Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Cyber Security Considerations For Consumers of Managed Services

MANAGEMENT

TLP:WHITE

Canada

FOREWORD

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

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

EFFECTIVE DATE

This publication takes effect on October 14, 2020.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	October 14, 2020

OVERVIEW

This document introduces different security topics that you should consider before and during the process of procuring managed services. Each section of this document includes a checklist of actions you should take and questions you should ask a service provider before signing up for the service.

You can use this document as a starting point when discussing service security in your organization. We have included considerations that can help you articulate your business and security requirements and the service levels that you expect when using managed services.

For more information, phone or email our Contact Centre:

Contact Centre
contact@cyber.gc.ca
613-991-8700
Toll-Free: 1-833-CYBER-88 (1-833-292-3788)

TABLE OF CONTENTS

1 Introduction 6
1.1 Managed Services 7
2 Security Considerations For Consumers 8
2.1 Data Security 8
2.2 Legal and Regulatory Compliance 11
2.3 Service Provider Assessments and Audit Reports 13
2.3.1 Service Provider Assessments 13
2.3.2 Security Control Audit Reports 14
2.4 Access Control 15
2.4.1 Access Control Policy 15
2.4.2 System Administrators and Physical Access to Servers 16
2.4.3 Password Policy 17
2.4.4 Federated Authentication 18
2.5 Encryption 19
2.5.1 Encryption in Transit and At Rest 19
2.5.2 Key Management outside Consumer Infrastructure 20
2.6 Incident Response 22
2.6.1 Event Logging Support 24
2.7 Business Continuity and Disaster Recovery 26
2.7.1 Redundancy 26
2.7.2 Disaster Recovery 27
2.8 Supply Chain Integrity 28
2.9 Data and Service Portability 29
2.10 Data Destruction 30
3 Supporting Content 31
3.1 List of Abbreviations 31
3.2 Glossary 32
3.3 References 33

LIST OF TABLES

Table 1: Consumer Activities Related to Data Security 9
Table 2: Consumer Activities Related to Legal and Organizational Compliance 12
Table 3: Consumer Activities Related to Service Provider Assessments 13
Table 4: Types of SOC Reports for ISA-3402 Compliance 14
Table 5: Questions Related to Security Audit Reports 14
Table 6: Consumer Activities Related to Access Control 15
Table 7: Consumer Activities Related to SAs and Physical Access to Servers 16
Table 8: Consumer Activities Related to Password Policies 18
Table 9: Consumer Activities Related to Federated Authentication Mechanisms 19
Table 10: Consumer Activities Related to Encrypting Data in Transit and Data at Rest 20
Table 11: Consumer Activities Related to Key Management 21
Table 12: Consumer Activities Related to Incident Response 23
Table 13: Consumer Activities Related to Event Logging Support 25
Table 14: Consumer Activities Related to Redundancy 26
Table 15: Consumer Activities Related to Disaster Recovery 27
Table 16: Consumer Activities Related to Supply Chain Integrity 28
Table 17: Consumer Activities Related to Data and Service Portability 29
Table 18: Consumer Activities Related to Data Destruction 30

1 INTRODUCTION

Small or medium businesses may want to use service providers to remotely manage their organizations' information technology (IT) infrastructure, cyber security, and other related business operations. However, managed service providers (MSPs) are attractive targets for cyber criminals because they have access to numerous client systems and a lot of data. If an MSP is compromised, their clients are also vulnerable; a compromise can result in stolen proprietary information and disrupted business operations, which can result in financial loss and potential harm to an organization's reputation.

You can use this document to help your organization determine whether an MSP has the capabilities to deliver services effectively and securely. This document introduces some security topics that you should consider before and during the process of procuring managed IT services. These topics include the following:

- Data security;
- Legal compliance;
- Service provider assessments;
- Access control;
- Encryption;
- Incident response;
- Business continuity and disaster recovery;
- Supply chain integrity;
- Exit strategies; and
- Data destruction.

Your organization and the MSP both have roles when it comes to protecting systems and data. Your organization is the data owner and is **legally responsible** for data security. Therefore, it is critical that you explicitly define your organization's security requirements and ask an MSP the right questions before you sign on to use a service. Having this information will ensure that you define an effective service level agreement with the MSP.

For an overview on some best practices when contracting an MSP, see *Cyber Security Best Practices: Contracting with Managed Service Providers* [1][1].

[1] Numbers in square brackets indicate a reference that is cited in the Supporting Content section of this document.

1.1 MANAGED SERVICES

An MSP is a company that remotely manages IT infrastructure and user end systems on behalf of a client. According to the MSP Alliance, MSPs typically have the following distinguishing characteristics:

- Provide some form of network operation centre (NOC) service and help desk service;
- Monitor and manage remotely all or most of the objects for the client;
- Maintain proactively the objects under management for the client; and
- Use some form of predictable billing model (i.e. client has an accurate total amount for regular IT management expenses).

Note that there are differences between cloud services and managed services. The main difference revolves around who has control over the data and the processes. With managed services, the **consumer** (e.g. your organization) dictates the technology and operating procedures. However, with cloud services, the **service provider** dictates both the technology and the operational procedures available to the consumer (e.g. your organization).

In this document, we assume that your organization will use at least some infrastructure in the cloud.

2 SECURITY CONSIDERATIONS FOR CONSUMERS

For each topic covered in this section, we include a description to provide you with more context, an explanation of why the topic is important, and a checklist of activities and questions to help you determine whether an MSP is right for your organization. Depending on your organization's business needs, some of the security topics may be more relevant than others.

Note that this document does not help you identify your organization's business requirements. Your business requirements are specific to your organizational environment and circumstances.

2.1 DATA SECURITY

Before contracting potential service providers, you should identify the data that will be accessible to the service provider and the sensitivity level of that data. By understanding your data and its sensitivity, you can identify the security controls that are required to protect it appropriately.

Data sensitivity is measured by the impact a compromise would have on your organization's ability to achieve its mandate. Data sensitivity is categorized as high, medium, or low:

- **High (H)**: Compromise has a critical or a prohibitive impact on your organization's ability to achieve its mandate;
- **Medium (M)**: Compromise has a major impact on your organization's ability to achieve its mandate; or
- **Low (L)**: Compromise has a moderate impact on your organization's ability to achieve its mandate.

