Security Policy Framework

Cloud Computing Security Policy and Standard

Version: 2.0

Release date: 2020-01-07

Document classification: PUBLIC

FORESIGHT® CYBER

INTRODUCTION

Document Purpose

Cloud computing is an approach to delivering IT services that promise to be highly agile and lower costs for Foresight Cyber. Many cloud service providers allow organisations to use new services, support new ways of working, and overcome the gap in internal IT capabilities.

This Cloud Security Standard sets the use of best practices for providing security assurance within Cloud Computing. The standard is setting the required processes and controls for cloud computing use in Foresight Cyber.

Scope

The document covers all security aspects of Cloud services, namely design, procurement, running and decommissioning. The Standard covers the whole Foresight Cyber Ltd group, systems, employees and contractors.

CLOUD SECURITY POLICY

It is the policy of Foresight Cyber to:

Cloud Services enable Foresight Cyber to be agile and concentrate on its core business, however the cloud services must be carefully assessed, selected and embedded into company' operational processes to limit to the extent possible business risks, such as but not limited to business disruption security incidents , and financial loss.

This policy is owned by CEO and enforced by Head of Operations. The cloud security standard statements that follow expand on this policy statement. Further guidance is located in wiki pages.

CLOUD SECURITY STANDARD

From the business perspective cloud computing is seen as a transformational technology and can provide Foresight Cyber with instant access to highly scalable IT services on demand where it only must pay for what it uses.

However, the use of certain types of cloud services increases risk to unacceptable levels and therefore the Foresight Cyber requirements related to Cloud are listed below:

Generic requirements

- Requirement 1: Discover Cloud services being used in Foresight Cyber
- Requirement 2: Enterprise Architecture ready for Cloud Services
- Requirement 3: Plan for Exits from Cloud Providers and Services

Before a Cloud service procurement

- Requirement 4: Comply with Foresight Cyber data classification requirements
- Requirement 5: Encrypt all sensitive data processed in the Cloud
- Requirement 6: Link the Cloud service into the Foresight Cyber Identity and Access architecture and monitoring of activities of users

During a Cloud service procurement

- Requirement 7: Perform due diligence activities before the contract is signed
- Requirement 8: Request "Right to audit" clause in the contract
- Requirement 9: Know locations of personal identifiable information in the cloud
- Requirement 10: Assess the availability of the Cloud services
- Requirement 11: Assess the cloud provider's security arrangements
- Requirement 12: Assess the Cloud provider's ability to comply with Foresight Cyber forensic investigations

Running a Cloud service

- Requirement 13: Limit the use of live data for testing and development purposes
- Requirement 14: Maintain security of cloud environments
- Requirement 15: Monitor Cloud providers security arrangements

Decommissioning a Cloud service

- Requirement 16: Destroy sensitive information when not required

GENERIC REQUIREMENTS

Requirement 1: Discover Cloud services being used in Foresight Cyber

Justification: Foresight Cyber needs to manage risk diligently. Knowing what Cloud services are deployed is key for managing unknown risks.

Detailed requirements:

1. Gather information about possible cloud deployments and correlate with the central cloud services register.
2. Monitor connections between Foresight Cyber internal networks / systems and external networks to identify new services that have been deployed.
3. Identify large amounts of data that are being transferred between Foresight Cyber and Cloud providers.

Requirement 2: Enterprise Architecture ready for Cloud Services

Justification: Business applications that are developed and deployed internally must conform to the Foresight Cyber enterprise and security architecture requirements. One of the main features of the security architecture is that it ensures that there is an integrated approach – helping to ensure that individual weaknesses in applications do not compromise the security, regulatory compliance and business continuity of Foresight Cyber. Additionally, as cloud native organisation, we must preferably use cloud security controls.

Detailed requirements:

1. CTO to outline how cloud services should and should not be used and how cloud services should integrate with standard security services
2. CTO to ensure security controls are extended to cloud, and where possible use cloud vendor native security controls.
3. The Security Architecture and associated controls & tooling should adapt to Cloud Shared Responsibility Model
4. Cloud Services to be assessed against the enterprise and security architectures
5. Document all Cloud Services in Foresight Cyber CMDB, as defined by Cloud Security Alliance Guidance[1] and detailed by each cloud provider (such as Azure [2]and AWS[3])

[1] https://cloudsecurityalliance.org/research/guidance/
[2] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[3] https://aws.amazon.com/compliance/shared-responsibility-model/

Requirement 3: Plan for Exits from Cloud Providers and Services

Justification: Cloud Providers and their Services change and Foresight Cyber may choose or be forced to exit a cloud provider service.

Detailed requirements:

1. When evaluating a cloud service for a business process, prepare a high-level plan for existing the cloud provider
2. Where possible setup automated data exports to ensure business continuity

BEFORE A CLOUD SERVICE PROCUREMENT

Requirement 4: Comply with Foresight Cyber data classification requirements

Justification: The data owner is accountable for ensuring the security controls for the data are adequate and without the data owner permission the data cannot be processed in the Cloud. Public clouds share infrastructure and potentially data with other customers and that could present unacceptable risk to Foresight Cyber.

