MITRATECH
Prevalent

A Complete Checklist for Compliance

ISO Third-Party Compliance Checklist

Table of Contents

ISO and Third-Party Risk Management 3

ISO 27001 and ISO 27002 3

ISO 27036-2 4

Mapping Mitratech Capabilities to ISO Standards 4

Table 1. Mitratech Mappings to ISO 27001 Security Standards 4

Table 2. Mitratech Mappings to ISO 27002 Security Standards for Supplier Relationships 10

Table 3. Mitratech Mappings to ISO 27036-2 Security Standards 19

The Mitratech Difference 24

About Mitratech 24

ISO and Third-Party Risk Management

The **International Organization for Standardization (ISO)** and the **International Electrotechnical Commission (IEC)** assemble experts from 165 countries to share knowledge and develop voluntary, consensus-based standards to solve global challenges. Organizations pursue ISO certifications to benefit from best-practice guidance, align with global frameworks, and signal to customers and partners that they adhere to accepted standards. ISO standards, therefore, provide the foundation for many compliance regimes.

Several ISO cybersecurity and data privacy standards address third-party supplier risks, including:

- **ISO/IEC 27001:2022** Information security, cybersecurity, and privacy protection — Information security management systems — Requirements
- **ISO/IEC 27002:2022** Information security, cybersecurity, and privacy protection — Information security controls
- **ISO/IEC 27036-2:2022** Cybersecurity — Supplier relationships — Part 2: Requirements

This guide examines supply chain security controls and guidance in the above ISO standards and identifies capabilities in the **Mitratech Third-Party Risk Management Platform** that can be used to meet ISO requirements for stronger supply chain security. For simplification, all standards are abbreviated as *ISO [number].*

ISO 27001 and ISO 27002

ISO 27001 provides a framework for establishing, implementing, maintaining, and continually improving information security management systems. It also outlines a systematic approach to securely managing sensitive company information.

ISO 27002 is a supplementary standard that provides advice on how to implement the security controls listed in Annex A of ISO 27001. It helps organizations identify what they need to meet these requirements. Together, ISO 27001 and 27002 are the foundation of most ISO standards related to cybersecurity.

With respect to managing information security in supplier relationships, **Section 15 of ISO 27001 and ISO 27002 summarizes the requirements for securely dealing with various types of third parties.** Using a top-down, risk-based approach, the specification provides the following guidance for managing suppliers:

- Create an information security policy for supplier relationships that outlines specific policies and procedures, mandating specific controls be in place to manage risk
- Establish contractual supplier agreements for any third party that may access, process, store, communicate, or provide IT infrastructure to an organization's data
- Include requirements to address the information security risks associated with information and communications technology services and product supply chain
- Manage changes to the supplier services, considering re-assessment of risks
- Monitor, review, and audit supplier service delivery

Mapping Mitratech Capabilities to ISO Standards

The summary table below maps capabilities in the **Mitratech Third-Party Risk Management Platform** to select third-party, vendor, and supplier controls present in ISO 27001, ISO 27002, and ISO 27036-2.

NOTE: This table should not be considered definitive guidance. For a complete list of controls, please review the complete ISO standards in detail and consult your auditor.

Table 1. Mitratech Mappings to ISO 27001 Security Standards

This table summarizes select supplier relationship controls most applicable to third-party risk management among the 93 identified in ISO 27001.

ISO 27001 Controls	How Mitratech Helps
5 Organizational Controls	
5.1 Policies for information security "Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."	Mitratech partners with you to build a comprehensive third-party risk management (TPRM) program in line with your broader information security, cybersecurity, and privacy protection programs—based on proven best practices and extensive real-world experience. Our **experts** collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence, to termination and offboarding – according to your organization's risk appetite.
5.1 Policies for information security "Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."	As part of this process, Mitratech can help you define: ▪ Clear roles and responsibilities (e.g., RACI) ▪ Third-party inventories ▪ Risk scoring and thresholds based on your organization's risk tolerance ▪ Assessment and monitoring methodologies based on third-party criticality ▪ Fourth-party mapping ▪ Sources of continuous monitoring data (cyber, business, reputational, financial) ▪ Key performance indicators (KPIs) and key risk indicators (KRIs) ▪ Governing policies, standards, systems, and processes to protect data ▪ Compliance and contractual reporting requirements against service levels ▪ Incident response requirements ▪ Risk and internal stakeholder reporting ▪ Risk mitigation and remediation strategies