Data sensitivity considers the compromise's impact on the data's confidentiality, integrity, and availability, which are the three pillars of IT security. Confidentiality protects information from unauthorized disclosure. Integrity protects information from unauthorized changes. Availability ensures that information is available when it is required. You should apply values of high, medium, and low for each of these three areas to construct a three-part *data security profile*.

For example, consider a data set that has a data security profile of H/M/L. You can interpret the three parts of the data security profile in the following ways:

1. A **data confidentiality compromise** (H) has a critical or prohibitive impact on your organization's ability to achieve its mandate;
2. A **data integrity compromise** (M) has a major impact on your organization's ability to achieve its mandate; and
3. A **data availability compromise** (L) has a moderate impact on your organization's ability to achieve its mandate.

Note that data classification can be time sensitive. For example, the sensitivity of election result data is much higher the day of an election than the day after. We recommend that you classify your data based on the highest level of expected injury that could result if that data is compromised. See Annex 1 of *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2] for more information on classifying and categorizing your data.

Table 1: Consumer Activities Related to Data Security

Number	Consumer Activity	Check
1	Define what *high, medium,* and *low* sensitivity means to your organization. **Note:** Refer to the generic definitions in section 2.1.	
2	Identify what information your organization is protecting (i.e. information about organizational strategy, personal data about Canadians, financial transactions). **Note**: You may want to group the data as follows: Data that is accessible to the public, operational data, trade secrets. Identify who (role) needs access to this data.	
3	Determine where the data is stored (i.e. internally, with the service provider).	
4	Identify highly sensitive data. **Note:** To protect highly sensitive data, you want to ensure that you are storing this data in your organization's infrastructure and not with a service provider. We recommend that your organization analyzes the risk of storing highly sensitive data outside of its infrastructure to determine whether it is an acceptable risk. Refer to section 2.3.1 for further details.	
5	Determine whether a potential data compromise would impact national security interests. **Note:** We recommend that you only store data that has a national security interest on your organization's trusted infrastructure and ensure that the proper security controls are in place to protect that data.	
6	Review Annex 4a of ITSG-33 [2] for a sample security profile for an M/M/M profile. **Note:** Your organization needs to tailor the controls in this profile to reflect the results of this checklist and meet your organization's specific requirements.	
7	Create a grid that lists each data group along the y-axis. Along the x-axis, list confidentiality, integrity, and availability. Apply the rating of high, medium, and low. Each three-part rating represents the classification of data. **Note:** See Figure 1 for a simple example of a data grid.	

Data Group	Confidentiality	Integrity	Availability	Who Needs Access	Storage Location
Data group A	High	High	High	System admin	Internal network
Data group B	Medium	High	Medium	Finance	Service provider
Data group C	Medium	Low	Low	Users Guest	System provider

Figure 1: Sample Data Grid

2.2 LEGAL AND REGULATORY COMPLIANCE

When data is stored outside of your organization's infrastructure, you need to know where it is stored (i.e. the geographical location). Data stored outside of Canada is subject to different privacy, security, and data ownership laws and regulations. Depending on the industry or the sector to which your organization belongs, the data may also be subject to different regulations and standards that govern the data's retention, disclosure to third parties, and chain of custody.

Canada's privacy laws (i.e. the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* [PIPEDA]) align with the European Union's (EU) privacy laws (e.g. *General Data Protection Regulations* [GDPR]). In Canadian and EU legislation, organizations must ask individuals for permission to collect their personal data. In Canada and the EU, individuals also have the right to be forgotten[2]. Other countries may view privacy differently and do not comply with the GDPR, which can interfere with the confidentiality of your organization's data.[3]

If data is stored outside of Canada, different laws (e.g. national security priorities) may take precedence over Canadian privacy laws. If you are using managed services that store data outside of Canada, you should review the applicable laws and the possible impacts to privacy. This precedence can interfere with the availability of consumer data if a security threat or a legal case occurs.

In the *IT Policy Implementation Notice: Direction for Electronic Data Residency* [3], the Treasury Board of Canada Secretariat (TBS) requires that sensitive data[4] collected or processed by the Government of Canada (GC) is stored within the geographical boundaries of Canada or within the premises of a GC department located abroad (e.g. Canadian consulate). This requirement ensures that the GC can maintain continuous access to the data for business continuity.

If your organization is a non-GC organization, we recommend that you ensure all sensitive data (M/M/M or above) is stored only in data centres located within the geographical boundaries of Canada. Additionally, various industries have specific compliance standards and directives, such as audit regulations, that require standard data retention periods. Your organization is responsible for determining whether or not a prospective MSP adheres to these requirements.

If your data is stored outside of your organizational premises or infrastructure (i.e. in a cloud infrastructure), it is critical to ensure that your organization retains legal ownership. Your organization is legally responsible for the privacy of data. Ensure that you can maintain control of this data by maintaining ownership within a cloud infrastructure. Ask your provider!

---

[2] The *right to be forgotten compels organizations that collect personal information to delete an individual's information when that individual requests them to do so.*

[3] Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the US are all non-EU countries that have data protection laws that the EU considers adequate. However, note that US privacy laws are industry-specific and do not comply with the GDPR. But the EU-US Privacy Shield designation, which replaced Safe Harbour, ensures that US companies can conduct business in the EU.

[4] Data that is profiled at the M/M/M level or above and data that relates to national security.

Table 2: Consumer Activities Related to Legal and Organizational Compliance

Number	Consumer Activity	Check
1	Refer to the data sensitivity levels (high, medium, low) in section 2.1. Does your organization have data that is classified at the medium or high sensitivity level? If so, we recommend that you store data within the geographical boundaries of Canada.	
2	Review the *Privacy Act* (GC organizations) or PIPEDA (non-GC organizations) and any industry-specific regulations to determine your organization's requirements for handling and protecting personal information.	
3	Determine your data retention policy. **Note:** Retention periods depend on the business functions that the information relates to (e.g. keep tax records for a period of six years from the end of the last tax year they relate to) and whether this information is considered transitory or of business value. Transitory information is information that serves solely as a convenience copy. Information of business value is information that is required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to provide evidence.	
Questions to Ask the Service Provider		
1	Can the service provider support the storage of your sensitive data within the geographical boundaries of Canada?	
2	Can the service provider adhere to requirements derived from industry-specific security guidelines and directives (e.g. data retention, audits, and destruction)?	
3	Does your organization retain legal ownership of the data stored in the service provider space?	
4	When the data is stored outside of your organization's infrastructure, can the service provider support your data retention requirements?	

