https://t.me/learningnets

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors.

Contact details:

This report has been edited by:

e-mail: Daniele.catteddu@enisa.europa.eu and Giles.hogben@enisa.europa.eu,

Internet: http://www.enisa.europa.eu/

Legal notice

Notice must be taken that this publication represents the views and interpretations of the editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of the-art in cloud computing and it may be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2009

https://t.me/learningnets

CONTENTS

https://t.me/learningnets

https://t.me/learningnets

TARGET AUDIENCE

The intended audience of this report are:

- Business leaders, in particular SME's to evaluate and mitigate the risks of adopting cloud computing technologies.
- Cloud Provider to standardize their cloud computing service compliance process vis a vis laws and regulations
- European policymakers to decide on research policy (to develop technologies to mitigate risks).
- European policymakers to decide on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives etc vis-a-vis cloud-computing technologies.

METHODOLOGY

The key sections of this document are based on the broad classes of controls from the ISO 27001/2 and BS25999 standards. Details within these sections are derived from both the standard, as well as industry best practice requirements. Throughout, we have selected only those controls which are relevant to cloud providers and third party outsourcers.

The detailed framework scheduled for release in 2010 is intended to include additional standards such as NIST SP 800-53.

https://t.me/learningnets

1. INFORMATION ASSURANCE FRAMEWORK

One of the most important recommendations in the ENISA's Cloud Computing Risk Assessment report (see full version) is the Information Assurance Framework, a set of assurance criteria designed to:

1. assess the risk of adopting cloud services (comparing the risks of maintaining a 'classical' organization and architecture with risks to migrate in a cloud computing environment) and
2. compare different Cloud Provider offers
3. obtain assurance from the selected cloud providers. The preparation of effective security questionnaires for third party service providers is a significant resource drain for cloud customers and one which is difficult to achieve without expertise in cloud-specific architectures.
4. reduce the assurance burden on cloud providers. A very important risk specific to cloud infrastructures is introduced by the requirement for NIS assurance. Many cloud providers find that a large number of customers request audits of their infrastructure and policies. This can create a critically high burden on security personnel and it also increases the number of people with access to the infrastructure, which significantly increases the risk of attack due to misuse of security-critical information, theft of critical or sensitive data etc. Cloud providers will need to deal with this by establishing clear framework for handling such requests.

The Framework provides a set of questions that an organisation can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them.

These questions are intended to provide a minimum baseline any organisation may therefore have additional specific requirements not covered within the baseline.

Equally this document does not provide a standard response format for the cloud provider, so responses are in a free text format. However it is intended to feed into a more detailed comprehensive framework which will be developed as a follow-up to this work, allowing a consistent, comparable set of responses. Such responses will provide a quantifiable metric as to the Information Assurance maturity of the provider.

It is intended for the aforementioned metric to be consistent against other providers that allow a comparison for end user organisations.

https://t.me/learningnets

2. MANAGING RISK

It is worth noting that although it is possible to transfer many of the risks to an externally provisioned supplier, the true cost of transferring risk is very rarely realised. For example, a security incident that results in the unauthorised disclosure of customer data may result in financial loss to the provider, however the negative publicity and loss of consumer confidence, and potential regulatory penalties (PCI-DSS) would be felt by the end customer. Such a scenario highlights the importance of distinguishing risk, with commercial risk. In that it is possible to transfer commercial risk, but the true risk always remains with the end customer.

Any response to the results of a risk assessment - in particular the amount and type of investment in mitigation, should be decided on the basis of the risk appetite of the organisation and the opportunities and financial savings which are lost by following any particular risk mitigation strategy.

Cloud customers should also carry out their own, context-specific risk analysis. Some of available Risk Management / Risks Assessment methodologies can be found at: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

As the business and regulatory environment changes and new risks arise, risk assessment should be a regular activity rather than a one off event.

3. DIVISION OF LIABILITIES

The following table shows the expected division of liabilities between customer and provider.

