Service Provider Management Policy Template

**CIS Critical Security Controls**

**March 2023**

# Contents

[Contents 2](#_Toc120739271)

[Acknowledgments 3](#_Toc120739272)

[Introduction 4](#_Toc120739273)

[Purpose 4](#_Toc120739274)

[Types of Service Providers 4](#_Toc120739275)

[Scope 5](#_Toc120739276)

[Service Provider Management Process 6](#_Toc120739277)

[Service Provider Management Policy Template 8](#_Toc120739278)

[Purpose 8](#_Toc120739279)

[Responsibility 8](#_Toc120739280)

[Exceptions 8](#_Toc120739281)

[Policy 8](#_Toc120739282)

[Revision History 10](#_Toc120739283)

[Appendix A: Acronyms and Abbreviations 11](#_Toc120739284)

[Appendix B: Glossary 12](#_Toc120739285)

[Appendix C: Implementation Groups 14](#_Toc120739286)

[Appendix D: CIS Safeguards Mapping 15](#_Toc120739287)

[Appendix E: References and Resources 16](#_Toc120739288)

# Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

**Editors:**

Joshua M Franklin, CIS

**Contributors:**

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Jon Matthies
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Robin Regnier, CIS
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to <http://www.cisecurity.org/controls/> when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Introduction

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure to manage core applications or functions. There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Most data security and privacy regulations require their protection extend to third service providers, such as with Health Insurance Portability and Accountability Act (HIPAA) Business Associate agreements in healthcare, Federal Financial Institutions Examination Council (FFIEC) requirements for the financial industry, and the United Kingdom (UK) Cyber Essentials. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise.

While reviewing the security of third-parties has been a task performed for decades there is not a universal standard for assessing security; and, many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. This is because every enterprise has a different “checklist”, or set of standards, to grade the service provider. Very few industry standards exist for grading service providers such as in finance, with the Shared Assessments Program, or in higher education, with their Higher Education Community Vendor Assessment Toolkit (HECVAT). Insurance companies selling cybersecurity policies also have their own measurements.

## Purpose

The Center for Internet Security® (CIS®) recommends several policies that an enterprise should have in place. This *Service Provider Management Policy* is meant as a “jumping off point” for enterprises that need help drafting their own policy. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise, such as the requirements for onboarding a service provider and the best way to assess service providers to those requirements.

In CIS Controls v8, Control 15 states:

**Control 15 – Service Provider Management –** Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise’s critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

To support this Safeguard, it is important for an enterprise to develop a program and processes to deal with third-party service providers. Most enterprises have traditionally used standard checklists, such as ones from International Organization for Standardization (ISO) 27001 or the CIS Controls. Often, this process is managed through spreadsheets; however, there are online platforms now that allow central management of this process. The focus of this CIS Control though is not on the checklist; instead it is on the fundamentals of the program. Make sure to revisit annually, as relationships and data may change. No matter what the enterprise’s size, there should be a policy about reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. There should also be language in the contracts to hold them accountable if there is an incident that impacts the enterprise. This document supports the development of a process for managing service providers and the implementation of Safeguards in this CIS Control. Further guidance is available in the [CIS Controls Version 8 Cloud Companion Guide](https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide).

## Types of Service Providers

Service providers are entities that offer platforms, software, and services to other enterprises. They are commonly referred to as “third-party service providers”. Although the benefits of CIS Control 15 can be applied to any form of service provider, it is primarily targeted to companies offering cloud services, also known as cloud service providers (CSPs). Examples of CSPs include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud, etc. There are multiple types of cloud service models as described below:

* IaaS (Infrastructure as a Service) is a cloud environment that computing resources such as virtual servers, storage, and networking hardware. The consumer utilizes their own software such as operating systems, middleware, and applications. The underlying cloud infrastructure is managed by the CSP.
* PaaS (Platform as a Service) is a cloud computing environment for development and management of a consumer’s applications. It includes the infrastructure hardware: virtual servers, storage, and networking while tying in the middleware and development tools to allow the consumer to deploy their applications. It is designed to support the complete application lifecycle while leaving the management of the underlying infrastructure to the CSP.
* SaaS (Software as a Service) is a cloud computing software solution that provides the consumer with access to a complete software product. The software application resides on a cloud environment and is accessed by the consumer through the web or an application program interface (API). The consumer can utilize the application to store and analyze data without having to worry about managing the infrastructure, service, or software, as that falls to the CSP.
* FaaS (Function as a Service) is a cloud computing service that allows the consumer to develop, manage, and run their application functionalities without having to manage and maintain any of the infrastructure that is required. The consumer can execute code in response to events that happen within the CSP or the application without having to build out or maintain a complex underlying infrastructure.

Another type of service provider is a managed service provider (MSP). An MSP will often be contracted to provide IT, cybersecurity, and other technology management services to enterprises who might internally lack those capabilities. MSPs are a popular option for smaller enterprises, and MSPs often end up being responsible for the IT for a large number of smaller enterprises. Finally, there are also general service providers that are contractors or other organizations providing IT, or non-IT related services.