2.3 SERVICE PROVIDER ASSESSMENTS AND AUDIT REPORTS

Once you have classified your organization's data, you can compare your organization's security control requirements with the service provider's ability to apply adequate safeguards to that data.

2.3.1 SERVICE PROVIDER ASSESSMENTS

Service providers can be assessed against recognized security standards and frameworks to determine their capabilities in terms of protecting sensitive data. Some examples of security standards and frameworks include:

- International Organization for Standardization (ISO) – ISO270001/2 [4];
- Information Systems Audit and Control Association (ISACA) – Control Objective for Information and Related Technologies (COBIT) [5];
- Cloud Security Alliance (CSA)– Security Trust Assurance and Risk (STAR) [6];
- National Institute of Standards and Technology (NIST) – Risk Management Framework [7]; and
- Our ITSG-33 [2].

We developed service provider assessment programs, which support TBS's Contract Security Program. We conduct these assessments by using recognized security frameworks to evaluate the security capabilities of service providers and their abilities to protect Canadians' sensitive data.

Table 3: Consumer Activities Related to Service Provider Assessments

Number	Consumer Activity	Check
1	Determine whether you are procuring services from an MSP, a CSP, or both. Refer to the definitions in section 1.1.	
2	Contact us to determine if the service provider has been evaluated by our CSP or MSP assessment programs. **Note:** You will need to understand the sensitivity of your data to request assessment results. If we have not assessed the service provider, you may wish to consider the following activities: • Ask the service provider whether they have been evaluated by a third party against any security standards (e.g. ISO270001/2, COBIT, ITSG-33, NIST, CSA). • Hire a third party to carry out an assessment of the service provider against ISO 27001/2, the CSA's STAR or similar standards.	
Questions to Ask the Service Provider		
1	Can the MSP produce a certificate of evaluation from a third party against security standards (e.g. ISO 270001/2 or COBIT)?	
2	Who are the MSP's suppliers? **Note:** The response to the question will enable you to conduct an independent assessment.	

2.3.2 SECURITY CONTROL AUDIT REPORTS

The *International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization* (ISAE 3402) [9][5] is an auditing standard for the controls used by service organizations. This standard ensures that adequate security controls are in place for accurate financial reporting. A third party audits the service provider's controls to produce service organization controls (SOC) reports to demonstrate the service provider's compliance with ISAE-3402. These reports can be used to determine the effectiveness of the design and the implementation of technical and non-technical security controls. See below for descriptions of SOC 2 and SOC 3 reports.

Table 4: Types of SOC Reports for ISA-3402 Compliance

Report	Description	Relevance
SOC 2	Evaluates an organization's information systems that are relevant to security availability, processing integrity, confidentiality, or privacy. There are two types of SOC 2 reports: Type 1: Control design Type 2: Control implementation effectiveness	SOC 2 Type 1 assesses the design of security controls (i.e. a single point in time). SOC 2 Type 2 assesses the effectiveness of implemented security controls over time (i.e. a period of 6+ months). The SOC 2 Type 2 tends to be the most sought after, but the service provider is less likely to release it, as it contains sensitive information on how they protect data. This information, in the wrong hands, can provide security posture details and be used to compromise a system. If the MSP is willing to share the report, it is likely to be shared under a non-disclosure agreement (NDA).
SOC 3	Attestation that the SSAE-16 standard is met. Does not provide insights into the controls that are tested.	A service provider is likely to provide this report. It confirms compliance without providing details on the controls used.

Table 5: Questions Related to Security Audit Reports

Number	Questions to Ask the Service Provider	Check
1	Has the service provider been audited by an independent third party to verify compliance with ISAE-3402? Can they provide SOC 3 attestation?	
2	Is the service provider willing to share their SOC 2[6] reports (Type 2) if you agree to sign an NDA?	

[5] The ISAE-3402 international standard is mirrored by the SSAE-16 US standard.

[6] To protect their own security, service providers may not provide SOC 2 reports, even with an NDA in place. In this case, your organization must rely on other means of verification, such as our MSP and CSP assessments programs.

2.4 ACCESS CONTROL

Access control (e.g. an access control policy) determines who can access your organization's data, systems, and networks. In this context, access control should align with the confidentiality and integrity pillars of the data sensitivity profile described in section 2.1.

Your organization's access control policy should persist when you use managed services, regardless of whether the data is stored on site or in the cloud. When using managed services, your organization and the service provider must agree on the roles and responsibilities related to access control. You must also define the authentication and authorization mechanisms, which are two elements of access control. Authentication refers to any process or measure that is used to verify a user's identity, and authorization refers to access privileges that are granted to a user, program, or process.

2.4.1 ACCESS CONTROL POLICY

Your organization is responsible for your access control policy. You must clearly define all access control requirements to the service provider so that you can determine whether they can support these requirements. Access control should be based on the **principle of least privilege**, meaning that individuals should only have the privileges that they need to perform their work functions. Service providers should only have the access that enables them to effectively manage their services.

Table 6: Consumer Activities Related to Access Control

Number	Consumer Activity	Check
1	If your organization does not have an access control policy, you should define your requirements, including: • Who can access the data and what types of data can be accessed? (Refer to Figure 1). • How will privileges be applied (e.g. roles, discretionary access, labels)? How will changes to access control be managed?	
2	Determine any other access control requirements (based on the principle of least privilege), such as account reviews when personnel change jobs or leave, separation of duties, etc.	
3	Construct an access control matrix that uses rules or roles to link resources to objects. For example, create a table that distinguishes administrative roles, such as system administrators and application administrators. Ensure that privileges are maintained and align with any changes in roles or job functions (e.g. if someone no longer requires administrative privileges).	
Questions to Ask the Service Provider		
1	Can the MSP support your organization's access control policy, including how privileges are assigned and how change is controlled?	
2	What network and system access does the service provider require to perform their services?	
3	What data does the service provider require to perform their services?	
4	Can your organization manage access controls (e.g. account provision, revocation, maintenance) in the MSP's service space?	

