Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Recommended contract clauses for security operations centre procurement

Management

Canada

Foreword

This is an UNCLASSIFIED publication, issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information or to suggest amendments, email or phone our Contact Centre:

contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on April 23, 2025.

Revision history

Revision	Amendments	Date
1	First release.	April 23, 2025

D97-4/00-500-2025E-PDF
ISBN 978-0-660-76378-1

Overview

To effectively protect against cyber threats, it's essential for your organization to have comprehensive visibility and control over its digital infrastructure and activities. Implementing a security operations centre (SOC) is one way to achieve this. To successfully deploy and manage a SOC, it's critical to establish clear contract clauses and principles when contracting the SOC to a managed security provider (MSP) or managed security service provider (MSSP). This ensures mutual understanding and documentation of expectations.

Key components of cyber security services must be outlined in these contracts. These include service-level agreements (SLAs), task orders, and governing standards, among others. Collectively, they form a prescriptive service framework, assuring clients that they will receive the expected services and solutions. This framework also guarantees the security of their data and identities.

This publication details the specific services, deliverables and responsibilities expected from an MSP/MSSP, as well as those of the organization procuring these services. The recommendations should be interpreted in the context of both the functional and fiduciary aspects of service contracting with any managed service provider.

Disclaimer:

The information provided in this document is provided “as-is”, without warrantee or representation of any kind, to be used at the users’ discretion. The users of this information shall have no recourse against any of the authors for any loss, liability, damage or cost that may be suffered or incurred at any time arising for the use of information in this document.

Table of contents

1 Introduction

As digital threats escalate, organizations increasingly rely on SOC services to monitor information security and manage digital risks effectively. While the specific functions of an SOC can vary, they typically involve centralized monitoring of the overall security posture through the collection of log data from network devices and systems. SOCs also rely on tools such as security information and event management (SIEM) systems, which interpret log data and correlate it with network incidents. Additionally, threat intelligence plays a crucial role in SOC operations by assessing events related to network systems.

Given the complexity of building a mature SOC from the ground up, this publication aims to outline fundamental expectations for evaluating SOC contracts and identifying procurement risks. These considerations should be aligned with the main functional and fiduciary aspects of contracting, whether your organization is working with an MSP or an MSSP.

While service providers may propose initial foundational service terms and conditions, management is responsible for ensuring that these terms address the organization's business security needs and remain flexible for future adjustments. The terms and conditions in the service contract should be designed to yield the best business outcomes for your organization. It is crucial for your organization to take proactive steps to guarantee service provisions, including mechanisms for identifying, preventing, detecting, responding to and recovering from security risks.

The clauses outlined in this publication are not legal advice but provide context for evaluating SOC services and understanding the terms and conditions from potential service providers.

1.1 Scope

This publication provides practical advice and guidance on contracting SOC services from a cyber security perspective. It is relevant for both the consuming organizations and the service providers. While the examples presented here are not exhaustive or definitive best practices, they do offer valuable insights based on successful applications by government and industry partners.

Please note that despite the TLP:CLEAR classification, standard copyright rules apply. The contents of this document are protected and should not be reproduced or distributed without proper authorization.

1.2 Guiding publications

In preparing this guidance, the Cyber Centre considered inputs from the following reference publications and frameworks.

1.2.1 Government of Canada resources

- Best practices for setting up a security operations centre (SOC) (ITSAP.00.500)
- Supply chain integrity (SCI) process and assessment requirements (PDF)
- Baseline cyber security controls for small and medium organizations
- Schedule 1 – Security obligations for Tier 2 Software as a Service (SaaS) (PDF)

- Schedule 2 – Privacy obligations (PDF)

1.2.2 Industry and other resources

- Federal Risk and Authorization Management Program (FedRAMP) Control-Specific Contract Clauses version 3.0 (PDF)
- Assessing Security Requirements for Controlled Unclassified Information (NIST SP 800-171)
- Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-172): A Supplement to NIST Special Publication 800-171
- Building a Security Operations Centre (SOC) (National Cyber Security Centre)

1.2.3 Recommended nomenclature

This publication highlights key contractual terms pertinent to procuring SOC services, especially those that are cloud-based, from a cyber security perspective. These terms are relevant for both immediate needs and future requirements.