ISO 27001 Controls	How Mitratech Helps
5.7 Threat intelligence "Information relating to information security threats shall be collected and analyzed to produce threat intelligence."	Mitratech continuously tracks and analyzes **external threats to third parties.** The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions, and financial information. Monitoring sources include: ▪ 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering 550,000 companies ▪ A database containing 10+ years of data breach history for thousands of companies around the world All monitoring data is correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, and response initiatives.
5.11 Return of assets "Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement."	When a **termination or exit** is required for critical services, Mitratech leverages customizable surveys, and workflows to report on system access, data destruction, access management, compliance with relevant laws, final payments, and more. The solution also suggests actions based on answers to offboarding assessments and routes tasks to reviewers as necessary.
5.19 Information security in supplier relationships "Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services."	Mitratech offers a library of more than 200 pre-built templates, including dedicated ISO questionnaires, **for assessing the information security risks** associated with third-parties. Assessments are centrally managed in the Mitratech Platform. They are backed by workflow, task management, and automated evidence review to enable visibility into risks throughout the supplier relationship. Importantly, Mitratech delivers built-in remediation recommendations based on risk assessment results to ensure that third parties address risks in a timely and satisfactory manner. For organizations with limited resources and expertise, Mitratech can **manage the third-party risk lifecycle on your behalf** – from onboarding suppliers and collecting evidence, to providing remediation guidance and reporting on contract SLAs. As a result, you reduce vendor risk and simplify compliance without burdening internal staff.

ISO 27001 Controls	How Mitratech Helps
5.20 Addressing information security within supplier agreements "Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship."	Mitratech centralizes the distribution, discussion, retention, and review of **supplier contracts**. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. Key capabilities include: ▪ Central tracking of contracts and contract attributes (e.g., type, key dates, value, reminders, and status) with custom, role-based views ▪ Workflow capabilities (based on user or contract type) to automate the contract management lifecycle ▪ Automated reminders and overdue notices to speed contract reviews ▪ Centralized contract discussion and comment tracking ▪ Contract and document storage with role-based permissions and audit trails of all access ▪ Version control tracking that supports offline contract and document edits ▪ Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access
5.21 Managing information security in the information and communication technology (ICT) supply chain "Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain."	Mitratech standardizes assessments against **ISO** best practices and other information security control frameworks, providing internal audit and IT security teams with a central platform for measuring and demonstrating adherence to secure software development and software development lifecycle (SDLC) practices.
5.22 Monitoring, review, and change management of supplier services "The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery."	Mitratech continuously tracks and analyzes **external threats to third parties**. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions, and financial information. Monitoring sources include: ▪ 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering ▪ 550,000 companies ▪ A database containing 10+ years of data breach history for thousands of companies around the world All monitoring data is correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, and response initiatives.

ISO 27001 Controls	How Mitratech Helps
5.23 Information security for use of cloud services "Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements."	Mitratech standardizes assessments against **SOC 2**, Cyber Essentials, **ISO**, and other information security control frameworks, providing key controls assessments against cloud services requirements. These same assessments are also used to assess information security controls when offboarding cloud services.
5.24 Information security incident management planning and preparation "The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities."	Mitratech enables your team to rapidly identify, respond to, report on, and mitigate the impact of **third-party vendor incidents** by centrally managing vendors, conducting event assessments, scoring identified risks, correlating against continuous cyber monitoring, and accessing remediation guidance. Key capabilities include: ▪ Continuously updated and customizable event and incident management questionnaires ▪ Real-time questionnaire completion progress tracking ▪ Defined risk owners with automated chasing reminders to keep surveys on schedule ▪ Proactively vendor reporting ▪ Consolidated views of risk ratings, counts, scores, and flagged responses for each vendor ▪ Workflow rules to trigger automated playbooks to act on risks according to their potential impact to the business ▪ Guidance from built-in remediation recommendations to reduce risk ▪ Built-in report templates ▪ Data and relationship mapping to identify relationships between your organization and third parties to visualize information paths and determine at-risk data
5.25 Assessment and decision on information security events "The organization shall assess information security events and decide if they are to be categorized as information se curity incidents."	
5.26 Response to information security incidents "Information security incidents shall be responded to in accordance with the documented procedures."	
5.28 Collection of evidence "The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events."	