5	Does the service provider support self-service password recovery?	
6	How does the service provider support access control (e.g. tools, help line)?	

2.4.2 SYSTEM ADMINISTRATORS AND PHYSICAL ACCESS TO SERVERS

System administrators (SAs) pose a large risk to data; SAs can access multiple clients and may have physical access to client servers. Examples of other personnel who may have physical access to servers include facility maintenance staff and external hardware and software maintenance staff. If managed services are deployed outside of your organization's infrastructure, you should consider other standards that address the ways in which you can effectively limit access to physical servers for administrators or other personnel.

Table 7: Consumer Activities Related to SAs and Physical Access to Servers

Number	Consumer Activity	Check
1	Consult the MSP's evaluation and security control audit reports; with these reports, you can identify service provider controls to limit or control SAs' access to your data.	
Questions to Ask the Service Provider		
1	How is your organization's data protected against unauthorized access (read or modification) by SAs?	
2	Are SAs screened (e.g. appropriate clearance level) before they can access your cloud space?	
3	Where are the SAs located? Are they in Canada where they are subject to Canadian laws?	
4	Are SAs required to sign NDAs?	
5	Do SAs have read-only rights to auditing functions?	
6	Can the MSP provide an audit trail of all administrator actions for incident response and general audit purposes?	
7	Do audit logs track individual SA actions?	
8	Do SAs have corporate user accounts (used for general user functions) and separate administrator accounts (used when they need elevated privileges to perform a task on behalf of your organization)?	
9	How does the MSP manage physical access and accountability to servers?	
10	Does the MSP limit or prevent local administrator access on an individual physical server?	
11	What are the physical access requirements to access the data centre and the server cages? Is the data centre shared?	
12	Does the MSP use external vendors to perform system or software maintenance? If so, which physical controls are used by the MSP to manage third-party access (e.g. escort individuals, clear these individuals to certain security level)?	
13	Does the MSP require that administrators and support staff take security training? Do they have to retake this training at regular intervals (e.g. annually)?	

2.4.3 PASSWORD POLICY

If an MSP provides services within your organization's infrastructure, the MSP must align with your access control structure (i.e. authentication and authorization). However, if an MSP provides services outside of your infrastructure, such as in a cloud infrastructure, you should ensure that the MSP supports authentication mechanisms that are appropriate to the classification level of the data being stored.

In a traditional on-premises IT infrastructure, it is your organization that dictates a minimum password policy (e.g. complexity, maximum time between mandatory password changes, use of passphrases). Passphrases and passwords must conform to this policy. With managed services, your organization and the MSP should agree on a password policy that meets or exceeds your existing password policy.

You need an effective password policy to prevent threat actors from easily guessing or cracking passwords. Although users may find it onerous to create passphrases and complex passwords, we recommend that you review the minimum practices defined in *ITSAP.30.032 Best Practices for Passphrases and Passwords* [10]. We find that the following standards produce the best deterrent effect:

- Passphrases should be at least 4 words and 15 characters long;
- Passwords should be at least 12 characters long; and
- Passcodes and PINs should only be used if you cannot use passphrases and passwords;
    - Use randomly generated PINs where available.

Two-factor authentication (2FA) uses a combination of two different authentication factors when you access an account, making it more secure. The authentication factors should include at least two separate factor types:

- **Something you know** (e.g. a password or PIN);
- **Something you have** (e.g. a token or a smartcard); and
- **Something you are** (e.g. a biometric, like a fingerprint).

Note that an authentication process that requires a password and a PIN is not true 2FA because both are a single factor type (i.e. something you know).

Because of the widespread nature of phishing attacks and password theft, many services, including most social media platforms, have added 2FA options. We strongly recommend that you use 2FA for these platforms, especially for important public-facing accounts.

Table 8: Consumer Activities Related to Password Policies

Number	Consumer Activity	Check
1	Review and define your organization's password policy, considering our recommendations on passphrases and complex passwords.	
Questions to Ask the Service Provider		
1	Can the service provider support your organization's password policy? If not, what is the MSP's policy and is it effective?	
2	Can the provider support 2FA as a requirement for accessing your data? Which authentication methods are supported?	

2.4.4 FEDERATED AUTHENTICATION

In an on-premises IT infrastructure, passwords are used and stored internally only. However, when identity is verified in the cloud, some of, or all, your infrastructure authentication services (including usernames and passwords) may exist outside your organization's internal IT infrastructure. Passwords are the "keys to the kingdom" because they are used to control access to your organization's data. Passwords need to be protected appropriately. As a best practice, passwords that reside outside your organization's trusted space must never be stored or transmitted in plaintext. Additionally, no entity outside of your organization should both hold your data and the credentials to access that data.

We recommend that you use federated identity, which works in the following way:

1. You enter a password to access resources that are stored outside of your organization's infrastructure;
2. An authentication mechanism hashes this password and sends the hash to a third-party federated service, which holds your organization's (encrypted) passwords;
3. The federated service performs a hash function on the stored password and compares this hash against the hash received to validate that they match;
4. The federated service generates a certificate (or token) if the hashes match; and
5. The certificate is sent to the service provider, authenticating you and authorizing your access to the appropriate resources.

A cloud provider may offer authentication services, but this is not true federation as they do not leverage a third party. These services can present a risk because the cloud provider can access both your credentials and your data. However, this can be a reasonable risk if the cloud provider has internal processes to isolate the authentication process from your data, protecting against possible exploits. You should ensure that, if the provider offers authentication services, they can attest that their authentication services are appropriately isolated from your data.