Below is a summary of essential clauses to consider, based on the specific SOC services required by an organization:

- When establishing service contracts, it is crucial to differentiate between mandatory and rated requirements. Mandatory requirements are those that the service provider must meet (related contract clauses stipulate “must have” or “shall provide”). Rated requirements, on the other hand, are more flexible, and use terms like “should”, “may”, or “consider”. These suggest that the provider already possesses these capabilities.
- For services that are part of a future roadmap or are not yet available, look for terms such as “will” or “capable of achieving”. These indicate a provider's commitment to meeting future expectations.

It's important to recognize that some services might require time for re-engineering to meet specific needs or may include updated features in future roadmaps. Therefore, organizations must balance immediate requirements with those that allow for development and evolution.

2 Security operations centre provider selection process

Many organizations may consider a SOC from an MSP or MSSP with different subscription models due to resourcing and capabilities of an outsourced SOC. The SOC can be hosted in an MSP or MSSP environment, whereby your organization can send all the logs to the MSP or MSSP within its cloud tenancy. Or you organization can hire an MSP or MSSP service to operate SOC features within its tenancy, on your behalf.

When selecting an MSP or MSSP provider, there are many considerations and decisions your organizations should make internally on the approach and services it requires.

- Service scope and offerings: Understand the range of services provided by the MSP/MSSP and determine if they offer both proactive threat hunting and reactive incident response capabilities
- Scalability and flexibility: Assess the provider's ability to scale services up or down based on your organization's changing needs and evaluate the flexibility of services in response to emerging threats or organizational growth
- Customization and integration: Ensure that the MSP/MSSP SOC service can be tailored to fit your organization's specific environment, industry, and existing security infrastructure and check for compatibility with your current systems and tools
- Data management and protection:
  - Inquire about the tools and technologies used for data collection and analysis
  - Understand what data will be captured, how it will be used, and where it will be stored
    - Understand where and with whom your data may be shared
    - Clarify the approval or permissions process for sharing data
  - Ensure robust measures are in place for protecting sensitive and confidential data
- Service level agreement (SLA): Examine the SLA for clear definitions of service expectations, deliverables, and response times and understand how the SLA will be measured, monitored, and enforced
- Compliance and security standards: Verify that the SOC provider follows industry-standard security practices and complies with relevant regulations to mitigate risks, including supply chain vulnerabilities
- Risk assessment and threat profiling: Perform a comprehensive cyber security risk assessment to identify specific threats and vulnerabilities relevant to your organization
  - Government of Canada departments should refer to IT security risk management: A lifecycle approach (ITSG-33)
  - Organizations outside the Government of Canada should consult the Structured Threat Information eXpression (STIX) 2.1 framework
- Contractual clarity and responsibilities: Establish clear contractual terms, outlining the responsibilities of both your organization and the service provider as per the shared responsibility model
- Key considerations for choosing a SOC provider: Ensure there are provisions for regular reviews, updates, and adjustments to the services as needed

For more information read, Best practices for setting up a security operations centre (SOC) (ITSAP.00.500).

Overall, as the organization requesting the services, you must do work upfront to decide on a SOC strategy and scope. This includes identifying which assets, such as systems and data, are sensitive and need to be monitored and protected. For more information on asset inventory and categorization, read Guidance on the security categorization of cloud-based services (ITSP.50.103).

2.1 Main services for consideration in a security operations centre

Below are the key services for an effective SOC, accompanied by examples of contract clauses to help you draft the language and expectations in your service agreements.

Consider the following essential services:

- **Security operations, monitoring, and reporting:** Continuous surveillance and analysis of security events, with timely reporting. Example clause: "Provider shall ensure 24/7 security monitoring and near-real time incident reporting.”
- **Incident support:** Rapid response and support for security incidents. Example clause: "Provider must offer near-real time incident response services."
- **Threat analysis and intelligence:** Proactive identification and analysis of potential threats. Example clause: "Provider is required to deliver regular threat intelligence updates.”
- **Documentation and standard operating procedures (SOPs):** Maintenance of detailed security documentation and SOPs. Example clause: "Provider shall keep comprehensive, up-to-date security documentation and SOPs based on the shared responsibility model."
- **Additional capabilities: Advanced incident management support, forensics and malware analysis:** Specialized support for complex incidents, including forensic analysis. Example clause: "Provider shall offer advanced incident management and forensic analysis capabilities."
- **Ongoing vulnerability assessments and security assurance scans:** Regular assessments to identify and mitigate vulnerabilities. Example clause: "Provider must conduct periodic vulnerability assessments and provide reports."
- **Security technology maintenance and operation:** Ensuring the effective operation and maintenance of security technologies. Example clause: "Provider must operate and maintain the infrastructure and technology supporting the service."