## Scope

This *Service Provider Management Policy* is divided into multiple sections based on how enterprise will structure their service provider management programs, and approach each activity in that process. As this policy template is meant to supplement the CIS Controls v8, the policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In [Appendix D](#_Appendix_D:_CIS), Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see [Appendix C](#_Appendix_C:_Implementation). Additionally, a glossary in [Appendix B](#_Appendix_B:_Definitions) is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1 and are welcome to do so. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise’s needs.

# Service Provider Management Process

Not all security trainings are made equal. The enterprise that takes the time and resources to develop and provide high quality security training to their users will have the best chance at defending themselves from some of the most pernicious and persistent threats. Shown below in Figure 1 are the high-level aspects of the *Service Provider Management Process*, followed by a detailed description of what each step entails. This is not the only way to run a program, but this can act as a foundation to build your own program upon.

Figure 1. Service Provider Management Process

* **Identify Service Providers** – Understand which service providers are currently being used within an enterprise.
* **Establish Requirements** – Develop requirements for all service providers to be used in the enterprise. This could include security obligations, performance, availability, reporting, shared responsibility, classify providers based on risk and/or sensitivity.
* **Classify Service Providers** – Consider the characteristics of each service provider to include the sensitivity of the data handled by that provider.
* **Assess Service Providers** – Analyze the extent to which service providers meet established security objects and fulfil business needs.
* **Onboard Service Providers** – Integrating service providers into an existing enterprise technology stack.
* **Monitor Service Providers** – Ensure that service providers are honoring contractual agreements and maintaining compliance with applicable security frameworks, such as vulnerability monitoring and notification.
* **Decommission Service Providers** – Remove enterprise data from service providers no longer in use, to include account information and enterprise data.

**Identify Service Providers**

Modern enterprises are already leveraging third-party service providers for a variety of business tasks. Yet a massive question exists: are all of the service providers leveraged by the enterprise authorized by IT? This may include users buying access to service provider systems and services without authorization, or users leveraging them on a personal basis, often known as “shadow IT”. Service provider platforms may integrate directly into enterprise systems and will likely host sensitive data. Therefore, it’s important to build an inventory of service providers, what business processes are supported by the service providers who has access to that service, and what are the defined roles and responsibilities for accessing and managing the cloud systems.

**Establish Requirements**

Just because a service provider offers a useful tool, service, or platform does not mean that they are fit to operate within or alongside your enterprise. A set of requirements should be established to ensure that any future service provider satisfies both internal and external requirements; be them technical, legal, or otherwise. This means that not all requirements will be related to security. During this phase, enterprises are encouraged to identify applicable frameworks and business requirements that service providers must meet. Other than security obligations, these could include performance, availability, reporting, shared responsibility, and simply classifying service providers based on risk and/or sensitivity of the data. Not all requirements may be met by every service provider, and it’s possible that exceptions will be made.

**Classify Service Providers**

Cloud service providers can be classified by a variety of attributes. This classification process helps the enterprise to quickly understand the benefits, drawbacks, and ways that a provider is integrated into the enterprise. The requirements created in the previous phase will be helpful in determining useful classification for the enterprise. A variety of characteristics can be used to help classify a service provider. Characteristics such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk should all be considered. These classifications will need to be updated from time to time, as capabilities of service providers change.

**Assess Service Providers**

The primary goal of this phase is to better understand the degree to which service providers meet the previously established requirements. Generally, this will require that a formal assessment is performed. Enterprise’s may accept previously provided documentation or leverage an external assessment firm to understand the extent to which the requirements are met. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. It’s important that service providers are reassessed annually, at a minimum, or with new and renewed contracts.

**Onboard Service Providers**

The precise method in which service providers are brought onboard will vary based on the provider in question. With some cloud-based applications, it may be as simple as obtaining accounts and uploading already existing data. Alternatively, the service provider may need to integrate directly into the enterprise active directory. The use of a Software Development Kit (SDK) may be required, or the new service provider will be acting as the primary set of infrastructure for the entire enterprise. Since it can be so different from provider to provider, it’s worth considering the process that will be used to bring the service provider into the fold and anticipate any hurdles that will prevent easy adoption. Discussing this plan with the service provider beforehand may be prudent to understand potential points of failure before they occur.

**Monitor Service Providers**

Service providers will need to be reassessed on an ongoing basis. This can be for a variety of reasons, such as monitoring for compliance with contractual agreements, a large change to the provider’s technological infrastructure, or a data breach. Patch or release notes will often detail changes in the service provider’s infrastructure, and from time-to-time issues with a service provider’s platform will make the news. Both of these avenues are solid. In a perfect world, monitoring needs to include finding the vulnerabilities that the service providers are experiencing, or notifying them of the issue(s), to see if an enterprise wants to continue using them. This isn’t always practical depending on language within the contractual agreement.