Table 9: Consumer Activities Related to Federated Authentication Mechanisms

Number	Consumer Activity	Check
1	Review your current authentication process, if applicable.	
2	Determine your minimum encryption requirements when storing passwords with a third party. See section 2.5 for GC encryption guidelines.	
3	Request a walkthrough of the service provider's authentication process.	
Questions to Ask the Service Provider		
1	Does the service provider support federated authentication via a third party?	
2	Alternatively, does the service provider offer authentication services?	
3	If the service provider offers authentication services, can the provider attest that they isolate authentication services (i.e. usernames and passwords) from your data?	
4	Does the service provider support your minimum encryption requirements for passwords?	
5	Which standards on hashing and salting are supported by the cloud provider? **Note:** Salting refers to adding characters to a password to achieve a standard length, further obscuring its true value.	

2.5 ENCRYPTION

Encryption uses a random string of bits (i.e. an encryption key) to convert readable information into unreadable cipher text. Encryption hides the contents of sensitive data to prevent unauthorized access. Encryption is the key mechanism to protect the confidentiality of data in transit over the Internet and data at rest. Therefore, encryption aligns with the confidentiality pillar of the data sensitivity profile (i.e. M/M/M as defined in section 2.1).

Your organization is the data owner and is legally responsible for protecting the privacy of your organization's sensitive data. You must decide which level of encryption to use. You also need to ensure that the MSP can support your selected level of encryption and that the MSP has controls in place so that no one outside your organization can access both your encrypted data and the associated encryption keys to decrypt the data.

2.5.1 ENCRYPTION IN TRANSIT AND AT REST

With sensitive data, you must ensure that you apply measures that protect data in its various states, such as when it is in transit and at rest. **Data in transit** is data that is active and moving from location to another, such as across the Internet or within a private network. **Data at rest** refers to data that is inactive. In this state, your data may reside in databases, data warehouses, spreadsheets, archives, back-ups, and mobile devices. You should consider which encryption levels to use for data in transit (e.g. HTTPS web traffic) and data at rest (e.g. the encrypted contents in storage at a data centre).

Table 10: Consumer Activities Related to Encrypting Data in Transit and Data at Rest

Number	Consumer Activity	Check
1	Review *ITSAP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information* [11]. This publication includes recommendations for encrypting data at rest that is categorized up to a medium sensitivity level (i.e. M/M/M). For encryption recommendations for highly sensitive data, email or call our Contact Centre.	
2	Review *ITSP.40.062 Guidance on Securely Configuring Network Protocols* [12]. This publication provides recommendations for encrypting data in transit that is categorized up to a medium sensitivity level (i.e. M/M/M). For encryption recommendations for highly sensitive data, email or call our Contact Centre.	
Questions to Ask the Service Provider		
1	Does the MSP support encryption (specifically AES or 3DES) for data at rest, as per the encryption minimums recommended in ITSP.40.111 [11]?	
2	Does the MSP support encryption for data in transit (specifically TLS 1.2 or HTTPS), as per the encryption minimums recommended in ITSP.40.062 [12]? **Note:** HTTPS is recommended as opposed to HTTP, which does not include encryption for web traffic. TLS 1.2 should be used because TLS 1.1 and SSL are retired given known vulnerabilities.	
3	Does the MSP support a level of encryption that is sufficient for password storage (recommendations in ITSP.40.111 [11])?	

2.5.2 KEY MANAGEMENT OUTSIDE CONSUMER INFRASTRUCTURE

Encryption is the predominant security control that is used to protect the confidentiality of data. However, note that if you lose control of the encryption keys (i.e. the random string of bits used to encrypt and decrypt data), you lose control of the data. In best practice, keys should be stored in your organization's trusted, internal infrastructure only. However, to manage encryption keys, your organization needs to manage infrastructure that can be expensive and have staff who specialize in key management. For smaller organizations, this is rarely feasible.

Service providers often have sound key management infrastructure and appropriate policies to lock down access. You can request to review the MSP's key management capabilities. Keep the following considerations in mind:

- Resources outside of your organization should never have access to both your data and the keys used to decrypt this data. Access control policies and mechanisms should be in place to ensure that encryption keys are isolated from the data they protect.
- Encryption keys should never exist in plaintext outside of your organization's trusted infrastructure. Encryption keys should be encrypted at rest, at the same level, or higher, than the data they are protecting.

Remember that your organization always has an option. You can use a third party to manage encryption keys if the MSP's key isolation policy is insufficient for your needs. This may add complexity to service level negotiations but would be worth it to keep your data safe.

Table 11: Consumer Activities Related to Key Management

Number	Consumer Activity	Check
1	Determine your requirements to secure encryption keys (e.g. keys should be encrypted at the same sensitivity level or greater than the data you are protecting).	
2	Determine your organization's capability to manage keys (e.g. is it feasible and preferable for your organization to manage them?).	
3	Request to review the MSP's policies that support key management and access control.	
4	Request a walkthrough of the key management process with the service provider to verify that the process is secure.	
5	Contact us to review the MSP's Service Provider Evaluation, which can help you determine whether the MSP has the appropriate key management capabilities.	
6	Determine whether it is feasible or preferable to use a third-party key management service.	
Questions to Ask the Service Provider		
1	Does the service provider support the backing up of encryption keys?	
2	Who has access to your encryption key back-ups?	
3	What level of encryption is used to protect stored encryption keys?	

2.6 INCIDENT RESPONSE

Even with security controls in place, incidents can still happen. A security incident is any intentional or unintentional damage, theft, or unauthorized access that has a direct or indirect impact on the security of your organization's systems or services. Incidents can impact the provisioning or the security of a service, causing unplanned business interruptions. An incident may be caused by one of the following examples:

- Data breach;
- Theft or loss of assets;
- Malicious code;
- Network scans;
- Denial-of-service attacks;
- Fraud; or
- Server failure.

When an incident occurs, your organization needs to respond quickly to minimize the resulting damage. A general incident response plan includes steps to identify, contain, remediate, and communicate the issue. When an incident occurs, it can be identified by your organization (e.g. usability issues with a service) or by the service provider (e.g. a back-end issue). Because of this, you need to ensure that you have an effective communication path and that you can support each other.

When you use a service provider, your organization remains accountable for incident response, even if your organization is not solely responsible for implementing all steps of the incident management process. You should work with the service provider to coordinate an incident response plan. In this response plan, you should separate the roles and responsibilities of your organization and the service provider. A service provider may offer similar services to many customers. As a result, the service provider's priorities will differ from your organizational priorities. For example, your organization might experience an issue that is catastrophic to your business and that requires an immediate response. However, your request for an immediate response may sit in the service provider's queue because they are busy supporting many other organizations with multiple critical issues.

