipment offsite.					
	A.11.2.7	Secure disposal or reuse of equipment	Control All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Check if the Workspace & Equipment Policy makes a reference to the disposal of unused equipment.					
				Check if the Security Awareness Training referred to the to the disposal of unused equipment.					
	A.11.2.8	Unattended user equipment	Control Users shall ensure that unattended equipment has appropriate protection.	Check if the Workspace & Equipment Policy makes a reference to unattended					
				Check if the Security Awareness Training referred to the unattended laptops/workstations/devices.					
	A.11.2.9	Clear desk and clear screen policy	Control A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Check if the Workspace & Equipment Policy makes					
				Check if the Security Awareness Training referred to the Clear desk and clear screen rules.					
A.12 Operations security	A.12.1 Operational procedures and responsibilities								
	A.12.1.1	Documented operating procedures	Control Operating procedures shall be documented and made available to all users who need them.	Check if procedures for operating information processing and communications (installation and configuration of systems, backup, equipment maintenance, media handling, recovery procedures, management of logs, monitoring procedures, etc.) are documented and approved PDF versions saved in Compleye Online Security Policies and Procedures.					
				Is there a procedure in place to monitor the system and is the team trained for it?					

A.12.1.2	Change management	Control Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Check if the Change Management Procedure was documented and the final and approved PDF versions saved in Compleye Online Security Policies					
			Check in Compleye Online Controls section and/or Security Meetings whether the controls for such changes are in place.					
			Check if in the change management procedure covers the following topics: changes to SW Code, Suppliers, Team Members, ISMS Team Members, Access of Tooling.					
			Check if the SDLC covers change management in the development process and if the implementation of the process is documented.					
A.12.1.3	Capacity	Control	Check if there are rules documented on data server					
A.12.1.4	Separation of development, testing and operational environments	Control Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Check in Compleye Online X-Ray Component Cloud Environment and/or SDLC if there is a separation of development, testing and production environment in place.					
A.12.2 Protection from malware								
A.12.2.1	Controls against malware	Control Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Check if the threat Malware is part of the annual ISRA assessment.					
			Check if the ISO27002 controls are documented in the ISRA assessment.					
			Check the Workspace & Equipment Policy if the controls to avoid malware on Laptops are in place.					
			Check if there is a Malware tool in place that detects malware on the server.					
			Check if the Malware topic is covered during Security Awareness Training.					
			Check if Team members are assessed on Malware attempts (e.g. Phishing) or at least informed about such attempts.					
A.12.3 Backup								
A.12.3.1	Information backup	Control Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Check Compleye Online Cloud Server component and/or Data Backup Plan whether there is a backup plan in place for data servers.					
			Check if there is in Compleye Online Contracts Overview section information related to service description, SLA with customer and whether there are contractual agreements on data backup plans.					
			Check if there is a list of Vendor Assessments. If so and if additional arrangements have been made with customers concerning Data Backup Plans, check if they are covered with a security control.					
			Check if there is a database restore/recovery plan in place that covers the Policy and/or contractual agreements.					
			Check if the database restore/recovery test have been performed as defined.					
			Check if the Backup Procedure was documented and the final and approved PDF version was saved in the Security Policies and Procedures Rules.					
A.12.4 Logging and monitoring								
A.12.4.1	Event logging	Control Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Check if the process for monitoring and storing log was documented and the final and approved PDF version was saved in the Security Policies and					
			Check if the events logs are analyzed on a regular basis and if this is documented.					
A.12.4.2	Protection of log information	Control Logging facilities and log information shall be protected against tampering and unauthorized access.	Check if the process specifies how log information is protected from tampering and unauthorized access.					
A.12.4.3	Administrator and operator logs	Control System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Check in the SW Access Overview if the system administrators are assigned.					
			Check if the System Administrators use admin@ account names.					
A.12.4.4	Clock synchronization	Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a	Check in Compleye Online if the Clock synchronization is organized between different					
			If the Clock Synchronization is outsourced check if the evidence to prove this was provided.					