Your organization should also consider additional services that may be required upfront or that can be optionally included later, depending on evolving security needs. These could include compliance management, risk assessment, cloud security, and cyber security training initiatives.

2.1.1 Security operations, monitoring and reporting

Security operations, monitoring, and reporting are crucial for observing and analyzing data related to events, incidents, or breaches and the status of information systems or networks. The primary objective is to detect unusual or unauthorized activity and to gather security-relevant data to understand system behaviour. This process is essential for mitigating network vulnerabilities and identifying internal and external threats.

Role and functionality of log aggregation tool suites or capabilities such as SIEM tools

The SIEM system is a pivotal tool in this process. SIEM facilitates the centralization of data from various sources, including devices, applications, and endpoints. It enables:

- real-time and historical event monitoring
- detailed analysis and correlation of information
- enhanced threat detection and response capabilities

Key considerations for outsourcing

When considering outsourcing monitoring and reporting within MSP/MSSP, it's important to assess:

- the depth and frequency of monitoring services
- data storage strategies, including data residency considerations and security measures
- the provider's certifications, particularly in cyber security and compliance standards
- the ability of the provider to integrate its services with your existing security infrastructure, in the case where the provider is operating within the organization's premises

Recommended contract clauses

The Cyber Centre recommends that organizations include specific clauses related to monitoring, reporting, and availability when contracting a SOC to an MSP/MSSP. Below are examples of wording that your organization may wish to include in its contracts.

Monitoring

The Contractor must:

- provide continuous (24/7/year-round) monitoring of security events
- analyze security event data for incident investigation using system logs and other detection methods
- review and record audit logs for inappropriate or illegal activity to facilitate event reconstruction during security incidents
- investigate and accurately identify anomalies detected by security devices or reported by various stakeholders

Reporting

The Contractor shall:

- deliver actionable notifications, escalations and daily summary reports based on threat intelligence and security event analysis
- document all investigative activities and incident reports to support the organization's incident response framework
- provide comprehensive written reports of all security events, adhering to established procedures and reporting protocols
- provide the organization with the ability to contact the provider and open an investigation when suspicious activities occur

Availability

The Contractor shall ensure the continuous availability and operational integrity of all SOC systems and applications.

References

- Network security logging and monitoring (ITSAP.80.085)
- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137, Appendix D)

2.1.2 Incident support

Incident support is a vital component of a SOC-as-a-service (MSP/MSSP) model. Your organization and the MSP/MSSP must collaborate to manage incidents effectively. It is crucial to have an organizational incident response plan, detailing how your organization will detect, respond to, and recover from incidents. This plan should clearly define the SOC's role, including the extent of its involvement and the responsibilities of your organization’s internal team. The following two scenarios outline the key aspects of incident support, as well as sample contract clauses, for SOCs hosted in an MSP/MSSP environment (hosted outside of your organization’s tenancy) and for SOCs operating within an organization’s tenancy.

In both scenarios, it is vital to establish a partnership based on transparency, trust and shared responsibility for security outcomes. The contractual agreement should be detailed and clear, with specific attention to incident response, data protection, compliance, and service levels. This ensures that both the organization and the MSP/MSSP have a common understanding of their respective roles and responsibilities in securing the organization’s digital assets.

Scenario 1: SOC hosted outside your organization’s tenancy

If your SOC is hosted outside your organization’s tenancy, consider the following key aspects related to incident support.

- **Incident detection and notification**: The MSP/MSSP must promptly identify and notify the organization of security incidents. The agreement should specify the timeframe for notification following incident detection
- **Incident analysis and response**: The MSP/MSSP should provide detailed analysis of incidents, including potential impact, and execute agreed-upon response actions
- **Data protection and confidentiality**: The MSP/MSSP must adhere to strict data protection and confidentiality standards, especially since sensitive organizational data will be stored and processed in their environment
- **Access control and audit trails**: The MSP/MSSP must implement robust access control measures and maintain audit trails of all activities related to the SOC services
- **Compliance and regulatory requirements**: The MSP/MSSP must comply with relevant regulatory and compliance requirements and provide necessary documentation and support for compliance audits

Example contract clause for incident support

The Contractor shall:

- notify the Client within the negotiated or agreed-upon expected timeframe when detecting any security incident, providing detailed information about the nature, scope, and impact of the incident

- implement and maintain comprehensive data protection measures, in compliance with applicable laws and regulations, to safeguard the Client’s data against unauthorized access, disclosure, alteration, or destruction
- upon detecting an incident, commit to a [insert specified] uptime SLA and commence remediation actions within [insert specified timeframe]

Scenario 2: SOC operating within your organization’s tenancy

If your SOC is operating within your organization’s tenancy, consider the following key aspects related to incident support.