You must establish clear requirements for incident response, and you should ensure that the service provider can support your requirements. We recommend that you work with the service provider to define and agree upon expectations related to the level of service your organization requires. Your service level agreement with the service provider should specify the expected turnaround times, communication media, escalation processes, metrics for assessing performance, and penalties for not meeting turnaround times.

Incidents can occur repeatedly, which can indicate a more significant problem. When procuring managed services, it is important to ensure that the service provider has a capability to report on incidents over time so that underlying problems can be identified. An example could be data spills involving sensitive data. If this occurs once or infrequently, incidents can be managed individually. However, if data spillage occurs numerous times, then there may be a more significant problem, which may justify costs to revamp security training to address data spillage or to implement measures such as data loss prevention (DLP) or cross-domain solutions (CDS).

Table 12: Consumer Activities Related to Incident Response

Number	Consumer Activity	Check
1	Review your organization's incident management process and identify how this process will be impacted by using managed services.	
2	Review the Information Technology Infrastructure Library (ITIL) incident management process. ITIL is a framework that defines and describes best practices for delivering IT services. ITIL defines standard incident management steps, definitions, and terminology, which will provide a baseline to define roles and responsibilities for incident response.	
3	Establish your incident response requirements so that you can ensure that you continue to meet your business needs and operational requirements. You should define your requirements for monitoring, detecting, analyzing, containing, responding, recovering, and following up on incidents. Consider the following: • Define what constitutes an incident; • Identify incident types; • Prioritize the incident types; • Assign a team lead who manages the incident response process; and • Define timelines for sending incident notifications to staff, service provider, and vendors. **Note:** As a consumer of managed services, your organization may have a defined incident management process or may be using a service provider's process.	
4	Request a walkthrough of the service provider's incident response process.	
5	Determine each business unit's acceptable business downtimes.	
6	Determine each business unit's acceptable loss of data (for each type of security incident) to inform back-up methods and schedules (e.g. how often do back-ups occur?). For example, if back-ups are performed daily, and the system goes down 23 hours later, then 23 hours of data will be lost. Is this an acceptable risk to your organization?	
7	Determine your organization's vision related to incident management roles and responsibilities (for each of the incident types identified) when using a managed service.	
8	Determine which incident response activities need to remain in your organization's control (e.g. for legal or regulatory compliance).	
Questions to Ask the Service Provider		
1	Does the service provider support the incident types and the roles that your organization has identified?	
2	Is the service provider interested in working with your organization to simulate incident response scenarios for the incident types identified?	

3	What are the service provider's roles and responsibilities with regards to incident response? What are the service provider's expectations of your organization's roles and responsibilities?	
4	What turnaround time does the MSP guarantee for the types of incidents you have identified?	
5	What are the penalties if the MSP does not respond within the maximum threshold of turnaround times?	
6	Who is the MSP's primary point of contact for incident response? **Note:** Provide your organization's primary contact information as well.	
7	Can the MSP support a hotline to initiate incident response? Availability?	
8	When a security incident that impacts your organization's data occurs, how does the MSP notify you?	

2.6.1 EVENT LOGGING SUPPORT

The service provider has direct access to systems associated with the services they provide. As such, the service provider may be able to provide log data or monitoring services related to the following:

- Virus scans;
- Detection of non-standard or suspicious code, files, or folders on hosts (host-based sensors);
- Signature auditing;
- Use of bandwidth;
- Event monitoring; and
- User activity monitoring.

You need to explicitly define your requirements and responsibilities with regards to log support to identify potential security incidents. You may not need to see all the logs, but you should be aware of events that impact your data.

Table 13: Consumer Activities Related to Event Logging Support

Number	Consumer Activity	Check
1	Determine your capabilities for reviewing and analyzing logs.	
2	Determine which log data you need to review (e.g. security incidents, legal proceedings, legal or regulatory compliance).	
3	Review your data retention policy (i.e. legal requirements and industry regulations for keeping data) and request to see the MSP's data retention policy.	
Questions to Ask the Service Provider		
1	Is sensitive log data stored in Canada?	
2	Can the MSP support and comply with your data retention policy for logs?	
3	What types of logs can the MSP provide?	
4	How often does the MSP provide logs (e.g. periodically, security incidents, upon request)?	
5	Can the MSP deliver logs through a media that adequately protects the sensitivity of data?	
6	Does the MSP provide monitoring services? If yes, request details or a walkthrough of services.	
7	How often does the MSP review logs?	
8	How are you notified about the occurrence of a security incident that impacts your data? How long after the incident are you notified?	
9	Does the MSP monitor only for known-malicious code (e.g. signature detection), or do they also use behavioural detection to monitor for zero-day attacks?	
10	Does the MSP have the capability to identify patterns in incidents that occur over time? Will they notify you?	

2.7 BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity refers to your organization's ability to continue operations when something goes wrong (e.g. a disruption or disaster). If you use a service provider, you depend on them to support the ongoing availability of the services that you use. You should know the actions that the service provider takes to prevent failures and the ways in which the service provider supports the recovery of these services in the event of disaster. Business continuity and disaster recovery refer directly to the availability pillar of the data sensitivity profile (see section 2.1).

2.7.1 REDUNDANCY

Uptime refers to the service provider's guaranteed percentage of time that they can provide services. Note that not all service providers, including CSPs, have the same uptimes. You should ensure that you can access your organization's data when it is needed.

Hardware failures happen, but systems can continue to operate based on the amount of redundancy and the failover mechanisms that are in place. As part of your organization's business continuity planning, determine your uptime requirements, as well as the maximum time you can afford to be down without significantly impacting your business (i.e. maximum tolerable downtime). Note that your uptime and maximum tolerable downtime requirements may vary depending on your business functions and processes. For example, the acceptable downtime for an electoral administration organization during election day is much less tolerable than downtime the day after the election.

