



THIRD PARTY RISK MANAGEMENT POLICY

This Document is version controlled, all amendments to be tracked in the table below:
For Internal Use Only

Version	Author(s)	Date
1.0	CIC Plc- Group Risk & Compliance Department	November 2022
2.0	CIC Plc- Group Risk & Compliance Department	May 2025

Content

Definition of Terms	ii
1 INTRODUCTION	1
1.1 Overview	1
1.2 Purpose	1
1.3 Scope and Applicability	1
2 THIRD PARTY RISK UNIVERSE	2
3 ROLES AND RESPONSIBILITIES	3
3.1 First Line of Defense - Business Owners	3
3.2 Second line of defense	3
3.3 Risk and Compliance	3
3.4 Procurement	4
3.5 Legal Function	4
3.6 Third Line of Defense - Internal Audit.	4
4 RISK ASSESSMENT	5
4.1 Risk Rating Framework	5
4.1.1 High Risk	5
4.1.2 Medium Risk	5
4.1.3 Low Risk	5
4.2 Third Party Due Diligence	5
5 OVERSIGHT AND PERFORMANCE MONITORING	7
6 REVIEW AND APPROVAL OF THE POLICY	8
6.1 Review of the Policy	8
6.2 Approvals	8

Definition of Terms

Third Party

For the purposes of this policy, a “third party” includes any entity or natural person not under the direct business control of Centum with whom Centum engages in a business relationship, including any vendor, supplier, support provider, fulfilment provider, agent, consultant, advisor, contractor, business, marketing or strategic partner, joint venture, associate, and correspondent.

Third parties do not include Centum employees, or its clients and customers that have not entered into any business relationship with Centum beyond their direct engagement.

Third parties include any entity or natural person covered by one of the following descriptions:

1. Provides systems, information, products, services, and professional services for the performance of specified functions or activities (e.g., vendors including business process outsourcing, technology providers, consultants, and law firms);
2. Provides products or services offered directly to Centum’s clients or supports the delivery of products or services to Centum’s clients (e.g., service providers including claims management, call centers, insurance monitoring and other outsourced contractors);
3. Actively provides customer lead or referral information to Centum (e.g., referral partners)
4. Suppliers such as brokers, appraisers, underwriters, and agencies.

Business Relationship Owner: Member of staff responsible for maintaining a positive relationship with third parties and ensuring that the third parties can meet the needs of the business.

Due Diligence: An examination or review performed to confirm facts or details of a matter under consideration before entering into a proposed transaction with another party.

Service Level Agreements: A service-level agreement (SLA) defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties should service levels not be achieved.

1 INTRODUCTION

1.1 Overview

Centum recognizes the aim of third part risk management is not to eliminate risk, but rather to provide structural means to allow Centum to identify, prioritize, manage, mitigate, or respond to the risks inherent in third part activities, while protecting the integrity of Centum's brand and reputation.

Centum relies on third party relationships to:

1. Perform services and provide products on its behalf; and
2. Provide services and products that Centum does not have the internal capacity.

Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, such as disruptions, delays, or other events causing a denigration of transaction processing, customer service, information security, physical security, and data privacy.

1.2 Purpose

This policy sets forth standards regarding Centum's engagement with third parties and is designed to provide a framework for Centum to identify, measure, monitor, and report third party risks.

This policy is intended to be implemented under a phased approach, to provide for the requirements to be appropriately and effectively operationalized. In addition, due to the nature of certain contractual agreements and business relationships, existing relationships with third parties may be addressed on a renewal or other forward-looking bases.

1.3 Scope and Applicability

This policy applies to all Centum staff with key stakeholders being:

1. The Business Owners;
2. The Risk and Compliance, which define specific risk policies in their area of responsibility; and,
3. The Procurement function, which partners with Business Owners to ensure that the source-to-contract process complies with the requirements of this policy.

2 THIRD PARTY RISK UNIVERSE

There are several third-party risk categories, which are typically spread across the company from an accountability perspective. Some may reside within the procurement function, while others may sit within risk management, the wider business or at times have no home at all and slip between the cracks.