	Customer	Provider
Lawfulness of content	Full liability	Intermediary liability with Liability exemptions under the terms of the E-commerce Directive and its interpretation.[1]

[1] Cf. definition of information society services as provided for in Art. 2 of Directive 98/48/EC as well as Art. 2 of Directive 2000/31/EC, in conjunction with exemptions contained in Articles 12-15 of Directive 2000/31/EC (e-Commerce Directive).

https://t.me/learningnets

Security incidents (including data leakage, use of account to launch an attack)	Responsibility for due diligence for what is under its control according to contractual conditions	Responsibility for due diligence for what is under its control
European Data Protection Law status	Data controller	Data processor (external)

4. DIVISION OF RESPONSIBILITIES

With respect to security incidents, there needs to be a clear definition and understanding between the customer and the provider of security-relevant roles and responsibilities. The lines of such a division will vary greatly between SaaS offerings and IaaS offerings, with the latter delegating more responsibility to the customer. A typical and rational division of responsibility is shown in the following table. *In any case, for each type of service, the customer and provider should clearly define which of them is responsible for all the items on the list below.* In the case of standard terms of service (ie, no negotiation possible), cloud customers should verify what lies within their responsibility.

4.1. SOFTWARE AS A SERVICE

Customer	Provider
• Compliance with data protection law in respect of customer data collected and processed • Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy)	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Security platform configuration (Firewall rules, IDS/IPS tuning, etc) • Systems monitoring • Security platform maintenance (Firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring

https://t.me/learningnets

4.2. PLATFORM AS A SERVICE

Customer	Provider
• Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy)	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Security platform configuration (firewall rules, IDS/IPS tuning, etc) • Systems monitoring • Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring

4.3. INFRASTRUCTURE AS A SERVICE

Customer	Provider
• Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy) • Management of guest OS patch and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Configuration of guest security platform (firewall rules, IDS/IPS tuning, etc)	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • Host Systems (hypervisor, virtual firewall, etc)

https://t.me/learningnets

• Guest systems monitoring • Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring	

Where cloud customers are responsible for the security of their Infrastructures (in IaaS), they should consider the following:

4.3.1. Application Security in Infrastructure as a Service

IaaS application providers treat the applications within the customer virtual instance as a 'black box' and therefore are completely agnostic to the operations and management of a customer's applications. The entire 'stack' – customer application, run time application platform (.Net, Java, Ruby, PHP etc) is run on the customers' server (on provider infrastructure) and is managed by customers themselves. For this reason it is vitally important to note that the customer must take full responsibility for securing their cloud deployed applications. Here is a brief checklist/description relating to best practice for secure application design and management:

- Cloud deployed applications must be designed for the internet threat model (even if they are deployed as part of VPC - virtual private cloud).
- They must be designed/embedded with standard security countermeasures to guard against the common web vulnerabilities (see OWASP guides).
- Customers are responsible for keeping their applications up to date – and must therefore ensure they have a patch strategy (to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorised access to their data within the cloud)
- Customers should not be tempted to use custom implementations of Authentication, Authorisation and Accounting (AAA) as these can become weak if not properly implemented.

In summary – enterprise distributed cloud applications must run with many controls in place to secure host (and network – see previous section), user access, application level controls (see OWASP guides relating to secure web/online application design). Also please note many main stream vendors such as Microsoft, Oracle, Sun etc publish comprehensive documentation on how to secure the configuration of their products.

https://t.me/learningnets

5. NOTE OF CAUTION

The series of questions detailed within the proceeding section are a selection of common controls. It is not intended to be an exhaustive list; equally certain questions may not be applicable to particular implementations. Subsequently this list should be used as a baseline of common controls, and further detail should be sought where required.