ISO 27001 Controls	How Mitratech Helps
5.30 ICT readiness for business continuity "ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements."	Mitratech automates the assessment, continuous monitoring, analysis, and remediation of **third-party business resilience** and **continuity** – while automatically mapping results to ISO and other control frameworks. To complement business resilience assessments and validate results, Mitratech: ▪ Automates continuous cyber monitoring that may predict possible third-party business impacts ▪ Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability ▪ Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns This proactive approach enables your organization to minimize the impact of third-party disruptions and stay on top of compliance requirements. The Mitratech Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: ▪ Categorize suppliers according to their risk profile and criticality to the business ▪ Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) ▪ Centralize system inventory, risk assessments, RACI charts, and third parties ▪ Ensure consistent communications with suppliers during business disruptions
5.31 Legal, statutory, regulatory and contractual requirements "Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date."	Mitratech centralizes the distribution, discussion, retention, and review of **supplier contracts**. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. Key capabilities include: ▪ Centralized tracking of all contracts and contract attributes such as type, key dates, value, reminders, and status – with customized, role-based views ▪ Workflow capabilities (based on user or contract type) to automate the contract management lifecycle ▪ Automated reminders and overdue notices to speed contract reviews ▪ Centralized contract discussion and comment tracking ▪ Contract and document storage with role-based permissions and audit trails of all access ▪ Version control tracking that supports offline contract and document edits ▪ Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access

ISO 27001 Controls	How Mitratech Helps
5.34 Privacy and protection of personal identifiable information (PII) "The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements."	Mitratech delivers a centralized, collaborative platform for conducting privacy assessments and mitigating both third-party and **internal privacy risks**. Key data security and privacy assessment capabilities include: ▪ Scheduled assessments and relationship mapping to reveal where personal data exists, where it is shared, and who has access – all summarized in a risk register that highlights critical exposures ▪ Privacy Impact Assessments to uncover at-risk business data and personally identifiable information (PII) ▪ Vendor assessments against GDPR and other privacy regulations via the Mitratech Compliance Framework (PCF) – reveals potential hot spots by mapping identified risks to specific controls ▪ GDPR risk and response mapping to controls. Includes percent- compliance ratings and stakeholder-specific reports. ▪ A database containing 10+ years of data breach history for thousands of companies – includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications ▪ Centralized onboarding, distribution, discussion, retention, and review of vendor contracts – ensures that data protection provisions are enforced from the beginning of the relationship
5.36 Compliance with policies, rules, and standards for information security "Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed."	With Mitratech, auditors can establish a program to efficiently achieve and demonstrate compliance. The solution automates **third-party risk management compliance** auditing by collecting vendor risk information, quantifying risks, recommending remediations, and generating reports for dozens of government regulations and industry frameworks. Mitratech automatically maps information gathered from control-based assessments to ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, SOX, NYDFS, and other regulatory frameworks, enabling you to quickly visualize and address important compliance requirements.

Table 2. Mitratech Mappings to ISO 27002 Security Standards for Supplier Relationships

This table provides greater detail into the supplier relationship controls reviewed in ISO 27001 5.19-5.22.

ISO 27002 Controls	How Mitratech Helps
5.19 Information security in supplier relationships "Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services."	
5.19 a) "identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;"	The Mitratech Platform enables organizations to automatically tier suppliers according to their **inherent risk scores**, set appropriate levels of diligence, and determine the scope of ongoing assessments. Organizations can also categorize vendors with rule-based logic based on a range of data interaction, financial, regulatory, and reputational considerations.
5.19 e) "defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information;"	
5.19 b) "establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, onsite assessments, certifications);"	Mitratech centralizes and automates the distribution, comparison, and management of requests for proposals (RFPs) and requests for information (RFIs) as part of **vendor selection decisions**. Mitratech moves each selected vendor into contracting and/or onboarding due diligence phases, automatically progressing the vendor through the third-party lifecycle. Mitratech features a library of more than 200 pre-built templates for ongoing third-party **risk assessments**. These are integrated with native cyber, business, reputational, and financial risk monitoring capabilities, which continuously validate assessment findings and fill gaps between assessments. Built-in remediation recommendations ensure that third parties address risks in a timely and satisfactory manner.
5.19 c) "evaluating and selecting supplier's products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier's information and information processing and hence the organization's information security;"	The **Mitratech Risk Profiling Snapshot** enables you to compare and monitor demographics, fourth-party technologies, ESG scores, recent business and reputational insights, data breach history, and financial performance of potential vendors. With the Snapshot, you can see results in line with RFx responses for a holistic view of suppliers – their fit for purpose and fit according to your organization's risk appetite.