- **Integration with existing infrastructure**: The MSP/MSSP must seamlessly integrate its SOC services with the organization’s existing infrastructure, ensuring minimal disruption
- **Incident handling procedures**: The MSP/MSSP must define clear procedures for incident escalation, response, and resolution, tailored to the organization’s policies and procedures
- **Training and awareness**: The MSP/MSSP may be required to provide training, knowledge transfer or both to the organization’s staff on security awareness and incident response procedures
- **Performance monitoring and reporting**: Regular performance reviews and reporting are essential to ensure the SOC services meet the organization’s security requirements
- **Continuous improvement**: The contract should include provisions for continuous improvement of the SOC services, including regular updates to security tools and processes

Example contract clause for incident support

The Contractor shall:

- ensure that SOC services are fully compatible with the Client’s existing systems and infrastructure and shall be responsible for any modifications required for integration
- adhere to the Client’s incident response procedures and timelines, ensuring incidents are resolved in a manner that minimizes impact on the Client’s operations
- provide monthly performance reports detailing incident detection, response times, and resolution outcomes, including any recommendations for improving security posture

Refer to Developing your incident response plan (ITSAP.40.003) for more information.

2.1.3 Threat analysis and intelligence

Threat analysis and intelligence are critical components of a proactive cyber security portfolio. Accurate and timely intelligence empowers decision makers to make informed, data-driven decisions. The Cyber Centre, along with other resources, offers valuable insights through publications and active services, aiding organizations in their threat intelligence efforts. It’s essential for organizations to ensure their MSP/MSSP stays abreast of emerging and sophisticated cyber threats.

Key elements of threat intelligence

- **Continuous monitoring:** keeping track of evolving cyber threats and trends
- **Technical analysis:** analyzing incidents in detail to understand attack vectors and methodologies

- **Intelligence sharing:** utilizing shared resources for a more comprehensive threat landscape view

Example contract clauses for threat analysis and intelligence

The Contractor shall:

- detect, monitor, analyze, and mitigate targeted, highly organized, or sophisticated cyber threats
- maintain situational awareness of current cyber security activities and risks
- utilize various intelligence sources to develop insights into cyber threats and conduct advanced technical analyses of incidents on the organization's networks
- analyze consolidated threat data from multiple sources to provide early warnings of impending attacks against the organization's networks
- report on technical network and host-based attack vectors, emerging cyber threats, new vulnerabilities, and current trends used by malicious actors
- develop and maintain databases to catalog and track ongoing threats, enhancing the organization's defensive posture
- integrate intelligence findings into the organization's broader cyber security strategies and incident response plans

Incorporating comprehensive threat analysis and intelligence into MSP/MSSP offerings is crucial for organizations to stay ahead of cyber threats. The MSP/MSSP's role extends beyond mere monitoring; it involves deep analysis, continuous learning, and integration of intelligence into the organization's overall cyber security framework.

References

- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137, Appendix D)
- Baseline cyber threat assessment: Cybercrime
- National Cyber Threat Assessments

2.1.4 Documentation and standard operating procedures

SOPs and comprehensive documentation are crucial in ensuring that all parties involved in the SOC are aligned on methods and practices. These documents serve as a reference point for consistent and effective operations within the SOC, aiding in training and providing operational clarity.

Key documentation elements

- **Security deployment diagrams:** providing visual representations of security deployments for reference and to ensure understanding
- **Regular SOP updates:** updating SOPs with operational changes to ensure ongoing relevance
- **Performance and incident reporting:** providing insights into SOC activities, incident handling, and operational efficiency

Example contract clauses for SOPs and documentation

The Contractor shall:

- create and maintain diagrams for new or revised security deployments, covering all systems and applications related to the SOC
- develop and regularly update SOC SOPs, particularly following changes in SOC operations or technologies, deliver regular written reports, including:
  - daily, weekly, and monthly summaries of SOC activities
  - performance metrics and status of security incidents
  - actions accomplished and milestones reached during the reporting period
- submit comprehensive reports, encompassing
  - monthly status updates on progress and developments
  - planned activities, identified problems/issues with proposed solutions
  - anticipated delays and resources utilized during the period

It is essential to establish clear and detailed SOPs and documentation protocols to maintain operational excellence in a SOC environment. These documents not only guide daily operations, but also serve as critical tools for training, performance tracking, and strategic planning.