**Decommission Service Providers**

From time to time, service providers may go out of business or the enterprise may no longer need their services. At this point, a service provider needs to be decommissioned from the enterprise. There needs to be a formal process for how to decommission service providers from the enterprise. This process should include removing enterprise data, accounts, and any access the service provider has to enterprise data. Specific service provider accounts with access to enterprise assets need to be removed (e.g., internal, third-party services, external contractors). The provider may be kept, but a specific account may need to be deactivated or removed. Removing accounts and access should be done in accordance with the enterprise’s *Identity Management Policy* and/or *Data Management Policy*.

# Service Provider Management Policy Template

## Purpose

Commonly referred to as “third-party service providers”, service providers are entities that offer platforms, software, and services to other enterprises. Service providers fulfill necessary business functions but their usage needs to be carefully managed to ensure that data they manage are not exposed to unauthorized third parties. The *Service Provider Management Policy* provides the processes and procedures for this program.

## Responsibility

The IT business unit has the primary responsibility for keeping an inventory of the service providers within the enterprise with the caveat of the business unit responsible for contracts and procurement. Before bringing new providers into service, IT must assess that these new providers appropriately fill the enterprise needs while meeting legal and regulatory obligations. Finally, IT must also maintain and decommission all providers. Employees are not empowered to store enterprise data on unauthorized service provider systems.

## Exceptions

Exceptions to this policy are likely to occur. Exception requests must be made in writing and must contain:

* The reason for the request,
* Risk to the enterprise of not following the written policy,
* Specific mitigations that will not be implemented,
* Technical and other difficulties, and
* Date of review.

## Policy

**Identify Service Providers**

1. At a minimum the inventory of service providers must include:
2. Name of service provider
3. Business unit leveraging the platform
4. Service provider classifications
5. Point of contact at service provider
6. Point of contact within the enterprise managing the service provider relationship
7. The service provider inventory must be reviewed and updated annually, or when significant enterprise or service provider changes occur.

**Classify Service Providers**

1. IT should classify each service provider according to attributes such as:
	1. business function
	2. geographical location
	3. data sensitivity
	4. data volume
	5. availability requirements
	6. applicable regulations
	7. inherent risk or mitigated risk

**Assess Service Providers**

There are no IG1 safeguards that support this portion of the security awareness training process.

**Onboarding of Service Providers**

There are no IG1 safeguards that support this portion of the security awareness training process.

**Monitor and Verify Service Providers**

There are no IG1 safeguards that support this portion of the security awareness training process.

**Decommission Service Providers**

There are no IG1 safeguards that support this portion of the security awareness training process.

Revision History

Each time this document is updated, this table should be updated.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Revision Description | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| AoC | Attestation of Compliance  |
| API | Application Program Interface  |
| AWS | Amazon Web Services  |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| CSP | Cloud Service Providers |
| FaaS | Function as a Service |
| FFIEC | Federal Financial Institutions Examination Council  |
| GCP | Google Cloud Platform  |
| GRC | Governance Risk and Compliance |
| HECVAT | Higher Education Community Vendor Assessment Toolkit |
| HIPAA | Health Insurance Portability and Accountability Act |
| IaaS | Infrastructure as a Service  |
| IG | Implementation Group |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| MSP | Managed Service Provider |
| PaaS | Platform as a Service  |
| PCI | Payment Card Industry |
| SaaS | Software as a Service  |
| SDK | Software Development Kit  |
| SOC 2 | Service Organization Control 2 |
| UK | United Kingdom |

# Appendix B: Glossary

|  |  |
| --- | --- |
| Asset | Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).Source: [Asset(s) - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| Asset inventory  | An asset inventory is a register, repository or comprehensive list of an enterprise’s assets and specific information about those assets.Source: [Asset Inventory | FTA (dot.gov)](https://www.transit.dot.gov/TAM/resources/assetinventory) |
| Asset owner | The department, business unit, or individual responsible for an enterprise asset.Source: CIS |
| Cloud environment | A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). |
| Enterprise assets | Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments.Source: CIS Controls v8  |
| Physical environment | Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.Source: CIS Controls v8 |
| Servers | A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.Source: CIS Controls v8 |
| User | Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.Source: CIS |
| Virtual environment | Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.Source: CIS Controls v8 |

# Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

**IG1**

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

**IG2**

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

**IG3**

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

# Appendix D: CIS Safeguards Mapping

**CIS Controls & Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 15: *Service Provider Management*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard Description |
| 15.1 | Identify Service Providers1, 2, 3Classify Service Providers 1 | Establish and Maintain an Inventory of Service Providers | Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard. |

# Appendix E: References and Resources

Center for Internet Security®

<https://www.cisecurity.org/>

CIS Critical Security Controls®

<https://www.cisecurity.org/controls/>

CIS Controls v8 Cloud Companion Guide
<https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide>

CIS Companion Guide—Establishing Essential Cyber Hygiene Through a Managed Service Provider (MSP)
<https://www.cisecurity.org/insights/white-papers/establishing-basic-cyber-hygiene-through-a-managed-service-provider>

FedRAMP
<https://www.fedramp.gov>