ISO 27002 Controls	How Mitratech Helps
5.19 g) "monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;"	With Mitratech, auditors can establish a program to efficiently achieve and demonstrate compliance. The solution automates third-party **risk management compliance auditing** by collecting vendor risk information, quantifying risks, recommending remediations, and generating reports for dozens of government regulations and industry frameworks. Mitratech automatically maps information gathered from control-based assessments to **ISO** and other regulatory frameworks and validates it with **continuous monitoring**, enabling you to quickly visualize and address important compliance requirements.
5.19 h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by other means;	
5.19 i) "handling incidents and contingencies associated with supplier products and services including responsibilities of both the organization and suppliers;"	The Mitratech **Third-Party Incident Response Service** enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
5.19 j) "resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier's information and information processing and hence the availability of the organization's information;"	Mitratech automates the assessment, continuous monitoring, analysis, and remediation of **third-party business resilience and continuity** – while automatically mapping results to ISO and other control frameworks. To complement business resilience assessments and validate results, Mitratech: ▪ Automates continuous cyber monitoring that may predict possible third-party business impacts ▪ Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability ▪ Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns This proactive approach enables your organization to minimize the impact of third-party disruptions and stay on top of compliance requirements. The Mitratech Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: ▪ Categorize suppliers according to their risk profile and criticality to the business ▪ Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) ▪ Centralize system inventory, risk assessments, RACI charts, and third parties ▪ Ensure consistent communications with suppliers during business disruptions

ISO 27002 Controls	How Mitratech Helps
5.19 m) "requirements to ensure a secure termination of the supplier relationship, including: 1. de-provisioning of access rights; 2. information handling; 3. determining ownership of intellectual property developed during the engagement; 4. information portability in case of change of supplier or insourcing; 5. records management; 6. return of assets; 7. secure disposal of information and other associated assets; 8. ongoing confidentiality requirements"	The Mitratech Platform automates contract assessments and **offboarding** procedures to reduce your organization's risk of post-contract exposure. ▪ Schedule tasks to review contracts to ensure all obligations have been met. Issue customizable contract assessments to evaluate status. ▪ Leverage customizable surveys and workflows report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more. ▪ Centrally store and manage documents and certifications, such as NDAs, SLAs, SOWs, and contracts. Leverage built-in automated document analysis based on AWS natural language processing and machine learning analytics to confirm key criteria are addressed. ▪ Take actionable steps to reduce vendor risk with built-in remediation recommendations and guidance. ▪ Visualize and address compliance requirements by automatically mapping assessment results to any regulation or framework.

5.20 Addressing security within supplier agreements

"Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship."

5.20 d) "legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;"	Mitratech centralizes the distribution, discussion, retention, and review of **vendor contracts**, ensuring that key provisions are included in supplier contracts and continually tracked. Key capabilities include: ▪ Centralized tracking of all contracts and contract attributes such as type, key dates, value, reminders, and status – with customized, role-based views ▪ Workflow capabilities (based on user or contract type) to automate the contract management lifecycle ▪ Automated reminders and overdue notices to streamline contract reviews ▪ Centralized contract discussion and comment tracking ▪ Contract and document storage with role-based permissions and audit trails of all access ▪ Version control tracking that supports offline contract and document edits ▪ Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access

ISO 27002 Controls	How Mitratech Helps
5.20 e) "obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting and auditing, and the supplier's obligations to comply with the organization's information security requirements;"	The Mitratech solution enables internal, control-based assessments (based on the **ISO** industry standard framework and/or custom questionnaires). The platform includes built-in workflow capabilities that enable assessors to interact efficiently with third parties during the due diligence collection and review periods. Robust reporting and audit capabilities give each level of management the information it needs to properly review the third party's performance. Organizations can assess third parties against cybersecurity, SLA performance, and other topics, and correlate findings with the results of continuous outside monitoring for a complete view of risks.
5.20 h) "information security requirements regarding the supplier's ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and risk criteria;"	Mitratech provides a framework for centrally measuring **third-party KPIs and KRIs** against your requirements and reducing gaps in vendor oversight with embedded machine learning (ML) insights and customizable, role-based reports. The capabilities can help your team to uncover risk and performance trends, determine third-party risk status, and identify exceptions to common behavior that could warrant further investigation. Built-in remediation recommendations ensure that third parties address risks in a timely and satisfactory manner
5.20 i) "indemnities and remediation for failure of contractor to meet requirements;"	
5.20 j) "incident management requirements and procedures (especially notification and collaboration during incident remediation);"	Mitratech enables your team to rapidly identify, respond to, report on, and mitigate the impact of **third-party vendor security incidents** as part of your broader **incident management strategy**. Armed with these insights, your team can better understand the scope and impact of the incident; what data was involved; whether the third party's operations were impacted; and when remediations have been completed – all by leveraging Mitratech experts.
5.20 l) "relevant provisions for sub-contracting, including the controls that need to be implemented, such as agreement on the use of sub-suppliers (e.g. requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change);"	Mitratech can identify **fourth-party and Nth-party subcontracting relationships** by conducting a questionnaire-based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk. Suppliers discovered through this process are continuously monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening. This approach provides insights to address potential technology or geographic concentration risk.