The table below represent risks that are considered within Centum as part of our end-to-end third-party lifecycle review:

Risk Category	Risk examples
Regulatory/compliance Risk	<ul style="list-style-type: none"> ▪ Regulatory requirements ▪ Theft/crime/dispute risk ▪ Fraud, anti-bribery, and corruption/scandals ▪ Compliance with internal procedures and standards
Strategic Risk	<ul style="list-style-type: none"> ▪ Service delivery risk ▪ Expansion/roll-out risk ▪ Mergers and acquisitions ▪ Alignment to outsourcing strategy ▪ Intellectual property risk
Concentration Risk	<ul style="list-style-type: none"> ▪ Supplier concentration across critical services ▪ Industry concentration (including subcontractor) ▪ Concentration of critical skills (i.e., technology support) ▪ Geographic concentration ▪ Reverse concentration
Technology/Cyber Risk	<ul style="list-style-type: none"> ▪ Information security ▪ Cyber Security ▪ Data privacy/data protection
Country Risk	<ul style="list-style-type: none"> ▪ Geopolitical risk ▪ Climate sustainability
Financial Viability	<ul style="list-style-type: none"> ▪ Liquidity risk
Operational/supply chain Risk	<ul style="list-style-type: none"> ▪ Business continuity ▪ Disaster recovery ▪ Physical security ▪ Operational resilience ▪ Performance management ▪ Human resource risk
Reputational Risk	<ul style="list-style-type: none"> ▪ Negative news ▪ Lawsuits (past and pending) ▪ Third party brand/reputation ▪ Key principals/owners of the third party ▪ Workplace safety
Legal risk	<ul style="list-style-type: none"> ▪ Jurisdiction of law ▪ Terms and conditions of the contract

3 ROLES AND RESPONSIBILITIES

Centum's Risk and Compliance function is the ultimate owner of this policy and is the governing body for overall risk activities for Centum including third party risk management. The Risk and Compliance function is responsible for:

1. Conveying Centum's risk to the Board;
2. Providing oversight of Centum's management of operational risk, such as risks associated with doing business with third parties;
3. Understanding the risks associated with third party arrangements and monitoring risk management practices
4. Reviewing the Third-Party Risk Management Policy

3.1 First Line of Defense - Business Owners

Centum's business units using third parties are responsible for managing all aspects of the relationships. The head of the business unit is responsible for designating the Business Owner (BO) for each third-party relationship.

The BOs will have primary responsibility for managing third party relationships and represent the first line of defense for ensuring compliance with this policy including:

1. Comprehensive understanding of the product and/or services being provided by third parties including risks and impacts to Centum's operations
2. Monitoring and reporting events that may have a material impact on the third party's ability to perform, such as regulatory compliance issues; data security incidents; changes in business continuity capabilities; and deterioration in financial condition; and Service Level Agreements (SLA) performance against defined metrics and contractual obligations.
3. Liaising with Risk and Compliance function to escalate significant incidents, issues, and matters e.g., third parties experiencing data security incidents, severe financial deterioration, or operational disruptions.

3.2 Second line of defense

Centum's Risk and Compliance Function is the Second Line of Defense and will work closely with the First Line of Defense with functional expertise needed to ensure risks associated with third parties are managed to an acceptable risk level. The Risk and Compliance function will be supported by other functions such as legal, procurement, information security, finance, and others.

3.3 Risk and Compliance

The Risk and Compliance Function will provide Third Party Risk Management Policy direction and coordination across Centum, such as:

1. Overseeing design, implementation, execution, and effectiveness of this policy and recommending approval of the policy and subsequent revisions;
2. Establishing a consistent metric-driven inherent risk ranking criteria;
3. Developing a schedule for risk assessments and periodic re-assessments;
4. Tracking and monitoring exceptions and provide periodic reports as required;
5. Investigating identified and reported violations.

3.4 Procurement

Centum's procurement function's responsibilities include:

1. Establishing regular reporting, including maintaining a list of active third-party relationships and relevant performance and compliance metrics;
2. Understanding under the direction of the Legal Function, the types of third parties who need contracts and those who don't;
3. Working with the Business Owners and the Legal Function during contract negotiation process to ensure relevant risks are adequately addressed in each contract and third-party agreement.