Detailed requirements:

1. Consult with the data owner and obtain the permission to process data in the cloud
2. Ensure all copies of personally identifiable information are protected by the same controls
3. Ensure the Cloud provider has appropriate system and data segregation controls in place, based on the criticality of the systems and data classification
4. Comply with the data classification table for Cloud services:

	Get data owner approval	
	Public cloud	Private cloud dedicated to Foresight Cyber
Public	No restriction	No restriction
Internal	CISO Approval	No restriction
Confidential	CISO Approval	CISO Approval
Personal identifiable information	DPO approval	DPO approval
Payment data	CEO Approval	CEO Approval

Requirement 5: Encrypt all sensitive data processed in the Cloud

Justification: Confidential information that is not encrypted may be exposed to unauthorised users. The encryption key is a secret that must be kept separately from the data in order to protect the encrypted data effectively.

Detailed requirements:

1. Encrypt all information, whether in-transit or at-rest, that is classified as internal and above.
2. Retain key management responsibility within Foresight Cyber, unless such architecture breaks the model of the Cloud provider (approval by CISO required).
3. Configure each new cloud encryption deployment to use the enterprise-wide key management service
4. Ensure the encryption keys are stored separately from the data.

Requirement 6: Link the Cloud service into the Foresight Cyber Identity and Access architecture and monitoring of activities of users

Justification: Different identity and access management solutions could be required for each cloud computing service or no solution being provided at all. This could result in users potentially having multiple unrelated user identities all of which need to be managed by both the user and Foresight Cyber.

Detailed requirement:

1. Evaluate the access controls of the cloud service to determine if they meet the Foresight Cyber requirements, specifically:
    a. log changes to access rights,
    b. prevent access by cloud service provider users to Foresight Cyber data
    c. satisfy the access requirements of Foresight Cyber including the appropriate granularity of access rights.
2. Determine how access control to cloud services will be managed and utilise Foresight Cyber Identity and Access systems to manage the access.
3. Require all cloud services to integrate with the Foresight Cyber Identity Access Management (AIM) architecture for provisioning and single sign-on (SSO)
4. Identify which events (e.g. login, access to data or changing user permissions) need to be logged.
5. Determine the level of event logging of user activity that is available with the cloud provider.
6. Commission transfer of logging information, together with correct mapping to enable parsing of logs, from the Cloud provider to Foresight Cyber logging platform.

DURING A CLOUD SERVICE PROCUREMENT

Requirement 7: Perform due diligence activities before the contract is signed

Justification: If cloud services are being purchased outside Foresight Cyber purchasing process, then the necessary assessments are missed. Proper process ensures technology solutions are fit for Foresight Cyber and do not increase the risk to unacceptable levels.

Detailed requirements:

1. Follow procurement process by involving procurement in any selection of cloud services.
2. Follow the Security Acceptance into Service process
3. Ensure that a copy of all contract documentation (terms and conditions) are downloaded, dated and archived to enable them to be reviewed and available in the case of a dispute
4. Require contracts to be reviewed for security requirements as adding the security requirements later is sometimes impossible or costly.
5. Require cloud providers to fully describe the service, such as: a diagram showing how and where the service will be delivered, the name of the provider of each component, the security controls in place for each component, the contractual arrangements that are in place between the suppliers of the different components.
6. Ensure the contract provides adequate protection in the event of cloud services being sub-contracted, such as: who will provide what services and in which jurisdiction, the security controls that will be in place, the SLAs that will be delivered, where liability lies and the level of liability.
7. Require the cloud provider to provide notification prior to any changes being made to the way the service is delivered
8. Review the controls the cloud provider uses to remove information once it is obsolete, such as:
    a) examining the cloud provider's information destruction processes
    b) checking how policies apply to the destruction of confidential information on redundant systems and information backups
    c) determining how information stored in shared media locations is removed (e.g. information in a common database)
9. Determine whether the cloud service is suitable for Foresight Cyber's data destruction requirements or can be modified to meet them by negotiation before purchasing the service.
10. Clearly define all information retention and destruction requirements in the contract with the cloud provider including details of how confidential information will be retained / destroyed at the end of its life and the end of the contract.

Requirement 8: Request "Right to review audit" clause in the contract

Justification: While Foresight Cyber may not exercise the right to audit for all Cloud providers, not having the right to review the audit results may constitute a breach of clients' contracts.

Detailed requirements:

1. Negotiate the right to see the results of security audits
2. Review audit results at agreed regular intervals and randomly

Requirement 9: Know locations of personal identifiable information in the cloud

Justification: Privacy (or data protection) legislation typically places restrictions on the geographical locations that can be used to store personally identifiable information. Often it specifies that information can only be stored in recognized jurisdictions and restricts the movement of the information across national boundaries. Placing personally identifiable information in the cloud may result in Foresight Cyber breaching privacy laws or regulations – possibly incurring severe penalties and causing reputational damage.