ISO 27002 Controls	How Mitratech Helps
5.20 o) "the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls;"	The Mitratech **Controls Validation Service** reviews third-party assessment responses and documentation against established testing protocols to validate that indicated controls are in place. Mitratech experts first review assessment responses, whether from custom or standardized questionnaires. We then map the responses to ISO and/or other control frameworks. Finally, we work with you to develop remediation plans and track them to completion. With remote and onsite options available, Mitratech delivers the expertise to help you reduce risk with your existing resources.
5.20 q) "supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;"	
5.20 x) "termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;"	Mitratech **contract lifecycle management** capabilities ensure that key provisions are included in supplier contracts and continually tracked. Automated contract assessments and **offboarding** procedures such as reporting on system access, data destruction, access management, compliance with all relevant laws, and final payments reduce your organization's risk of post-contract exposure.
5.20 y) "provision of a method of securely destroying the organization's information stored by the supplier as soon as it is no longer required;"	
5.20 z) "ensuring, at the end of the contract, handover support to another supplier or to the organization itself;"	
5.21 Managing information security in the ICT supply chain "Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain."	
5.21 b) "termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;"	Mitratech can identify **fourth-party and Nth-party subcontracting relationships** by conducting a questionnaire- based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk.

ISO 27002 Controls	How Mitratech Helps
5.21 c) "requiring that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities (e.g. sub-contracted software developers and hardware component providers);"	*(continued)* Suppliers discovered through this process are continuously monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening. This approach provides insights to address potential technology or geographic concentration risk.
5.21 f) "implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements. Examples of such supplier review methods can include penetration testing and proof or validation of third- party attestations for the supplier's information security operations;"	
5.21 g) "implementing a process for identifying and documenting product or service components that are critical for maintaining functionality and therefore require increased attention, scrutiny and further follow up required when built outside of the organization especially if the supplier outsources aspects of product or service components to other suppliers;"	Mitratech enables you to assess and monitor third parties based on criticality or the extent of threats to their information assets by capturing, tracking, and quantifying **inherent risks**. Criteria used to calculate inherent risk for third-party classification includes: ▪ Type of content required to validate controls ▪ Criticality to business performance and operations ▪ Location(s) and related legal or regulatory considerations ▪ Level of reliance on fourth parties (to avoid concentration risk) ▪ Exposure to operational or client-facing processes ▪ Interaction with protected data ▪ Financial status and health ▪ Reputation From this inherent risk assessment, your team can automatically tier suppliers; set appropriate levels of further diligence; and determine the scope of ongoing assessments. Rule-based tiering logic enables vendor categorization using a range of data interaction, financial, regulatory and reputational considerations.

ISO 27002 Controls	How Mitratech Helps
5.22 Monitoring, review, and change management of supplier services "The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery."	
5.22 a) "monitor service performance levels to verify compliance with agreements;"	With the Mitratech Platform, organizations can customize surveys to make it easy to gather and analyze necessary performance and contract data in a single risk register. Mitratech identifies key contract attributes relating to **SLAs or performance**, populates those requirements in the Platform, and assigns tasks to you and your third party for tracking purposes.
5.22 b) "monitor changes made by suppliers including: 1. enhancements to the current services offered; 2. development of any new applications and systems; 3. modifications or updates of the supplier's policies and procedures; 4. new or changed controls to resolve information security incidents and to improve information security;"	Mitratech continuously tracks and analyzes **external threats to third parties**. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. All monitoring data is correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting and response initiatives. Monitoring sources include: ▪ 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering 550,000 companies ▪ A database containing 10+ years of data breach history for thousands of companies around the world Because not all threats are direct cyberattacks, Mitratech also incorporates data from the following sources to add context into cyber findings: ▪ 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, operational updates, and more ▪ A global network of 2 million businesses with 5 years of organizational changes and financial performance, ▪ including turnover, profit and loss, shareholder funds, etc. ▪ 30,000 global news sources ▪ A database containing over 1.8 million politically exposed person profiles ▪ Global sanctions lists and over 1,000 global enforcement lists and court filings