Table 14: Consumer Activities Related to Redundancy

Number	Consumer Activity	Check
1	Determine your uptime requirements (i.e. percentage of time that your organization's functions and processes need to be up and running to effectively conduct business).	
2	Determine the maximum tolerable downtime that your organization can tolerate without significant impact to your business. This will determine the service requirements (e.g. the maximum time the MSP can be down without incurring penalties) that you establish with the MSP.	
3	Refer to the acceptable downtimes and acceptable data losses identified in section 2.6.	
Questions to Ask the Service Provider		
1	What expected outages will occur?	
2	How will the MSP notify you of planned and unplanned outages?	
3	Which failover mechanisms are used by the MSP?	
4	Is redundant data stored in Canada?	

5	What is the MSP's uptime guarantee?	
6	How will uptime requirements be enforced?	

2.7.2 DISASTER RECOVERY

In a perfect situation, disasters do not occur, and recovery is not necessary. However, your organization needs to be prepared for scenarios in which things go wrong so that you can recover quickly and reduce the impact to your business operations. Your organization is responsible for establishing and testing a disaster recovery plan. You may want to outsource certain aspects of that plan (e.g. backing up data) to a service provider. You must work with the MSP to ensure that outsourced services work and that your roles and responsibilities are clear.

Table 15: Consumer Activities Related to Disaster Recovery

Number	Consumer Activity	Check
1	Define disaster recovery requirements (e.g. if a disaster occurs what do you need to do to resume operations?).	
2	Determine your organization's ability to meet disaster recovery requirements (i.e. what must or can be outsourced?) and establish a disaster recovery plan.	
3	Determine how your organization will test the disaster recovery plan and determine the requirements for service provider participation.	
4	Determine the requirements for the frequency and the method of back-ups. **Note:** This depends on factors such as how much data you can lose. For example, if a failure occurs 23 hours after the last daily back-up, 23 hours of data could be permanently lost. But hourly back-ups can be expensive.	
5	Determine your data retention policy for back-ups (see section 2.2).	
6	Identify your organization's primary point of contact for disaster recovery.	
Questions to Ask the Service Provider		
1	Can the service provider walk you through their disaster recovery service offerings?	
2	Does the MSP support your organizational data back-up requirements (e.g. back-up frequency, method, retention policy)?	
3	Does the MSP support a delivery medium for back-ups as per the level of sensitivity of your data (e.g. secure channel or appropriate level of encryption)?	
4	Is sensitive back-up data stored in Canada?	

5	Is the MSP willing to actively participate in your disaster recovery testing?	
6	Is the back-up site a cold, warm, or hot site? **Note:** A hot site refers to a back-up site that has hardware, an HVAC system, and a data duplicate, making it a fully operational site in hours. A warm site has the hardware and an HVAC system, but this site may take up to a week to get up and running with your organization's data. A cold site has an HVAC system, but it needs hardware and must be set up before it is usable, usually in 1-2 months.	
7	How does the MSP isolate back-ups from operational data? **Note:** Best practice is that back-ups should not be stored in the same place as operational data. The same disaster (e.g. fire, flood, vendor lockout) that caused loss of operational data could impact the back-ups as well.	
8	Does the MSP have a secure emergency line to initiate the disaster recovery plan?	

2.8 SUPPLY CHAIN INTEGRITY

Your supply chain is your network of suppliers, service providers (also referred to as sub-processors), partner organizations, and resources that are involved in creating and delivering your business products and services. Your supply chain is critical to your business activities, but it can also be a high-value target for threat actors.

As indicated in the Cyber Centre's *National Cyber Threat Assessment 2018* [13] , sophisticated cyber threat actors continue to exploit the relationships between businesses and their suppliers and service providers, including information and communication technology (ICT) supply chains. Industry research also confirms that half of all observed cyber attacks involve supply chain compromises.

Regardless of the size of your organization, you should consider the risks associated with your supply chain and ICT products and services (e.g. end user devices, software, networking solutions, servers). When procuring managed services, it remains your responsibility to protect the security of your information. Therefore, you must understand the assurance level that the service provider can provide for the technology that they are responsible for.

Table 16: Consumer Activities Related to Supply Chain Integrity

Number	Consumer Activity	Check
1	Review the potential services that you are procuring from the MSP. Who is responsible for procuring and managing the technology for these services? The answer to this question will direct the scope of your conversation with the service provider.	
	Questions to Ask the Service Provider	
1	For the technology that the service provider is responsible for managing, does the service provider's supply chain assurance align with the guidance given in ITSG-33 [2] security control, SA-12? Does the assurance align with *NIST Special Publication 800-161 Supply Chain Risk Management Practices for*	

	Federal Information Systems and Organizations [14] or *ISO/IEC 27036-1:2014 Information Security for Supplier Relationships* [15]? If so, can the service provider demonstrate this alignment in their policy or planning documents?	
2	When the MSP contracts with a service provider (sub-processor), how do they review the vendor to ensure supply chain integrity? How does the vendor demonstrate supply chain integrity?	
3	When changes occur to the platform, how does the service provider review supply chain risk? Does the service provider notify your organization to discuss opt-in or opt-out parameters?	

2.9 DATA AND SERVICE PORTABILITY

After entering a contract with a service provider, your organization may decide to go another way due to service dissatisfaction or changing business needs. Vendor lock-in occurs when it is not financially feasible to port data from one provider to another (e.g. large penalties associated, proprietary data formats, ownership of data).

Data portability refers to the ability to move data from one system or server to another. Your organization should consider an exit strategy, in case the need arises, when entering a service contract.

Table 17: Consumer Activities Related to Data and Service Portability

Number	Consumer Activity	Check
1	Discuss data portability with the service provider before you sign a service contract (to prevent vendor lock-in).	
2	Look into your potential MSP. Their reputation can help you determine whether you can trust the MSP with your data.	
Questions to Ask the Service Provider		
1	Who retains legal ownership of the data in the following circumstances: • A service provider contract is dissolved? • A service provider moves servers/data/back-ups to a location not agreed upon when the contract was negotiated? • If significant changes to security practices occur that undermine your organization's confidence in the service provider's ability to secure the data? • If the service provider is acquired by an organization that does not evaluate security or that raises concerns from the perspective of supply chain integrity?	
2	What are the penalties if your organization wants to change to another MSP (i.e. costs of moving)?	
3	Are any of the data formats not industry standard (i.e. vendor proprietary standards)?	
4	What costs are associated with porting legacy systems to the MSP's storage infrastructure?	
5	What happens if the service provider goes bankrupt? How can you get your organization's data back?	

