Security Accreditation

Current Offerings

28 June 2023

Contents

1 Description

This service is provided to support an organization that wishes to be accredited against a particular cyber security standard. There are a number of such standards including:

1.1 Cyber Essentials

1.2 Cyber Essentials +

1.3 IASME Governance

1.4 NIST 800-53

1.5 NIST 800-171

1.6 PCI-DSS

1.7 AICPA SOC 2

1.8 HIPAA

1.9 GDPR

1.10 BS 31111

1.11 ISO 27001

1.12 ISO 27002

1.13 ISO 27003

1.14 ISO 27005

1.15 ISO 27017

1.16 ISO 27032

1.17 ISO 27033

1.18 ISO 27034

1.19 ISO 27701

1.20 BS 7799-3

The IASME Cyber Assurance standard, formerly known as IASME Governance, is a comprehensive, flexible and affordable cyber security standard.

1.21 Security Policy Service

A pre-requisite for this service is that the organization takes our Security Policy Service.

This service comprises:

a) Analyzing the cyber security requirements of the particular standard to be met.

b) Identifying the necessary measures that need to be included in a security policy to achieve the standard and linking these to the overarching requirement in the standard.

c) Adopting the revised security policy.

d) Creating a report that describes how each requirement is met by the security policy.

1.22 Security Policy Templates

We have pre-prepared templates for a sophisticated security policy that if implemented will deliver the standard.

This service comprises the following activities:

a) Reviewing all the responses required to provide a submission to achieve the standard.

b) Identifying typical security requirements to achieve compliance with the standard.

c) Reviewing the existing customer security policy and determining what extra items if any need to be included within the security policy to achieve the requirements.

d) Promulgating the additional items if any of the security policy to those staff responsible for ensuring the requirements are met.

e) Monitoring implementation of the updated security policy and auditing records to demonstrate that the policy is being complied with.

f) Providing to the accreditor of the standard a report describing how the organization meets the standard and an audit report to demonstrate governance is in place to comply with the policy.

Delivery of this service assumes that our Security Policy service is being taken. This service ensures that the enhanced security policy is being followed and links the policy to the standard, hence illustrating that the standard is being met.

It should be noted that using our templates does not guarantee compliance with a standard because we cannot cater for every different customer scenario. What we do is to ensure that you implement the policy you have defined that has been agreed as compliant with the standard.

2 Commercial Terms

2.1 Fees

You pay the charges for our Security Policy service for every member of you organization that is required to carry out activity and have a record of that activity held to demonstrate compliance.

If we have already implemented the standard and have organizations that have achieved the standard using the Security Policy service then you shall pay a charge for using the standard, identified in our price list.

2.2 Upfront fee

If you wish to utilize a standard which is not currently supported, we reserve the right to charge an upfront fee to be agreed in advance to implement the standard and typical additional security policy items so that our standard security policy template is consistent with the standard.

You do not directly pay for own any underlying perpetual licenses or third-party subscriptions for our service. We manage all of the underlying technology.

2.3 Monthly charges

When you take our service there is an initial 1-year commitment. You can terminate use of the service completely giving 30 days' notice on completion of the 3-month commitment.

If you terminate the service, then we stop managing your network and have no further responsibilities to you. The equipment is yours and remains in place and we will provide you the appropriate details for you to manage it yourself.

Your charge is monthly in advance for payment within 15 days. We can take check or credit card but request you set up regular ACH payments to minimize administration and costs for both parties.

A small discount is available for increased long-term commitment or annual payments in advance provided payments are via ACH.

3 Service benefits

This service means that:

a) You have a single policy which is extended to cover any additional requirements of a standard or standards that you wish to comply with.

b) Any task that is common to all of your standards needs only to be carried out once.

c) If you decide to cease complying with a standard, you can identify all of the activity linked to that standard and determine whether each individual activity should remain included within your security policy.

d) If you identify any tasks that are included in your policy and which are considered onerous, you can identify which standards are associated with that task and hence review the importance of continued adherence or the scope to change the task if a more effective and cheaper approach to compliance can be identified.

e) Our reporting dashboard can alert the board to non-compliance and any associated risks of failing a future audit, so that corrective action can be taken by the board.

f) A single report generated by the system can be provided to the auditor for review and sign off.