A.12.5 Control of operational software								
A.12.5.1	Installation of software on operational systems	Control Procedures shall be implemented to control the installation of software on operational systems.	Check if there are specific rules documented for installing software on Operating Systems (e.g. your own product BackEnd)					
A.12.6 Technical vulnerability management								
A.12.6.1	Management of technical vulnerabilities	Control Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Check if technical vulnerabilities scanning is performed at the planned intervals.					
			Check if the security metrics were established and monitor the technical related incidents.					
			Check if the technical vulnerabilities are considered in ISRA.					
			Check if the PEN Testing was performed at the planned intervals and the findings addressed.					
A.12.6.2	Restrictions on software installation	Control Rules governing the installation of software by users shall be established and implemented.	Check if these rules on software installation restrictions are addressed in Workspace &					
			Check if the rules on software installation restrictions were addressed in the Security Awareness Training.					

				Are there rules on software tools to be used on the hardware? Are they documented?					
	A.12.7 Information systems audit considerations								
	A.12.7.1	Information systems audit controls	Control Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Check if the person responsible for operations is also involved in test or audit plans making sure there is no disruption in normal operations.					
A.13 Communications security	A.13.1 Network security management								
	A.13.1.1	Network controls	Control Networks shall be managed and controlled to protect information in systems and	Are there controls in place to secure office network?					
				If outsourced, are there agreements on how that is organized?					
	A.13.1.2	Security of network services	Control Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Do you have a policy around your own network? If outsourced is there a SLA in place?					
	A.13.1.3	Segregation in networks	Control Groups of information services, users and information systems shall be segregated on networks.	Did you address the segragation of network in the SLA (or did you organized it self)? E.g. the separation of critical networks from the Internet and other internal, less sensitive networks.					
	A.13.2 Information transfer								
	A.13.2.1	Information transfer policies and procedures	Control Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Check if the Communication Policy was documented and the transfer of information documented in the Communication Policy.					
	A.13.2.2	Agreements on information transfer	Control Agreements shall address the secure transfer of business information between the organization and external parties.	Check if the contract with the key external parties address the secure transfer of information (e.g. DPAs in place and/or Data transfer agreements).					
	A.13.2.3	Electronic messaging	Control Information involved in electronic messaging shall be appropriately protected.	Check if the messaging system is protected against spam/viruses/phishing, if message encryption, IP address monitoring and email blocking are implemented.					
				Check if the data in transit is encrypted, this should be specified in the Cryptography procedure.					
	A.13.2.4	Confidentiality or nondisclosure agreements	Control Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Check if Non-Disclosure Agreements are in place and used with third parties.					
				Check if confidentiality clauses are included in the employment/ contractor contracts and terms and conditions/agreements executed with clients/customers.					
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems								
	A.14.1.1	Information security requirements analysis and specification	Control The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Check if the security assessment was performed on all of the suppliers.					
				Check that if the organization develops/buys a new tool, security related requirements are taken into consideration. Check if this is documented.					
	A.14.1.2	Securing application services on public networks	Control Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Check if the security measures applied on public networks were documented.					
	A.14.1.3	Protecting application services transactions	Control Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Check if the encryption methods were applied and specified in the Cryptography Procedure					
	A.14.2 Security in development and support processes								
	A.14.2.1	Secure development policy	Control Rules for the development of software and systems shall be established and applied to developments within the organization.	Check if the SDLC was documented and saved in Compleye Online SLDC Documentation.					
	A.14.2.2	System change control procedures	Control Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Is there a change management process in place in the SDLC?					
	A.14.2.3	Technical review of applications after operating platform changes	Control When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Is there a test plan in place for deployment? And are security issues part of that testplan? Is that documented?					
	A.14.2.4	Restrictions on changes to software packages	Control Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Check if software packages (multiple applications or code modules that work together to meet various goals and objectives) are applicable to your product or supporting tooling. If so, check if this was addressed in your SDLC.					
	A.14.2.5	Secure system engineering principles	Control Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Check if your SDLC covers security, security issues definition, checking security during writing requirements and testplan (technical requirements: check if there is a potential security impact/issue).					