5.1. NOTE TO GOVERNMENTS

The following controls are aimed primarily at SMEs assessing cloud providers. They may also be useful to governments with the following provisos. *The characteristics of the cloud used should be considered carefully in relation to any government body's information classification scheme.*

- The use of public clouds – even with favourable responses from the following questionnaire – is not recommended for anything but the lowest assurance classes of data.
- For higher assurance classes of data, the list of suggested checks in this report is valid but should be supplemented with additional checks. This report is not intended to cover such controls, but the following are examples of issues which should be covered:
    - Does the provider offer transparent information and full control over the current physical location of all data? High assurance data is often restricted by location.
    - Does the provider support the data classification scheme used?
    - What guarantees does the provider offer that customer resources are fully isolated (e.g., no sharing of physical machines)?
    - Assuming physical machines are not shared between customers, to what degree are storage, memory and other data traces fully erased before machines are reallocated.
    - Does the provider support or even mandate physical token based 2-factor authentication for client access?
    - Does the provider hold ISO 27001/2 certification? What is the scope of the certification?
    - Do the products used by the provider have Common Criteria certifications? At which level? Which protection profile and security target for the product?

https://t.me/learningnets

6. INFORMATION ASSURANCE REQUIREMENTS

6.1. PERSONNEL SECURITY

The majority of questions relating to personnel will be similar to those you would ask your own IT personnel or other personnel who are dealing with your IT. As with most assessments, there is a balance between the risks and the cost.

- What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include:
  - pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting (for senior personnel in high privilege roles)).
- Are there different policies depending on where the data is stored or applications are run?
  - For example, hiring policies in one region may be different from those in another.
  - Practices need to be consistent across regions.
  - It may be that sensitive data is stored in one particular region with appropriate personnel.
- What security education program do you run for all staff?
- Is there a process of continuous evaluation?
  - How often does this occur?
  - Further interviews
  - Security access and privilege reviews
  - Policy and procedure reviews.

6.2. SUPPLY-CHAIN ASSURANCE

The following questions apply where the cloud provider subcontracts some operations that are key to the security of the operation to third parties (eg, a SaaS provider outsourcing the underling platform to a third party provider, a cloud provider outsourcing the security services to a managed security services provider, use of an external provider for identity management of operating systems, etc). It also includes third parties with physical or remote access to the cloud provider infrastructure. It is assumed that this entire questionnaire may be applied recursively to third (or nth) party cloud service providers.

- Define those services that are outsourced or subcontracted in your service delivery supply chain that are key to the security (including availability) of your operations.
- Detail the procedures used to assure third parties accessing your infrastructure (physical and/or logical).
  - Do you audit your outsourcers and subcontractors and how often?
- Are any SLA provisions guaranteed by outsourcers lower than the SLAs you offer to your customers? If not, do you have supplier redundancy in place?

https://t.me/learningnets

- What measures are taken to ensure third party service levels are met and maintained?
- Can the cloud provider confirm that security policy and controls are applied (contractually) to their third party providers?

6.3. OPERATIONAL SECURITY

It is expected that any commercial agreement with external providers will include service levels for all network services. However, in addition to the defined agreements, the end customer should still ensure that the provider employs appropriate controls to mitigate unauthorised disclosure.

- Detail your change control procedure and policy. This should also include the process used to re-assess risks as a result of changes and clarify whether the outputs are available to end customers.
- Define the remote access policy.
- Does the provider maintain documented operating procedures for information systems?
- Is there a staged environment to reduce risk, e.g., development, test and operational environments, and are they separated?
- Define the host and network controls employed to protect the systems hosting the applications and information for the end customer. These should include details of certification against external standards (e.g., ISO 27001/2).
- Specify the controls used to protect against malicious code.
- Are secure configurations deployed to only allow the execution of authorised mobile code and authorised functionality (e.g., only execute specific commands)?
- Detail policies and procedures for backup. This should include procedures for the management of removable media and methods for securely destroying media no longer required. (Depending on his business requirements, the customer may wish to put in place an independent backup strategy. This is particularly relevant where time-critical access to back-up is required.)

Audit logs are used in the event of an incident requiring investigation; they can also be used for troubleshooting. For these purposes, the end customer will need assurance that such information is available:

- Can the provider detail what information is recorded within audit logs?
  - For what period is this data retained?
  - Is it possible to segment data within audit logs so they can be made available to the end customer and/or law enforcement without compromising other customers and still be admissible in court?
  - What controls are employed to protect logs from unauthorised access or tampering?
  - What method is used to check and protect the integrity of audit logs?

https://t.me/learningnets

- How are audit logs reviewed? What recorded events result in action being taken?
- What time source is used to synchronise systems and provide accurate audit log time stamping?