3.5 Legal Function

Legal function responsibilities may include ensuring contracts clearly states the duties, obligations, contingencies, and responsibilities of third parties and the obligation to maintain adequate internal controls, such as:

1. Setting measurable Service Level Agreements performance metrics that define the expectations and responsibilities for both parties including conformance with regulatory standards;
2. Responsibilities for providing, receiving, retaining and disposal of information;
3. The right to audit and require remediation;
4. Ownership and license;
5. Third party code of ethics, integrity, and confidentiality;
6. Business resumption and contingency plans;
7. Third party's right to use a subcontractor and right to notification.

3.6 Third Line of Defense - Internal Audit.

The Internal Audit team will provide reasonable assurance over the compliance status of Centum with this policy.

4 RISK ASSESSMENT

4.1 Risk Rating Framework

A risk rating criterion shall be applied to each third-party relationship based on the criticality of the products/services provided and the manner in which they are provided. The risk rating shall be used to determine the scope and depth of the due diligence performed, contractual terms and conditions, scope, depth, and frequency of monitoring the relationship, and the transition process for off-boarding.

The scope of the third-party risk assessment should be scaled based upon the criticality, complexity and risk of business functions or services.

4.1.1 High Risk

The following third-party relationships will be classified under this category:

1. Any third party, that while providing its products or services to Centum, regularly has access to confidential information, or data which depicts or is reasonably understood to represent Centum's competitive advantage;
2. Any third party whose services are deemed unique or critical to Centum's business or where there is a limited pool of qualified third parties to select from.

4.1.2 Medium Risk

Any third party with access to Centum's proprietary information or any other internal information will be classified under this category.

4.1.3 Low Risk

The following third-party relationships will be classified under this category:

1. Third parties without access to confidential information, proprietary or other sensitive information will be classified as low risk;
2. Any third party that only have access to publicly available information;
3. Any third party that performs services that do not materially affect Centum's operations.

4.2 Third Party Due Diligence

Due diligence should be conducted on all potential third parties before selecting and entering into contracts or relationships. Centum acknowledges that prior experience and/or knowledge of the third party is not an acceptable proxy for due diligence.

A standardized risk assessment questionnaire will be used to assess the criticality and/or sensitivity of services provided by the third party. The results of the risk assessment questionnaire should dictate the level of due diligence required.

The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. Enhanced due diligence shall be performed when a third-party relationship involves critical activities; with the option of on-site visits conducted to fully understand the third party's operations, capacity and understand and assess risk. If information is uncovered that warrants additional scrutiny the scope or assessment methods of the due diligence shall be expanded appropriately.

The following factors shall be considered as part of due diligence processes at minimum:

1. Overall financial condition and viability;
2. Compliance with legal, regulatory, and industry requirements;

3. Adequacy of internal controls including privacy, information, and physical security controls;
4. Ability to comply with service level performance commitments;
5. Adequacy of the third party's business continuity planning and capabilities;
6. Adequacy of the third party's governance program over their subcontractors.

5 OVERSIGHT AND PERFORMANCE MONITORING

The objective of the oversight and performance monitoring requirements is to identify actual risks, emerging risks, and deterioration in performance early to facilitate timely corrective action.

The Business Relationship Owner (BRO) should keep senior management apprised of the overall health of the third-party relationships and flag and escalate significant issues or concerns identified during monitoring.

Third parties' risk are subject to a periodic risk assessment if the nature of the business relationship and/or criticality of services provided materially changes. The purpose of the assessment is to determine any changes to the supplied services that may result in the risk rating change, which may in turn require revisions to the monitoring and assessment scope and frequency and contractual terms and conditions.

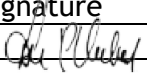
6 REVIEW AND APPROVAL OF THE POLICY

6.1 Review of the Policy

Risk and Management Function is responsible for reviewing and updating the policy annually to ensure that it is aligned to business and regulations changes. However, earlier revisions will be done in the event of any material changes in the operating environment of the business.

6.2 Approvals

This document is approved for use by:

Designation	Signature	Date
Board Chairman		11 July 2025