	A.14.2.6	Secure development environment	Control Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	How is your development environment secured? Did you document that in the SDLC? Is the whole SDLC part of that secured environment?					
	A.14.2.7	Outsourced development	Control The organization shall supervise and monitor the activity of outsourced system development.	Check if the outsourcing rules are documented and the final approved version saved in Compleye Online Security Policies and Procedures list.					
				Check if the outsourcing rules specify the data the outsourcing party has access to (manual check).					
				Check if the outsourcing party is profiled as high risk on information security and business continuity and if there is an additional assessment					
	A.14.2.8	System security	Control	Check if security is part of Test Protocol?					
	A.14.2.9	System acceptance testing	Control Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Is acceptance testing part of SDLC?					
	A.14.3 Test data								
	A.14.3.1		Control Test data shall be selected carefully, protected and controlled.	Check if protection of test data rules were addressed and documented in the SLDC document or any other procedural document. Check what kind data are used for test data.					
A.15 Supplier relationships	A.15.1 Information security in supplier relationships								
	A.15.1.1	Information security policy for supplier relationships	Control Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Check if a Supplier management procedure was implemented and the final approved version saved in Compleye Online Security Policies and Procedures section.					
				Check if the supplier overview is filled in and has been updated less than a year ago					
				In Additional supplier assessment, check if all fields are filled and that residual risk is approved					
				Check if all tools listed in the Software overview are also listed in the supplier overview (manual check for now, suggestion on the roadmap)					
				Check that all suppliers have been assessed on information security and business continuity risks					
				Check that all suppliers have an owner (suggestion on the roadmap)					
	A.15.1.2	Addressing security within supplier agreements	Control All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	If the field "Access to restricted data" is checked for a supplier, this supplier should be profiled as high risk for information security risks					
				Check if suppliers for which the field "Stakeholder in access management overview" is checked, are profiled as high risk for information security risks					
				Check if the additional assessment for High/Medium Risk profiled suppliers was performed on all fields					
	A.15.1.3	Information and communication technology supply chain	Control Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Check if the additional assessment for High/Medium Risk profiled suppliers was reviewed and approved					
				Check if the additional assessment for High/Medium					
				Check if improvements resulting from the additional assessment are included in the improvement section					
				For High/Medium Risk profiled suppliers, check if compliance tab is filled in (manual check)					
	A.15.2 Supplier service delivery management								
	A.15.2.1	Monitoring and review of supplier services	Control Organizations shall regularly monitor, review and audit supplier service delivery.	Check in the Access Management Procedures/Overview if suppliers have access to data and if they do check if controls are arranged (check assessment).					
				Check in the Supplier overview if suppliers have access to restricted data. If so verify if the DPA is in place.					
	A.15.2.2	Managing changes to supplier services	Control Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks	Check if the changes to Supplier overview is being assessed during the monthly security meeting.					
				Check if suppliers are being assessed on an annual basis.					
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements								
	A.16.1.1	Responsibilities and procedures	Control Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Check if the incident procedure was documented and the final approved PDF version saved in the Security Policies and Procedures section.					
	A.16.1.2	Reporting information security events	Control Information security events shall be reported through appropriate management channels as quickly as possible.	Check if the ISMS team is established and the roles assigned and the escalation process is established in the incident/breach procedure.					
	A.16.1.3	Reporting information security weaknesses	Control Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Check if the subject of incident management was addressed during the Security Awareness Training.					

	A.16.1.4	Assessment of and decision on information security events	Control Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Check if incidents are reported and monitored in the Security Metrics.					
				Check if the reported incidents were adequately classified.					
	A.16.1.5	Response to information security incidents	Control Information security incidents shall be responded to in accordance with the documented procedures.	Check if the incident/breach procedural steps were followed and the evidenced documented.					
	A.16.1.6	Learning from information security incidents	Control Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Check if the improvements are created following the incident.					
	A.16.1.7	Collection of evidence	Control The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Check if the security incident/breach reports are					
				Check if every procedural step for Incident procedures was evidenced and adequately documented.					