6.3.1. SOFTWARE ASSURANCE

- Define controls used to protect the integrity of the operating system and applications software used. Include any standards that are followed, e.g., OWASP, SANS Checklist , SAFECode.
- How do you validate that new releases are fit-for-purpose or do not have risks (backdoors, Trojans, etc)? Are these reviewed before use?
- What practices are followed to keep the applications safe?
- Is a software release penetration tested to ensure it does not contain vulnerabilities? If vulnerabilities are discovered, what is the process for remedying these?

6.3.2. PATCH MANAGEMENT

- Provide details of the patch management procedure followed.
- Can you ensure that the patch management process covers all layers of the cloud delivery technologies – i.e., network (infrastructure components, routers and switches, etc), server operating systems, virtualisation software, applications and security subsystems (firewalls, antivirus gateways, intrusion detection systems, etc)?

6.3.3. NETWORK ARCHITECTURE CONTROLS

- Define the controls used to mitigate DDoS (distributed denial–of-service) attacks.
  - Defence in depth (deep packet analysis, traffic throttling, packet black-holing, etc)
  - Do you have defences against 'internal' (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks?
- What levels of isolation are used?
  - for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.
- Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa (e.g., is there a critical dependency on the customer LDAP system)?
- Is the virtual network infrastructure used by cloud providers (in PVLANs and VLAN tagging 802.1q architecture) secured to vendor and/or best practice specific standards (e.g., are MAC spoofing, ARP poisoning attacks, etc, prevented via a specific security configuration)?

https://t.me/learningnets

6.3.4. HOST ARCHITECTURE

- Does the provider ensure virtual images are hardened by default?
- Is the hardened virtual image protected from unauthorized access?
- Can the provider confirm that the virtualised image does not contain the authentication credentials?
- Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?
- Can a host-based intrusion prevention service (IPS) be run in the virtual instance?

6.3.5. PAAS – APPLICATION SECURITY

Generally speaking, PaaS service providers are responsible for the security of the platform software stack, and the recommendations throughout this document are a good foundation for ensuring a PaaS provider has considered security principles when designing and managing their PaaS platform. It is often difficult to obtain detailed information from PaaS providers on exactly how they secure their platforms – however the following questions, along with other sections within this document, should be of assistance in assessing their offerings.

- Request information on how multi-tenanted applications are isolated from each other – a high level description of containment and isolation measures is required.
- What assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?
- The platform architecture should be classic 'sandbox' – does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?
- PaaS providers should be able to offer a set of security features (re-useable amongst their clients) – do these include user authentication, single sign on, authorisation (privilege management), and SSL/TLS (made available via an API)?

6.3.6. SAAS – APPLICATION SECURITY

The SaaS model dictates that the provider manages the entire suite of applications delivered to end-users. Therefore SaaS providers are mainly responsible for securing these applications. Customers are normally responsible for operational security processes (user and access management). However the following questions, along with other sections within this document, should assist in assessing their offerings:

- What administration controls are provided and can these be used to assign read and write privileges to other users?

https://t.me/learningnets

- Is the SaaS access control fine grained and can it be customised to your organisations policy?

6.3.7. RESOURCE PROVISIONING

- In the event of resource overload (processing, memory, storage, network)?
  - What information is given about the relative priority assigned to my request in the event of a failure in provisioning?
  - Is there a lead time on service levels and changes in requirements?
- How much can you scale up? Does the provider offer guarantees on maximum available resources within a minimum period?
- How fast can you scale up? Does the provider offer guarantees on the availability of supplementary resources within a minimum period?
- What processes are in place for handling large-scale trends in resource usage (eg, seasonal effects)?

6.4. IDENTITY AND ACCESS MANAGEMENT

The following controls apply to the cloud provider's identity and access management systems (those under their control).