2.10 DATA DESTRUCTION

Once data is no longer needed for business purposes, and it meets its retention period, it should be destroyed. Data destruction involves destroying the data that is stored on tapes, hard disks, and other forms of electronic or physical media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes. Proper data destruction ensures that your organization complies with legal and regulatory requirements. It also decreases the risk of data spills and breaches. Data spills can lead to non-compliance with legislative and policy requirements, loss of reputation, negative media coverage, loss of revenue, regulatory fines, prosecution, and legal fees.

When procuring cloud services, you must ensure that data is secured and effectively destroyed according to your organization's requirements (e.g. information management policy, retention schedule). In the cloud, physical destruction of hardware is extremely difficult because the CSP owns the hardware and may host multiple clients on the same hardware. Instead the most effective means of destroying data is crypto-shredding. Crypto-shredding refers to encrypting data that is no longer needed and then deliberately deleting or overwriting the encryption keys to make the data inaccessible.

Please note that cloud infrastructure is built on the principle of redundancy (i.e. there are many instances of data). To destroy the data completely, all instances of the data must be located. Also be aware of offline copies, such as back-ups or other downloads, to ensure that they are included in the destruction process.

Table 18: Consumer Activities Related to Data Destruction

Number	Consumer Activity	Check
1	Identify your organization's data destruction requirements, considering the sensitivity of the data. **Note:** If data resides in the cloud, effective destruction requires crypto-shredding.	
2	Contact our Contact Centre and review ITSP.40.006 IT Media Sanitization [16] for more information on data destruction.	
Questions to Ask the Service Provider		
1	What approach will the MSP take to ensure complete and secure data deletion?	
2	Will the MSP be able to locate all instances of data for destruction purposes?	
3	When hardware is life cycled, how is it sanitized?	

3 SUPPORTING CONTENT

3.1 LIST OF ABBREVIATIONS

Term	Definition
ADFS	Active Directory Federated Services
CDS	Cross-domain solution
COBIT	Control Objective for Information and Related Technologies
CSA	Cloud Security Alliance
CSP	Cloud service provider
DLP	Data loss prevention
EU	European Union
GC	Government of Canada
GDPR	*General Data Protection Regulations*
ISACA	Information Systems Audit and Control Association
ISAE	*International Standard on Assurance Engagements*
ISO	International Organization for Standardization
IT	Information technology
ITS	Information technology security
MSP	Managed service provider
NOC	Network operation centre
NIST	National Institute for Standards and Technology
PIN	Personal identification number
PIPEDA	*Personal Information Protection and Electronic Documents Act*
SA	System administrator
SCI	Supply chain integrity
SOC	Service organization controls (report)
STAR	Security Trust Assurance and Risk
TBS	Treasury Board of Canada Secretariat
2FA	Two-factor authentication

3.2 GLOSSARY

Term	Definition
Authentication	The process of confirming the identity of a user or another entity (e.g. application) as valid and genuine.
Authorization	The use of authentication information to determine whether an entity (i.e. person or application) can access data or perform a function.
Availability	A value that is assigned to information assets, software, and hardware (infrastructure and its components). Data with the highest possible availability rating must always be accessible. Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Cold site	A site that has an HVAC system, but it needs hardware and requires set up before it is usable.
Confidentiality	A value that is assigned to a set of information to indicate its sensitivity level and any access restrictions that prevent unauthorized people from accessing it.
Crypto-shredding	Encrypting data that is no longer needed and then deliberately deleting or overwriting the encryption keys to make data inaccessible.
Data at rest	Data that is inactive (e.g. residing in a database, data warehouse, spreadsheet, archives, back-ups, mobile devices).
Data in transit	Data that is active and moving from one location to another, such as across the Internet or within a private network.
Encryption key	A random string of bits that are generated by an algorithm and that are used to encrypt and decrypt data.
Federated identity	The means of linking a person's electronic identity and attributes, which are stored across multiple identity systems.
Hash	A mathematical function that is used to convert a block or group of data into a fixed-length value, which is usually shorter than the original data. Hashes mask the original data with another value that can only be decoded by looking up the value from a hash table.
Hot site	A back-up site that has hardware, an HVAC system, and a data duplicate, making it a fully operational site in hours.
Integrity	A value that is assigned to information to indicate how sensitive it is to data loss. Implied in its definition is that integrity includes protecting information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Least privilege	The access control principle in which you only grant users the privileges that they require to carry out their functions.
Salting	Adding characters to a password to achieve a standard length, further obscuring their true value.
Two-factor authentication	An authentication method in which two separate authentication factors (e.g. something you know, something you are, something you have) are required before access is granted.
Warm site	A site that has the hardware and an HVAC system.

3.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *Cyber Security Best Practices: Contacting with Managed Service Providers.* 3 April 2017.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	Treasury Board of Canada Secretariat. *Direction for Electronic Data Residency: IT Policy Implementation Notice*. 1 November 2017.
4	International Organization for Standardization. *ISO27001/2 Information Security Management.*
5	Information Systems Audit and Control Association. *Control Objective for Information and Related Technologies (COBIT).*
6	Cloud Security Alliance. *Security Trust Assurance and Risk (STAR).*
7	National Institute of Standards and Technologies. *Risk Management Framework*.
8	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information*. October 2018.
9	International Auditing and Assurance Standards Board. *International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization*. June 2011.
10	Canadian Centre for Cyber Security. *ITSAP.30.032 Best Practices for Passphrases and Passwords*. September 2019.
11	Canadian Centre for Cyber Security. *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information.* August 2016.
12	Canadian Centre for Cyber Security. *ITSP.40.062 Guidance on Securely Configuring Network Protocols*. October 2020.
13	Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2018.*
14	National Institute of Standards and Technology. *Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. April 2015.
15	International Organization for Standardization. *ISO/IEC 27036-1:2014 Information Security for Supplier Relationships.* April 2014.
16	Canadian Centre for Cyber Security. *ITSP.40.006 IT Media Sanitization.* July 2017.