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity								
	A.17.1.1	Planning information security continuity	Control The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Check if the BCP assessment was performed and documented.					
				Check if the BCP assessment addressed the information security management planning.					
				As per above, check if the BCP assessment was performed in the last 12 months.					
	A.17.1.2	Implementing information security continuity	Control The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Check if the DRP assessment was performed and documented.					
				As per above, check if the DRP assessment was performed in the last 12 months.					
	A.17.1.3	Verify, review and evaluate information security continuity	Control The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Check if the security continuity related security controls were established at the planned intervals. This includes Data/ Code Restore, Backups, Pen					
				As per above, check if the controls were concluded at the planned intervals and the required evidence provided.					
	A.17.2 Redundancies								
	A.17.2.1	Availability of information processing facilities	Control Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Check if there is a DRP Plan in place or if the BCP assessment is performed on an annual basis or at planned intervals.					
				Check if the improvements created following the BCP or DRP assessment were concluded at the planned intervals and the required evidence documented.					
				Check if contracts and SLAs with customers are aligned with the content of your BCP/DRP and other policies where applicable (sample check).					
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements								
	A.18.1.1	Identification of applicable legislation and contractual requirements	Control All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Check in the Interested Parties & Legal Requirements if the applicable regulatory and legislative framework was defined and documented.					
	A.18.1.2	Intellectual property rights	Control Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Check if the Intellectual Property scope and purpose was defined in the Intellectual Property section in Compleye Online Legal section.					
				Check if the contract with service providers that participate in the IP creation includes the relevant IP protective clauses.					
				Check if they have a IP statement.					
				Check if the contract with employees/contractors that participate in the IP creation includes the relevant IP protective clauses.					
				As per above, the employee/contractors contract should be received and attached as an evidence.					
				Check if NDA with relevant third parties are saved as evidence in the Legal or Supplier sections.					
	A.18.1.3	Protection of records	Control Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	Check in Compleye Online Interested parties and legal requirements section if the ISMS reference field is filled in to evidence how the requirements are addressed in the organization's ISMS.					
	A.18.1.4	Privacy and protection of personally identifiable information	Control Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Check if the GDPR assessment was concluded in the last twelve months.					
				Check if the improvements following the GDPR assessment were created in the Improvement section.					
				Check if the findings were implemented					
				Check if GDPR Legal basis and User documentation subsections are filled in					
				If the organization has customers in several countries, check if section global impact is used to list additional requirements.					

				Check if all countries of operations are listed and if the section was reviewed less than a year ago.					
				Check if a DPIA was performed and concluded and the required evidence documented.					
	A.18.1.5	Regulation of cryptographic controls	Control Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Check if the Cryptographic Procedure was documented and if the final and approved PDF version was saved in the Security Policies and					
				If applicable, check if the Cyptographic Procedure makes a reference to any specifc rules and regulations.					
				Check if the Cryptographic related controls are established in the Security Control and Measures section together with the assigned owners and planned review intervals.					
	A.18.2 Information security reviews								
	A.18.2.1	Independent review of information security	Control The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Check if the internal audit was performed and concluded at planed intervals.					
				Check if the improvements /non conformities identified following the internal audit were addressed and the required evidence provided and attached					
				Check if all Policies & Procedures are reviewed on planned intervals (check the review and approvals in Compleye Online)					
				Check if all controls are conducted on planned intervals. (check the overdue controls in Compleye Online)					
	A.18.2.2	Compliance with security policies and standards	Control Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Check if regular Security Meetings have been taking place to review the Security Metrics on interval					
				Check if all other topics (and changes) have been subject to security meetings.					
	A.18.2.3	Technical compliance review	Control Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Check if the annual assessment of all of the security policies and procedures was assessed and concluded.					
				Check if the PEN Testing was performed at the planned intervals (at least annually) and if the improvements defined were actioned and addressed.					
				Check if the scanning of technical vulnerabilities is performed and if the vulnerabilities defined were actioned and addressed.					