ISO 27002 Controls	How Mitratech Helps
5.22 e) "conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;"	The Mitratech **Controls Validation Service** reviews third-party assessment responses and documentation against established testing protocols to validate that indicated controls are in place. Mitratech experts first review assessment responses, whether from custom or standardized questionnaires. We then map the responses to ISO and/or other control frameworks. Finally, we work with you to develop remediation plans and track them to completion. With remote and onsite options available, Mitratech delivers the expertise to help you reduce risk with your existing resources.
5.22 f) "provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;" **5.22 g)** "review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;" **5.22 h)** "respond to and manage any identified information security events or incidents;"	Mitratech enables your team to rapidly identify, respond to, report on, and mitigate the impact of **third-party vendor incidents** by centrally managing vendors, conducting event assessments, scoring identified risks, correlating against continuous cyber monitoring, and accessing remediation guidance. Key capabilities include: ▪ Continuously updated and customizable event and incident management questionnaires ▪ Real-time questionnaire completion progress tracking ▪ Defined risk owners with automated chasing reminders to keep surveys on schedule ▪ Proactively vendor reporting ▪ Consolidated views of risk ratings, counts, scores, and flagged responses for each vendor ▪ Workflow rules to trigger automated playbooks to act on risks according to their potential impact to the business ▪ Guidance from built-in remediation recommendations to reduce risk ▪ Built-in report templates ▪ Data and relationship mapping to identify relationships between your organization and third parties to visualize information paths and determine at-risk data
5.22 i) "identify information security vulnerabilities and manage them;"	Mitratech continuously tracks and **analyzes external threats to third parties**. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, correlating monitoring data with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, and response initiatives. Monitoring sources include: ▪ 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering 550,000 companies ▪ A database containing 10+ years of data breach history for thousands of companies around the world

ISO 27002 Controls	How Mitratech Helps
5.22 j) "review information security aspects of the supplier's relationships with its own suppliers"	Mitratech can identify **fourth-party and Nth-party subcontracting relationships** by conducting a questionnaire- based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk. Suppliers discovered through this process are continuously monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening.
5.22 k) "ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster;"	Mitratech automates the assessment, continuous monitoring, analysis, and remediation of **third-party business resilience and continuity** – while automatically mapping results to ISO and other control frameworks. The Mitratech Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: ▪ Categorize suppliers according to their risk profile and criticality to the business ▪ Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) ▪ Centralize system inventory, risk assessments, RACI charts, and third parties ▪ Ensure consistent communications with suppliers during business disruptions This proactive approach enables your organization to minimize the impact of third-party disruptions and stay on top of compliance requirements.
5.22 m) "evaluate regularly that the suppliers maintain adequate information security levels;"	Mitratech automates **risk assessments** to extend the visibility, efficiency, and scale of your third-party risk management program across every stage of the third-party lifecycle. With a library of 200+ standardized assessments, customization capabilities, and built-in workflow and remediation, the solution automates everything from survey collection and analysis to risk rating and reporting. With Mitratech, you can easily gather and correlate intelligence on a wide range of vendor controls to determine threats to information management, based on the criticality of the third party as determined by the inherent risk assessment. Results of assessments and continuous monitoring are collated in a single risk register with heat map reporting that measures and categorizes risks based on likelihood and impact. With this insight, teams can easily see the consequences of a risk and have ready-made remediation recommendations for third parties to mitigate the risks.

Table 3. Mitratech Mitratech Mappings to ISO 27036-2 Security Standards

Although the entire ISO 27036-2 standard is applicable for supplier relationships, this table highlights only the most prominent controls.

ISO 27036-2 Controls	How Mitratech Helps
6 Information security in supplier relationship management	
6.1.1.1 Agreement processes / Acquisition process / Objective Establish a supplier relationship strategy that: ▪ is based on the information security risk tolerance of the acquirer; ▪ defines the information security foundation to use when planning, preparing, managing, and terminating the procurement of a product or service.	Mitratech partners with you to build a comprehensive third-party risk management (TPRM) program in line with your broader information security and governance, risk, and compliance programs based on proven best practices and extensive real-world experience. Our **experts** collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence, to termination and offboarding – according to your organization's risk appetite. As part of this process, Mitratech can help you define: ▪ Clear roles and responsibilities (e.g., RACI) ▪ Third-party inventories ▪ Risk scoring and thresholds based on your organization's risk tolerance ▪ Assessment and monitoring methodologies based on third-party criticality ▪ Fourth-party mapping ▪ Sources of continuous monitoring data (cyber, business, reputational, financial) ▪ Key performance indicators (KPIs) and key risk indicators (KRIs) ▪ Governing policies, standards, systems and processes to protect data ▪ Compliance and contractual reporting requirements against service levels ▪ Incident response requirements ▪ Risk and internal stakeholder reporting ▪ Risk mitigation and remediation strategies
6.1.2.1 Agreement processes / Supply process / Objective Establish an acquirer relationship strategy that: ▪ is based on the information security risk tolerance of the supplier; ▪ defines the information security baseline to use when planning, preparing, managing and terminating the supply of a product or service.	
6.2.1 Organizational project-enabling processes / Life cycle model management process a) The acquirer and the supplier shall establish the life cycle model management process when managing information security in supplier relationships.	Mitratech helps to eliminate the security and compliance exposures that come from working with vendors, suppliers, and other third parties across the entire vendor risk lifecycle – from sourcing and selection to offboarding and everything in between.