6.4.1. AUTHORISATION

- Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)?
- How are the accounts with the highest level of privilege authenticated and managed?
- How are the most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) authorised (single or dual, and by which roles within the organisation)?
- Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?
- Do you use role-based access control (RBAC)? Is the principle of least privilege followed?
- What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency?
- Is there an 'administrator' role for the customer? For example, does the customer administrator have a role in adding new users (but without allowing him to change the underlying storage!)?

https://t.me/learningnets

6.4.2. IDENTITY PROVISIONING

- What checks are made on the identity of user accounts at registration? Are any standards followed? For example, the e-Government Interoperability Framework?
  - Are there different levels of identity checks based on the resources required?
- What processes are in place for de-provisioning credentials?
- Are credentials provisioned and de-provisioned simultaneously throughout the cloud system, or are there any risks in de-provisioning them across multiple geographically distributed locations?

6.4.3. MANAGEMENT OF PERSONAL DATA

- What data storage and protection controls apply to the user directory (eg, AD, LDAP) and access to it?
- Is user directory data exportable in an interoperable format?
- Is need-to-know the basis for access to customer data within the cloud provider?

6.4.4. KEY MANAGEMENT

For keys under the control of the cloud provider:

- Are security controls in place for reading and writing those keys? For example, strong password policies, keys stored in a separate system, hardware security modules (HSM) for root certificate keys, smart card based authentication, direct shielded access to storage, short key lifetime, etc.
- Are security controls in place for using those keys to sign and encrypt data?
- Are procedures in place in the event of a key compromise? For example, key revocation lists.
- Is key revocation able to deal with simultaneity issues for multiple sites?
- Are customer system images protected or encrypted?

6.4.5. ENCRYPTION

- Encryption can be used in multiple places – where is it used?
  - data in transit
  - data at rest
  - data in processor or memory?
- Usernames and passwords?
- Is there a well-defined policy for what should be encrypted and what should not be encrypted?

https://t.me/learningnets

- Who holds the access keys?
- How are the keys protected?

6.4.6. AUTHENTICATION

- What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.
  - Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc?

6.4.7. CREDENTIAL COMPROMISE OR THEFT

- Do you provide anomaly detection (the ability to spot unusual and potentially malicious IP traffic and user or support team behaviour)? For example, analysis of failed and successful logins, unusual time of day, and multiple logins, etc.
- What provisions exist in the event of the theft of a customer's credentials (detection, revocation, evidence for actions)?

6.4.8. IDENTITY AND ACCESS MANAGEMENT SYSTEMS OFFERED TO THE CLOUD CUSTOMER

The following questions apply to the identity and access management systems which are offered by the cloud provider for use and control by the cloud customer.

6.4.8.1. IDENTITY MANAGEMENT FRAMEWORKS

- Does the system allow for a federated IDM infrastructure which is interoperable both for high assurance (OTP systems, where required) and low assurance (eg. username and password)?
- Is the cloud provider interoperable with third party identity providers?
- Is there the ability to incorporate single sign-on?

6.4.8.2. ACCESS CONTROL

- Does the client credential system allow for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)?
- How do you manage access to customer system images – and ensure that the authentication and cryptographic keys are not contained within in them?

https://t.me/learningnets

6.4.8.3. AUTHENTICATION

- How does the cloud provider identify itself to the customer (ie, is there mutual authentication)?
  - when the customer sends API commands?
  - when the customer logs into the management interface?
- Do you support a federated mechanism for authentication?

6.5. ASSET MANAGEMENT

It is important to ensure the provider maintains a current list of hardware and software (applications) assets under the cloud providers control. This enables checks that all systems have appropriate controls employed, and that systems cannot be used as a backdoor into the infrastructure.

- Does the provider have an automated means to inventory all assets, which facilitates their appropriate management?
- Is there a list of assets that the customer has used over a specific period of time?

The following questions are to be used where the end customer is deploying data that would require additional protection (i.e.. deemed as sensitive).

- Are assets classified in terms of sensitivity and criticality?
  - If so, does the provider employ appropriate segregation between systems with different classifications and for a single customer who has systems with different security classifications?