4 Deploying and Operating the Service

A new standard that is not already maintained in the system would need to be developed and then linked to the security policy and then loaded. The effort and complexity of this together with the associated time will need to be evaluated.

Once a standard is available, setting up the service involves selecting the standard from our menu of standards if it is already loaded.

The activity to deploy and operate a new standard is an extension of the security policy service involving:

a) Adding details of the standard.

b) Collecting responses to the standard that can then be output as a report.

c) If there is a capability to automatically provide results to an accreditation authority, building the integration to populate the auditor's system.

d) Building the links between a particular requirement of the standard and the actions that need to be carried out to implement that standard.

e) Building dashboard displays that monitor progress with the standard and generate alerts for management if the organization is at risk of going out of compliance.

From time to time the standards change. If we make a standard available, we have an obligation to update the online standard from time to time. We will priorities updates based on customer demand.

We provide a standard SLA for all customers, and we report to you against that SLA monthly.

5 Supporting Documentation

In our knowledge base we provide you references to the underlying standards, and copies of the standards where we are permitted to do so, as well as links to industry bodies and other relevant information you may wish to consider when developing your approach to meeting the standard and your underlying policies to implement those approaches.

We provide an extensive user guide showing you how to operate the service.

6 How Support Works

The following is a brief description of our support mechanism. This is explained fully in our support manual:

- If you encounter an issue when using our service, it is raised from the user interface by using a simple form or selecting the option to access our Atlassian our service desk environment.
- Once a call is raised you will be emailed from our service desk environment giving you the details.
- All information related to the issue should be entered via service desk but we will accept calls to escalate urgent/serious issues by email or phone.
- Once an issue is raised, you can then track the issue through to resolution.

Support is provided during the working day between 0800 and 1800 in your geography. Optionally you can purchase extended support for out of hours or 24 x 7 though this is subject to an additional charge and may involve a preparation period where we assign the resources to provide this.

Onsite support is not included as part of this service: we work with your onsite representative. However, we are able to provide onsite support as part of our Equipment Managed service offering.

At the end of each month, you are provided with a report describing our performance against agreed KPIs.

Our service desk is available at the following URL

https://cysure.atlassian.net/servicedesk/customer/portal/2

7 What is not included

This service does not include consultancy support to help you collect data about your organization that needs to be entered into the system. Neither does it include support to help you evaluate your response to the accrediting organization considering whether you meet the standard you are seeking.

We can provide consultancy services or introduce you to third party consulting organizations who are experts in the standard and who can help you ensure that your overall processes are likely to satisfy the accreditor.

.

8 How we may change the service from time to time

Our service is based on purchasing software licenses and subscriptions which we then use to deliver the service. From time to time the technology vendors of these products increase their prices and we need to similarly increase our prices.

We will publish any revised prices on our website and will notify you of any price rises giving you 3 months' notice of such price rises. By taking this service you agree to accept any such price rises. You may terminate the service if you wish.

You should also read how we may change our Security Policy service as this service is dependent on that.

If the standard changes, then we intend to upgrade the standard in our solution. Whenever possible we shall preserve responses to the previous standard unchanged for your historical record.

9 Terminating our service

If you decide to terminate our service, then for this service you must provide us 30 days' notice of termination.

On termination and provided we have received payment in full on all outstanding invoices, we will if asked, provide to you a copy of your data held within the system in CSV form

After one month or sooner if you request, we will remove all information related to your implementation of the service and then remove all details of your organization from the platform.

It is your responsibility to archive any reports important to you before you terminate as once we remove your organization from the platform all historic data is deleted.

If you require any assistance from us when terminating, for example to transfer to an in-house solution or to an alternative vendor, then as a responsible supplier we will

assist you in this process if requested and charge you at our standard professional services rates on a time and materials basis.