CIS 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.

Why is this CIS Control Critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on infrastructure for 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 service providers in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly due to one of its 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 service providers, such as 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 (U.K.) Cyber Essentials. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise is transferred to entities outside the enterprise.

While reviewing the security of third parties has been a task performed for decades, there is no universal standard for assessing security; and many service providers are being audited by their customers multiple times a month, causing impacts on their own productivity. This is because every enterprise has a different "checklist" or set of standards to grade the service provider. There are only a few industry standards, 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.

While an enterprise might put a lot of scrutiny into large cloud or application hosting companies because they are hosting their email or critical business applications, smaller firms are often a greater risk. Oftentimes, a service provider contracts with additional parties to provide other plugins or services, such as when a third-party uses a fourth-party platform or product to support the main enterprise.

15.1: 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, including 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.

Asset Type	Security Function	Implementation Groups
Users	Identify	1, 2, 3

Dependencies

- None

Inputs

1. `GV44`: Service Provider Inventory List
2. `GV46`: Date of last review or update of the service provider inventory

Operations

1. Determine whether the enterprise maintains a service provider inventory list by checking for Input 1,
    1. If Input 1 exists, M1 = 1
    2. If Input 2 does not exist, M1 = 0
2. Review Input 1 and determine if it includes, at a minimum, the following components: service provider, classification of provider, and an enterprise contact for the provider
    1. For each component included, assign a value of 1. Sum all values. (M2)
3. For each service provider identified in Input 1 `GV45`, determine whether they are accurately listed
    1. Identify and enumerate providers that are accurately listed (M4)
    2. Identify and enumerate providers that are erroneously listed (M5)
    3. Identify and enumerate providers that should be listed but are missing (M6)
4. Compare the date from Input 2 with the current date and capture the time frame in months (M7)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the inventory
- M3 = Count of service providers in the inventory
- M4 = Count of accurately listed providers
- M5 = Count of erroneously listed providers
- M6 = Count of missing providers from the list
- M7 = Timeframe since the last update or review of the inventory

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M7 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	**The percentage of components included in the inventory**
Calculation	`M2 / 3`

Accuracy of Inventory

Metric	**The percentage of accurately listed service providers in the inventory**
Calculation	`M4 / (M3 - M5 + M6)`

15.2: Establish and Maintain a Service Provider Management Policy

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	2, 3

Dependencies

- None

Inputs

1. `GV45`: Service Provider Management Policy
2. Date of last review or update of the policy

Operations

1. Determine whether the enterprise maintains a service provider management policy by checking for Input 1,
    1. If Input 1 exists, M1 = 1
    2. If Input 2 does not exist, M1 = 0
2. Review Input 1 and determine if it includes, at a minimum, the following components: service provider inventory, classification, assessment, monitoring, and decommissioning of service providers
    1. For each component included, assign a value of 1. Sum all values. (M2)
3. Compare the date from Input 2 with the current date and capture the time frame in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the policy
- M3 = Timeframe since the last update or review of the policy

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Policy

Metric	**The percentage of components included in the policy**
Calculation	`M2 / 5`

15.3: Classify Service Providers

Classify service providers. Classification considerations may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	**Security Function**	**Implementation Groups**
Users	Govern	2, 3

Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy
3. `GV46`: Date of last review or update to service provider inventory

Operations

1. Use Input 2 `GV45` to determine if the enterprise policy includes the classification process of service providers by one or more characteristics
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0

2. Compare the date of Input 3 `GV46` to the current date and capture timeframe in months (M2)

3. Review Input 1 `GV45` and determine whether service providers are classified using one or more characteristics per the enterprise's policy

    1. Identify and enumerate service providers with an assigned classification (M4)
    2. Identify and enumerate service providers without a classification (M5)

Measures

- M1 = Output of Operation 1
- M2 = Timeframe since the last update or review of the service provider inventory
- M3 = Count of service providers in inventory
- M4 = Count of service providers with classification
- M5 = Count of service providers without classification