6.6. DATA AND SERVICES PORTABILITY

This set of questions should be considered in order to understand the risks related to vendor lock-in.

- Are there documented procedures and APIs for exporting data from the cloud?
- Does the vendor provide interoperable export formats for all data stored within the cloud?
- In the case of SaaS, are the API interfaces used standardised?
- Are there any provisions for exporting user-created applications in a standard format?
- Are there processes for testing that data can be exported to another cloud provider – should the client wish to change provider, for example?
- Can the client perform their own data extraction to verify that the format is universal and is capable of being migrated to another cloud provider?

https://t.me/learningnets

6.7. Business Continuity Management

Providing continuity is important to an organisation. Although it is possible to set service level agreements detailing the minimum amount of time systems are available, there remain a number of additional considerations.

- Does the provider maintain a documented method that details the impact of a disruption?
  - What are the RPO (recovery point objective) and RTO (recovery time objective) for services? Detail according to the criticality of the service.
  - Are information security activities appropriately addressed in the restoration process?
  - What are the lines of communication to end customers in the event of a disruption?
  - Are the roles and responsibilities of teams clearly identified when dealing with a disruption?
- Has the provider categorised the priority for recovery, and what would be our relative priority (the end customer) to be restored? Note: this may be a category (HIGH/MED/LOW).
- What dependencies relevant to the restoration process exist? Include suppliers and outsource partners.
- In the event of the primary site being made unavailable, what is the minimum separation for the location of the secondary site?

6.7.1. Incident management and response

Incident management and response is a part of business continuity management. The goal of this process is to contain the impact of unexpected and potentially disrupting events to an acceptable level for an organization.

To evaluate the capacity of an organization to minimize the probability of occurrence or reduce the negative impact of an information security incident, the following questions should be asked to a cloud provider:

- Does the provider have a formal process in place for detecting, identifying, analyzing and responding to incidents?
- Is this process rehearsed to check that incident handling processes are effective? Does the provider also ensure, during the rehearsal, that everyone within the cloud provider's support organisation is aware of the processes and of their roles during incident handling (both during the incident and post analysis)?
- How are the detection capabilities structured?
  - How can the cloud customer report anomalies and security events to the provider?
  - What facilities does the provider allow for customer-selected third party RTSM services to intervene in their systems (where appropriate) or to co-ordinate incident response capabilities with the cloud provider?

https://t.me/learningnets

- Is there a real time security monitoring (RTSM) service in place? Is the service outsourced? What kind of parameters and services are monitored?
- Do you provide (upon request) a periodical report on security incidents (eg,. according to the ITIL definition)?
- For how long are the security logs retained? Are those logs securely stored? Who has access to the logs?
- Is it possible for the customer to build a HIPS/HIDS in the virtual machine image? Is it possible to integrate the information collected by the intrusion detection and prevention systems of the customer into the RTSM service of the cloud provider or that of a third party?

- How are severity levels defined?
- How are escalation procedures defined? When (if ever) is the cloud customer involved?
- How are incidents documented and evidence collected?
- Besides authentication, accounting and audit, what other controls are in place to prevent (or minimize the impact of) malicious activities by insiders?
- Does the provider offer the customer (upon request) a forensic image of the virtual machine?
- Does the provider collect incident metrics and indicators (ie,. number of detected or reported incidents per months, number of incidents caused by the cloud provider's subcontractors and the total number of such incidents, average time to respond and to resolve, etc)?).
  - Which of these does the provider make publicly available (NB not all incident reporting data can be made public since it may compromise customer confidentiality and reveal security critical information)??)
- How often does the provider test disaster recovery and business continuity plans?
- Does the provider collect data on the levels of satisfaction with SLAs?
- Does the provider carry out help desk tests? For example:
  - Impersonation tests (is the person at the end of the phone requesting a password reset, really who they say they are?) or so called 'social engineering' attacks.
- Does the provider carry out penetration testing? How often? What are actually tested during the penetration test – for example, do they test the security isolation of each image to ensure it is not possible to 'break out' of one image into another and also gain access to the host infrastructure?. The tests should also check to see if it is possible to gain access, via the virtual image, to the cloud providers management and support systems (e.g, example the provisioning and admin access control systems).
- Does the provider carry out vulnerability testing? How often?
- What is the process for rectifying vulnerabilities (hot fixes, re-configuration, uplift to later versions of software, etc)?

https://t.me/learningnets

6.8. PHYSICAL SECURITY

As with personnel security, many of the potential issues arise because the IT infrastructure is under the control of a third party – like traditional outsourcing, the effect of a physical security breach can have an impact on multiple customers (organizations).