ISO 27036-2 Controls	How Mitratech Helps
6.2.2.2 Organizational project-enabling processes / Infrastructure management process / Activities b) Define, implement, maintain, and improve contingency arrangements to ensure that the procurement or the supply of a product or service can continue in the event of its disruption caused by natural or man-made causes.	Mitratech automates the assessment, continuous monitoring, analysis, and remediation of **third-party business resilience and continuity** – while automatically mapping results to ISO and other control frameworks. To complement business resilience assessments and validate results, Mitratech: ▪ Automates continuous cyber monitoring that may predict possible third-party business impacts ▪ Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability ▪ Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns This proactive approach enables your organization to minimize the impact of third-party disruptions and stay on top of compliance requirements. The Mitratech Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: ▪ Categorize suppliers according to their risk profile and criticality to the business ▪ Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) ▪ Centralize system inventory, risk assessments, RACI charts, and third parties ▪ Ensure consistent communications with suppliers during business disruptions
6.2.3.2 Project portfolio management process / Activities a) Define, implement, maintain, and improve a process for identifying and categorizing suppliers or acquirers based on the sensitivity of the information shared with them and on the access level granted to them to acquirer's or supplier's assets, such as information and information systems;	Mitratech enables you to assess and monitor third parties based on criticality or the extent of threats to their information assets by capturing, tracking, and quantifying inherent risks. Criteria used to calculate **inherent risk** for third-party classification includes: ▪ Type of content required to validate controls ▪ Criticality to business performance and operations ▪ Location(s) and related legal or regulatory considerations ▪ Level of reliance on fourth parties (to avoid concentration risk) ▪ Exposure to operational or client-facing processes ▪ Interaction with protected data ▪ Financial status and health ▪ Reputation From this inherent risk assessment, your team can automatically tier suppliers; set appropriate levels of further diligence; and determine the scope of ongoing assessments. Rule-based tiering logic enables vendor categorization using a range of data interaction, financial, regulatory and reputational considerations.

ISO 27036-2 Controls	How Mitratech Helps
6.3.4.1 Project processes / Risk management process / Objective a) Continuously address information security risks in supplier relationships and throughout their life cycle including re-examining them periodically or when significant business, legal, regulatory, architectural, policy, and contractual changes occur.	Mitratech continuously tracks and analyzes **external threats to third parties**. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. All monitoring data is correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting and response initiatives. Monitoring sources include: ▪ 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering 550,000 companies ▪ A database containing 10+ years of data breach history for thousands of companies around the world Because not all threats are direct cyberattacks, Mitratech also incorporates data from the following sources to add context into cyber findings: ▪ 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, operational updates, and more ▪ A global network of 2 million businesses with 5 years of organizational changes and financial performance, ▪ including turnover, profit and loss, shareholder funds, etc. ▪ 30,000 global news sources ▪ A database containing over 1.8 million politically exposed person profiles ▪ Global sanctions lists and over 1,000 global enforcement lists and court filings
6.3.7.1 Project processes / Measurement process / Objective a) Collect, analyze, and report information security measures related to the procurement or supply of a product or service to demonstrate the maturity of information security in a supplier relationship and to support effective management of processes.	Mitratech automates **risk assessments** to extend the visibility, efficiency, and scale of your third-party risk management program across every stage of the third-party lifecycle. With a library of 200+ standardized assessments, customization capabilities, and built-in workflow and remediation, the solution automates everything from survey collection and analysis to risk rating and reporting. With Mitratech, you can easily gather and correlate intelligence on a wide range of vendor controls to determine threats to information management, based on the criticality of the third party as determined by the inherent risk assessment. Results of assessments and continuous monitoring are collated in a single risk register with heat map reporting that measures and categorizes risks based on likelihood and impact. With this insight, teams can easily see the consequences of a risk and have ready-made remediation recommendations for third parties to mitigate the risks.

