ICT Vendor Management Policy

1 INTRO

This policy covers the RiskPoint Group on global basis. It outlines the strategy for handling relationships with ICT vendors and with a focus on those supplying Core Applications which are critical to the performance of the RiskPoint Group.

An ICT Vendor is one who provides ICT Services which includes:

- digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis
- hardware as a service and hardware services which includes the provision of technical support via software or firmware updates

A business impact analysis is used in evaluating the business criticality of all third party vendors and their services to determine the risk inherent to it, and whether it should be considered a core applications.

As part of this policy, the RiskPoint Group has established an ICT Vendor Register of Information[1]. It is maintained by IT Compliance, reviewed annually and continuously updated as contracts are entered into and exited from.

A key feature of healthy vendor management is the avoidance of conflicts of interests. As such, the RiskPoint Group has enacted a comprehensive Conflicts of Interest Policy that guides the topic. The principles in that policy guides every aspect of ICT Vendor management.

Nothing in this policy is meant to relieve the RiskPoint Group or its management group from regulatory obligations or responsibilities to its clients. Similarly, nothing is meant to prevent the effective supervision or contravene any supervisory activities.

2 CONTRACTUAL CLAUSES

All ICT Contracts entered into by the RiskPoint Group must be set out in writing. And shall include elements as outlined in this section.

Specifically, all ICT contracts must include provisions covering the following:

- Description of the service being provided
- Location of where the service is to be provided, where any data is stored, and that a notice must be sent in case of these being changed
- Data Protection provision, including the return/recovery of data in case of vendor facing insolvency
- Service level provisions outlining the estimated up and downtime of the service
- The providing of assistance in cases of ICT incidents related to the service
- An obligation for the vendor to fully corporate with applicable authorities
- Termination rights including notice periods

For Core Applications, the following elements must be included in the contract:

- Notice periods for any development that might have an impact on the vendor's ability to perform under the contact
- Requirements for the vendor to implement and test contingency plans, and have in place ICT security measures
- And obligation to participate in the RiskPoint Group's Threat Led Penetration Test as applicable

[1] Exact form and content of Register of Information has not yet been determined by the authorities. It is expected that this will be done in the first half of 2025. Following this, these must be completed and uploaded to the authorities on a regular basis.

- A right for the RiskPoint Group to monitor the performance of the vendor

In addition, all ICT contracts must specify whether the vendor is audited or certified, and grant the RiskPoint Group access to these items, as applicable.

3 CONTRACT LIFE CYCLE

This section outlines the contract life cycle, including approval, monitoring, and exit plans.

Prior to any engagement with a ICT vendor, a requester of the engagement must determine that there is a business need for the engagement.

3.1 ICT Vendor Risk Assessment and Due Diligence Process

As the first step in the contract life cycle, IT Compliance performs an ICT Vendor Risk Assessment, including determining whether to much ICT risk has been concentrated at the same vendor. At the same time, due diligence is performed to make sure the applicable vendor can fulfil certain objective requirements of the contractual relationship.

Based on the ICT Vendor Risk Assessment IT Management approves the contract. An overview of approved ICT contracts and applicable ICT Vendor Risk Assessments are presented to the Security Board. Once the applicable contract is signed, the engagement is added to the ICT Vendor Register of Information.

ICT Vendor Risk Assessment and Due Diligence worksheet template is attached as Appendix 1, and is adjusted on an ad-hoc basis to account for the specifics of the engagement.

3.2 Monitoring

All ICT contractual relationships are monitored as to whether they live up to the contractual provisions agreed upon. This includes contractual provisions such as those outlining confidentiality, availability of service, and integrity of data as applicable. In cases where the third party vendor does not live up to the provisions, the RiskPoint Group will evaluate on an ad-hoc basis the repercussions this will have on the relationship.

For core applications, contractual provisions must outline that the RiskPoint Group receive appropriate reports on activities and services or that same is made available. This could include, but is not limited to, the following: incident reports, ICT security reports, performance reports, audit results. The received information will be used in the ICT Vendor Register of Information.

Any shortcomings found based on the monitoring will result in consequences decided on an ad-hoc basis.

3.3 Exit Plans

Based on the parameters below and tracked in the ICT Vendor Register of Information, the RiskPoint Group will continuously evaluate all entered into ICT contracts with core vendors as to whether they should be exited from, and how they could be replaced. The purpose is to have a failsafe in place and not be overly reliant on the stability of a single vendor for the digital resilience of the RiskPoint Group.

Parameters include persistent service interruptions, failed service delivery, deterioration of quality, breach of contract clauses, and the unexpected termination of the contract.

As part of the annual ICT Vendor Register of Information review, the exit plans are reviewed.

riskpoint
rp underwriting

Appendix 1 - Template

ICT Vendor Risk Assessment and Due Diligence Worksheet

Date:
Author:

ICT VENDOR RISK ASSESSMENT
This risk assessment considers risks posed by the provision of ICT services. Specifically, the below items are evaluated for each ICT vendor relationship prior to entering it.

Type of risk	Evaluation of risk
Operational	
Legal	
ICT	
Reputational	
Personal data	
Data availability	
Data storage location	
Service provider location	
ICT risk-concentration	
Internal Contract Owner	

ICT DUE DILIGENCE ASSESSMENT
In order to have objective measures for each prospective vendor, the below questions must be answered yes/no prior to the entering into a relationship. Similarly, it must be determined which objective element has been used to further evaluate the vendor engagement.

Does the prospective service provider:	Yes/No
Have the necessary reputation, ability, expertise, and financial, human and technical resources, information security standards to provide the ICT service?	
Have the ability to monitor relevant technological developments on ICT security?	
Use subcontractors?	
Located within the European Union?	
Which country?	
Consents to auditing (including by third parties)?	
Acts in an ethical and socially responsible manner, respects human rights and children's rights	

Which of the following elements have been used to determine the required level of assurance that the third-party provider lives up to the due diligence requirements?

Element	Yes/No
External audits or independent assessments by vendor	
Internal Audits or independent assessments by vendor	
Audits or independent assessments by the RiskPoint Group	
Appropriate third-party certifications	
Other relevant information available to the RiskPoint Group – potentially provided by the vendor	

riskpoint
rp underwriting