- What assurance can you provide to the customer regarding the physical security of the location? Please provide examples, and any standards that are adhered to, eg,. Section 9 of ISO 27001/2.
    - Who, other than authorised IT personnel, has unescorted (physical) access to IT infrastructure?
        - For example, cleaners, managers, 'physical security' staff, contractors, consultants, vendors, etc.
    - How often are access rights reviewed?
        - How quickly can access rights be revoked?
    - Do you assess security risks and evaluate perimeters on a regular basis?
        - How frequently?
    - Do you carry out regular risk assessments which include things such as neighboring buildings?
    - Do you control or monitor personnel (including third parties) who access secure areas?
    - What policies or procedures do you have for loading, unloading and installing equipment?
    - Are deliveries inspected for risks before installation?
    - Is there an up-to-date physical inventory of items in the data centre?
    - Do network cables run through public access areas?
        - Do you use armoured cabling or conduits?
    - Do you regularly survey premises to look for unauthorized equipment?
    - Is there any off-site equipment?
        - How is this protected?
    - Do your personnel use portable equipment (eg,. laptops, smart phones) which can give access to the data centre?
        - How are these protected?
    - What measures are in place to control access cards?
    - What processes or procedures are in place to destroy old media or systems when required to do so?
        - data overwritten?
        - physical destruction?

https://t.me/learningnets

- What authorization processes are in place for the movement of equipment from one site to another?
  - How do you identify staff (or contractors) who are authorized to do this?
- How often are equipment audits carried out to monitor for unauthorised equipment removal?
- How often are checks made to ensure that the environment complies with the appropriate legal and regulatory requirements?

6.9. ENVIRONMENTAL CONTROLS

- What procedures or policies are in place to ensure that environmental issues do not cause an interruption to service?
- What methods do you use to prevent damage from a fire, flood, earthquake, etc?
  - In the event of a disaster, what additional security measures are put in place to protect physical access?
  - Both at the primary as well as at the secondary sites?
- Do you monitor the temperature and humidity in the data centre?
  - Air-conditioning considerations or monitoring?
- Do you protect your buildings from lightening strikes?
  - Including electrical and communication lines?
- Do you have stand-alone generators in the event of a power failure?
  - For how long can they run?
  - Are there adequate fuel supplies?
  - Are there failover generators?
  - How often do you check UPS equipment?
  - How often do you check your generators?
  - Do you have multiple power suppliers?
- Are all utilities (electricity, water, etc) capable of supporting your environment?
  - How often is this re-evaluated and tested?
- Is your air-conditioning capable of supporting your environment?
  - How often is it tested?
- Do you follow manufacturers recommended maintenance schedules?
- Do you only allow authorised maintenance or repair staff onto the site?
  - How do you check their identity?
- When equipment is sent away for repair, is the data cleaned from it first?
  - How is this done?

https://t.me/learningnets

6.10. LEGAL REQUIREMENTS

Customers and potential customers of cloud provider services should have regard to their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with.
The key legal questions the customer should ask the cloud provider are:

- In what country is the cloud provider located?
- Is the cloud provider's infrastructure located in the same country or in different countries?
- Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
- Where will the data be physically located?
- Will jurisdiction over the contract terms and over the data be divided?
- Will any of the cloud provider's services be subcontracted out?
- Will any of the cloud provider's services be outsourced?
- How will the data provided by the customer and the customer's customers, be collected, processed and transferred?
- What happens to the data sent to the cloud provider upon termination of the contract?

https://t.me/learningnets