2.1.5 Additional capabilities: Advanced incident management support, forensics and malware analysis

In addition to standard incident management support, organizations often require or desire advanced capabilities such as forensics and malware analysis. These services are crucial for thoroughly investigating and resolving sophisticated cyber incidents, understanding attack vectors, and enhancing future security postures.

Key advanced support services

- **Forensics and malware analysis:** in-depth investigation of incidents to understand the nature and impact of compromises.
- **Reverse engineering and traffic analysis:** detailed examination of malicious software and network traffic to uncover threat methodologies.

Example contract clauses for advanced incident management support

The Contractor must:

- provide both on-site and remote computer security incident management, response, and recovery support as necessary
- conduct advanced technical analyses of potentially malicious activities using security event data from the SOC
- perform detailed endpoint/host-based forensics and memory analysis
- undertake triage and in-depth analysis of malware, including reverse engineering of Windows software, phishing emails, and other client-side exploits
- conduct digital forensics on media from compromised hosts to assess intrusion scope and nature

- reverse engineer the sequence of events in breaches or attacks for comprehensive understanding
- execute static and dynamic file analysis to identify malware characteristics, intent, and origin
- recommend countermeasures against malware and other malicious code exploiting the organization's systems
- propose changes to policies and procedures based on investigative findings to strengthen malware incident response
- perform advanced network traffic analysis at the packet level to identify anomalies, trends, and patterns

Advanced incident management support, particularly in forensics and malware analysis, is a critical component of a robust MSP/MSSP offering. These services not only aid in resolving current security incidents but also play a key role in refining organizational policies and strengthening the overall cyber security framework.

Refer to Developing your incident response plan (ITSAP.40.003) for more information.

2.1.6 Security technologies maintenance and operation

In an MSP/MSSP setup, managing key technologies, such as the SIEM system, intrusion detection and prevention systems (IDS/IPS), and data loss prevention (DLP) systems, is paramount. These technologies form the backbone of effective cyber security operations. Contracts should include specific clauses to ensure these tools are operated and maintained effectively, especially as the organization evolves and grows.

Key responsibilities for technology management

- **System maintenance and tuning:** regularly updating and tuning security systems to ensure accuracy and efficiency
- **Operational effectiveness:** ensuring continuous operation and optimal performance of all security technologies
- **Adaptability to change:** ensuring flexibility to adapt tools and systems to the changing needs and scale of the organization

Example contract clauses for technology management

The Contractor must:

- effectively maintain the SIEM to aggregate and analyze data from various sources like network sensors, firewalls, antivirus systems, and vulnerability scanners.
- handle administration, management, and configuration of all SOC tools, including SIEM, IDS/IPS, DLP, and other dedicated security systems
- develop and update security device signatures, performance reports, and relevant metrics to track system efficiency
- fine-tune the SIEM and IDS/IPS to minimize false positives and enhance detection accuracy
- continuously operate, manage, and update all security technologies, ensuring they are configured appropriately for optimal performance
- ensure that all relevant security feeds are logged and correlated effectively within the SOC's SIEM system
- install, update, or modify network security components and tools as needed to maintain comprehensive coverage and optimal performance in line with organizational growth

- install or modify network security components, tools, and other systems as required to maintain optimal coverage and performance

Effective management of key technologies within an MSP/MSSP framework is essential for maintaining a robust cyber security posture. This includes not only the operational maintenance of these tools but also improving and adapting them to meet the evolving needs of the organization.

3 Vendor readiness

When contracting with an MSP for SOC services, it’s crucial to include specific clauses that ensure the vendor can provide services at the required scale and meet certain standards. These clauses help verify the provider's experience, compliance with legal requirements, and readiness to handle your organization's specific needs.