ISO 27036-2 Controls	How Mitratech Helps
7 Information security in a supplier relationship instance	
7.2.1 Supplier selection process / Objectives a) Select a supplier that provides adequate information security for the product or service that may be procured.	The Mitratech **Risk Profiling Snapshot** enables you to compare and monitor demographics, fourth-party technologies, ESG scores, recent business and reputational insights, data breach history, and financial performance of potential vendors. With the Snapshot, you can see results in line with RFx responses for a holistic view of suppliers – their fit for purpose and fit according to your organization's risk appetite.
7.3.1 Supplier relationship management process / Objective Establish and agree on a supplier relationship agreement addressing the following: ▪ information security roles and responsibilities of the acquirer and the supplier; ▪ security controls required across information security, ICT security, personnel security, and physical security; ▪ a transition process when the product or service has been previously operated or manufactured by a party different from the supplier; ▪ information security change management; ▪ information security incident management; ▪ compliance monitoring and enforcement;	The Mitratech Platform automates workflows required to assess, manage, continuously monitor and remediate third-party security, privacy, compliance, and procurement/supply chain-related risks across every stage of the vendor lifecycle. The solution: ▪ Automates vendor onboarding and offboarding ▪ Profiles, tiers, and scores inherent risk for all suppliers ▪ Automates fourth-party mapping and vendor demographics in a central profile ▪ Delivers the largest library of standardized and custom risk assessments with built-in workflow, tasks, and evidence management ▪ Integrates native cyber, business, reputational, and financial risk monitoring to correlate risks against assessment results and validate findings ▪ Includes machine learning analytics to normalize and correlate findings from multiple sources ▪ Delivers compliance and risk reporting by framework or regulation ▪ Improves remediation management with built-in guidance ▪ Includes Contract and RFx management to enable more complete risk management prior to onboarding ▪ Automates third-party incident response
7.4.1 Supplier relationship management process / Objectives a) Maintain information security during the execution period of the supplier relationship in accordance with the supplier relationship agreement and by particularly considering the following: 4) Monitor and enforce compliance of the supplier with information security provisions defined in the supplier relationship agreement.	With the Mitratech Platform, acquirers can automatically map information gathered from control-based assessments to regulatory frameworks – including ISO and many others – to quickly visualize and address important compliance requirements at every stage of the supplier lifecycle.

ISO 27036-2 Controls	How Mitratech Helps
7.5.1 Supplier relationship termination process / Objectives a) Protect the product or service supply during termination to avoid any information security, legal and regulatory impacts after the notice of termination; b) Terminate the product or service supply in accordance to the termination plan.	The Mitratech Platform automates contract assessments and **offboarding** procedures to reduce your organization's risk of post-contract exposure. ▪ Schedule tasks to review contracts to ensure all obligations have been met. Issue customizable contract assessments to evaluate status. ▪ Leverage customizable surveys and workflows report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more. ▪ Centrally store and manage documents and certifications, such as NDAs, SLAs, SOWs,zzzz and contracts. Leverage built- in automated document analysis based on AWS natural language processing and machine learning analytics to confirm key criteria are addressed. ▪ Take actionable steps to reduce vendor risk with built-in remediation recommendations and guidance. ▪ Visualize and address compliance requirements by automatically mapping assessment results to any regulation or framework.

The Mitratech Difference

The ISO standards presented in this paper require robust management and tracking of third-party supplier security and data privacy risk. They specify the following:

- A policy for selecting suppliers based on information security practices should be in place;
- A policy for managing risk should be in place;
- A policy should be codified in supplier agreements; and
- Suppliers should be managed and audited to the agreed requirements.

Having strong information security management systems is part of the supplier lifecycle and requires a complete, internal view of the controls in place – as well as continuous monitoring of all third parties to validate the presence and effectiveness of certain controls. This cannot be addressed with a simple, external automated scan or with spreadsheets.

Mitratech's Third-Party Risk Management Solutions offers a complete framework for implementing policy management, auditing and reporting related to the third-party risk and supply chain compliance requirements of ISO 27001, 27002, and 27036-2 – with dedicated questionnaires and risk registers for each standard.

Contact Mitratech for a **free maturity assessment** to determine how your current TPRM policies stack up to ISO standards, or **request a demo**.

About Mitratech

Mitratech is a proven global technology partner for corporate legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility, and spurring collaboration across an enterprise. Mitratech serves over 20,000 organizations worldwide, spanning more than 160 countries.

For more info, **visit: www.mitratech.com.**

EMPOWER. AUTOMATE. ELEVATE.