Detailed requirements:

1. Require cloud providers to restrict the storage of personally identifiable information to approved locations (including DR facilities).
2. Require cloud providers to give written notification of any changes to the proposed location of personally identifiable information
3. Assess the risks to Foresight Cyber of a data protection / privacy breach at the cloud provider

Requirement 10: Assess the availability and recovery capabilities of the Cloud services

Justification: Cloud services offer flexible and sometimes inexpensive way of supporting business processes. However, disasters and other disruptions can happen, such as criminal investigations, and the potential business impact for lost time and data can be order of a magnitude bigger than the compensation from the cloud provider.

Detailed requirement:

1. Evaluate the availability requirements and the business impact of the cloud computing service in case of disaster or criminal investigation
2. Request the Cloud provider's disaster recovery plan and update Foresight Cyber's plans accordingly:
3. Add SLAs and compensation clauses in the contract, based on impact of loss of service or loss of access to service.

Requirement 11: Assess the cloud provider's security arrangements

Justification: Foresight Cyber needs to exercise due diligence when acquiring services of 3rd parties, including the Cloud providers.

Detailed requirement:

1. Require the cloud provider to provide information about the security architecture, the security controls deployed to protect their services and details of any incidents they have experienced via the 3rd party assessment.
2. Obtain details of the timing, scope, results and mitigating actions for any independent audits or certification assessments performed on the cloud provider and its services

Requirement 12: Assess the Cloud provider's ability to comply with Foresight Cyber forensic investigations

Justification: Foresight Cyber must exercise due diligence and be able to perform forensic investigations on Systems and Data provided to Foresight Cyber by the Cloud Provider, and on Systems, Data, and Processes used by the Cloud Provider to provision and manage the Foresight Cyber Cloud infrastructure.

Detailed requirements:

1. Include a forensic assessment as part of the cloud services review. A forensic vulnerability assessment should include:
   a) determining the level of access available from the cloud provider to perform forensic investigations
   b) an examination of the processes around the chain of custody of evidence
   c) investigation of alternative event logging activities to support forensic investigations, identifying their associated costs

RUNNING A CLOUD SERVICE

Requirement 13: Limit use of live data for testing and development purposes

Justification: Foresight Cyber may face issues related to the privacy of personally identifiable information if the test information is an exact copy of the live information.

Detailed requirements:

1. Determine if information can be used to test cloud services

2. Sanitise test information using a structured approach and signed off by the CISO prior to use in testing cloud services

Requirement 14: Maintain security of cloud environments

Justification: Running IT systems and Business applications, observing the constrains and principles of Shared Responsibility Model, is key control to ensure Foresight Cyber maintains the business benefits of cloud computing whilst limiting business, security and compliance risks.

Detailed Requirements:

1. Secure all cloud systems and applications according to information security policy requirements, adjusting controls to fit the Shared Responsibility model and cloud specific attributes
2. Monitor improvements in security controls natively available by cloud providers that allow Foresight Cyber secure workloads, and implement these by default unless there is a good business justification not to do so, an exception can be approved by CTO

Requirement 15: Monitor Cloud providers security arrangements

Justification: Security arrangements need to be monitored not just at the point of contract signing but throughout the contract life, in order to ensure that the security of Foresight Cyber data and processes is not affected.

Detailed requirements:

1. Where possible integrate Cloud provider logging and monitoring solution with that of Foresight Cyber
2. At minimum annually, review Cloud provider security posture

DECOMMISSIONING A CLOUD SERVICE

Requirement 16: Destroy sensitive information when no longer required

Justification: Information may be exposed to unauthorized access. In some cases, information may be more exposed after the service has terminated because the cloud provider is no longer obligated to maintain any additional controls, specified in the contract.

Detailed requirement:

1. Remove Foresight Cyber Data from the cloud provider system, application, data storage
2. Remove technical integrations, such as IAM, logging, data transfers
3. Update the CMDB to reflect the decommissioning of the cloud service

DEFINITIONS, ABBREVIATIONS AND ACRONYMS

For the purpose of this standard the following terms are defined as per industry best practice defined by NIST SP 800-145.

Essential Characteristics

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models

- Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.

- Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

- Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Foresight Cyber Ltd

Registered address:
International House, 24 Holborn Viaduct,
City of London, London, EC1A 2BN,
United Kingdom

Business address UK:
Universal House, Suite 3,56-58 Clarence Street,
Kingston upon Thames, KT1 1NP,
United Kingdom

Business address CZ:
Fryštátská 64/9, 733 01 Karvina,
Czech Republic

Contacts:
UK Office: +44 20 7183 9858
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017

OUR CERTIFICATIONS

aws CERTIFIED Solutions Architect Associate

CISSP® ISSAP®

CCSP℠

CISSP® ISSMP®

CISSP®

CISCO CERTIFIED CCNA

CCSK™ Certificate of Cloud Security Knowledge

CYBER ESSENTIALS PLUS

Qualys®

SKYBOX™ SECURITY