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	**The percentage of service providers with a classification**
Calculation	`M4 / M3`

15.4: Ensure Service Provider Contracts Include Security Requirements

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Asset Type	**Security Function**	**Implementation Groups**
Documentation	Govern	2, 3

Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Inputs

1. GV44: Service Provider Inventory List
2. GV45: Service Provider Management Policy
3. Date of last update or review of contracts

Operations

1. Use Input 2 GV45 to determine if the enterprise policy includes security program requirements for service providers

    1. If the security requirements exist, M1 = 1
    2. If the security requirements do not exist, M1 = 0

2. Use Input 1 GV44 to determine if each listed service provider has a contract

    1. Identify and enumerate service providers with contracts (M3)
    2. Identify and enumerate service providers without contracts (M4)

3. For each service provider with a contract identified in Operation 2.1, compare the date from input 3 to the current date and capture the timeframe in months

    1. Identify and enumerate service providers whose contract has been reviewed within twelve months or less (M5)
    2. Identify and enumerate service providers whose contract has been reviewed outside the twelve-month window (M6)

Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with contracts
- M4 = Count of service providers without contracts
- M5 = Count of service providers with up-to-date contracts
- M6 = Count of service providers without outdated contracts

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	**The percentage of service providers with up-to-date contract**
Calculation	M5 / M2

15.5: Assess Service Providers

Assess service providers consistent with the enterprise's service provider management policy. 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. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Asset Type	Security Function	Implementation Groups
Users	Govern	3

Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Inputs

1. GV44: Service Provider Inventory List
2. GV45: Service Provider Management Policy

Operations

1. Use Input 2 GV45 to determine if the enterprise policy includes monitoring guidance for service providers

    1. If the assessment scope exists, M1 = 1
    2. If the assessment scope does not exist, M1 = 0

2. Use Input 1 GV44 to determine if each listed service provider has monitoring guidance included in the policy

    1. Identify and enumerate service providers with monitoring guidance (M3)
    2. Identify and enumerate service providers without monitoring guidance (M4)

Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with monitoring guidance
- M4 = Count of service providers without monitoring guidance

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	**The percentage of service providers with monitoring guidance included in policy**
Calculation	`M3 / M2`

15.6: Monitor Service Providers

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Asset Type	Security Function	Implementation Groups
Data	Govern	3

Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy

Operations

1. Use Input 2 `GV45` to determine if the enterprise policy includes monitoring guidance for service providers
    1. If the monitoring guidance exists, M1 = 1
    2. If the monitoring guidance does not exist, M1 = 0
2. Use Input 1 `GV44` to determine if each listed service provider has monitoring guidance provided in the policy
    1. Identify and enumerate service providers with monitoring guidance provided (M3)
    2. Identify and enumerate service providers without monitoring guidance provided (M4)

Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with monitoring guidance provided
- M4 = Count of service providers without monitoring guidance provided

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of service providers with up-to-date assessments
Calculation	`M3 / M2`

15.7: Securely Decommission Service Providers

Securely decommissioned service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy

Operations

1. Use Input 2 `GV45` to determine if the enterprise policy includes guidance for securely decommissioning service providers

    1. If the monitoring guidance exists, M1 = 1
    2. If the monitoring guidance does not exist, M1 = 0

2. Use Input 1 `GV44` to identify and enumerate any service providers terminated over the last twelve months (M2)

3. For each service provider identified in Operation 2, determine if the provider was decommissioned per the policy

    1. Identify and enumerate service providers properly terminated (M3)
    2. Identify and enumerate service providers improperly terminated (M4)

Measures

- M1 = Output of Operation 1
- M2 = Count of service providers terminated over the last twelve months
- M3 = Count of service providers properly terminated
- M4 = Count of service providers improperly terminated

Metrics

- If M1 is a 0, this Safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	**The percentage of service providers properly terminated**
Calculation	`M3 / M2`