Key contract clauses for vendor readiness

- **Experience requirements:** The contractor should have a minimum number of years of experience in providing SOC services and engagements of similar size, scale, and complexity
- **Compliance with Canadian laws:** The contractor should have experience in delivering services within Canada and adhering to Canadian privacy and data laws
- **Audit and compliance rights:** The organization reserves the right to perform SOC visits for audit, review, and compliance purposes
- **Business continuity planning:** The contractor must have a robust business continuity plan (BCP) for its SOC to ensure service continuity
- **Certification requirements:** The contractor must meet any industry or sector certification requirements, for example, SOC2 Type2, ISO 27001, CIS CSC, Cloud Security Alliance (CSA) Tier2, ISO 27017
- **Staff clearances and background checks:** The contractor’s personnel should have necessary clearances and background checks (as required)
- **Cyber security controls framework alignment:** Recognized cyber security controls frameworks must be implemented at SOC facilities (DRI Institute, NIST)
- **Liability and compensation:** The contractor should provide clarification on shared responsibilities for breaches and details on the provider’s liability insurance coverage for compensation

Including these key clauses in your contract with an MSP for SOC services is essential to ensure that the provider is fully prepared and capable of meeting your organization's specific requirements. These clauses cover a range of critical areas, from experience and legal compliance to business continuity and cyber security frameworks, ensuring a comprehensive approach to vendor readiness.

4 Terms and conditions

From a security perspective, contract elements must be prescriptive and conform to recognized frameworks and approaches for the MSP/MSSP to establish how it addresses and maintains the security posture as indicated by an organization. In many cases, relying on a given provider's terms and conditions, as outlined in a contract or end user licensing agreement (EULA), can be considered acceptable. However, if organizations have specific needs or are bound by regulated authorities, negotiation may be required between legal teams using some of the example clauses provided in this document. If you are concerned about any specific areas, seek legal advice where possible.

Organizations should carefully consider and, if necessary, consult with their legal counsel on the following areas when negotiating contracts with service providers:

- **Trade secret protections**
  - Inquire how the service provider will separate or secure trade secrets (e.g., patented material, legal branding, etc.) within its system
  - Ensure terms and conditions stipulate that the organization retains ownership and control over its trade secrets, even when placed with the service provider
- **Intellectual property**
  - Discuss measures for tagging, identifying, and securing intellectual property, which may not be officially registered like patents but is crucial to the organization's operations
  - Clarify in the contract that intellectual property remains the property of the organization, regardless of its placement with the service provider
- **Indemnification/limitation of liability:** Define the level of liability and responsibility in the contract, considering complexities that may arise, especially when multiple service providers are involved
- **Support model considerations**
  - If your organization is subject to regulatory constraints on support locations or resource residency, discuss and agree on support models with the service provider
  - Consider how the provider's global support model, like a “follow the sun” approach, aligns with regulatory requirements.
- **Data migration policies:** Address potential future needs for data migration, including
  - costs associated with data ingress and egress
  - timeframes and processes for migration activities
  - data retention policies post-migration
- **Conformity with security frameworks**: Ensure that contract elements conform to established cyber security frameworks and best practices
- **EULA versus custom contracts**: While standard terms outlined in an EULA might be acceptable for general purposes, they may not suffice for organizations with specific security needs or those under stringent regulatory requirements.
- **Legal negotiations for custom needs**
  - For organizations with unique requirements or regulatory obligations, negotiations between legal teams are often necessary to tailor the contract appropriately

  - The example clauses provided in this document can guide these negotiations
- **Seeking legal advice**
  - The organization should seek legal counsel, particularly if there are specific areas of concern or if the organization operates under regulated authorities
  - Legal expertise can ensure that contracts are comprehensive, compliant, and tailored to the organization's unique needs

When contracting with a service provider, especially in areas such as MSP/MSSP, organizations must ensure that specific legal and operational considerations are clearly addressed in the contract. This includes retaining ownership of intellectual property and trade secrets, clearly outlining liability terms, understanding support models in the context of regulatory constraints, and preparing for potential data migration. Organizations should consult legal counsel to ensure that these aspects are adequately covered to protect the organization’s interests.

5 Summary

A SOC combines people processes and technology to improve an organization’s resilience against cyber threats.

Whether this is done by an in-house team in a dedicated room within an organization or whether it is fully or partially outsourced to a team of information security professionals, SOCs are a first line of defence that is critical for preventing, detecting, and recovering from cyber attacks.

This is especially true given the increase in operational technology, mobile and cloud technology, and industrial control systems. Whether work is in-house, hybrid, or fully remote, your organization will require the same inputs and outputs to your SOC. The guidance included in this document should help your organization write contract clauses that ensure your providers are meeting your expectations. As indicated, this is not to be taken as legal advice.

Overall, the key message is that your organization should work with its selected MSP/MSSP provider to ensure common understanding and to also inquire and establish what can be done to meet your organization’s specific needs.