Regulatory Framework for Fraud Disclosure on Cloud Computing Environments

Dimitrios D. Vergados[1,2] and Theodoros Mavroeidakos[1,3]

[1]Department of Informatics, University of Piraeus
80, Karaoli and Dimitriou St., GR-185 34, Piraeus, Greece
Email: vergados@unipi.gr
Tel: +30 210 4142479
Fax: +30 210 4142119

[2]Hellenic Telecommunications and Post Commission (EETT)
60, Kifissias Avenue
GR- 151 25 Maroussi, Greece

[3]National Technical University of Athens, Greece
Heroon Polytechniou 9, GR-15780 Zografou, Greece
Email: mavroeidakos.theodoros@gmail.com

Outline

Introduction

What happens today?

- Cloud Computing constitutes an emerging computing paradigm consisting of elements of grid computing, utility computing and software-defined networks (SDN).
- Cloud computing can deliver a vast majority of IT capabilities in real time using many different types of resources.
- Cloud computing provides cost-efficient opportunities for companies and organizations by offering a variety of dynamic, scalable, and shared services.

Cloud Computing Environment

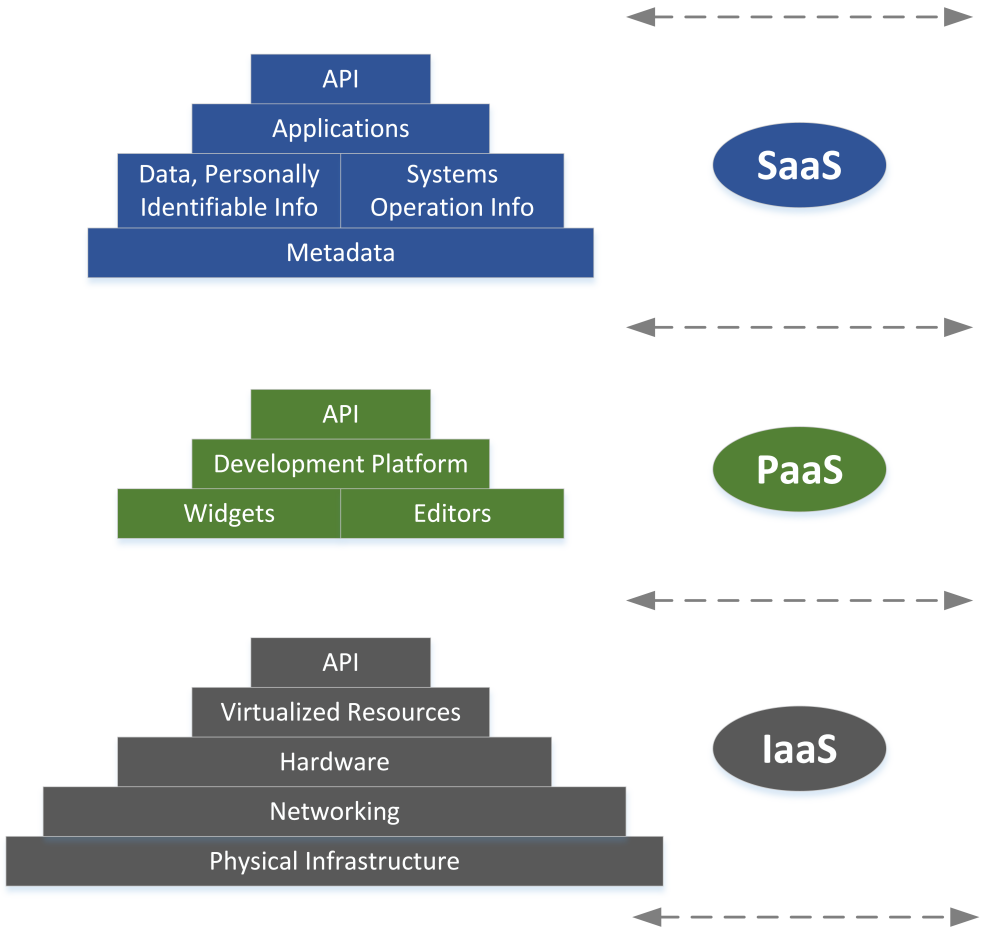
- Cloud computing (CC) environments provide capabilities which are unique among the distributed environments, covering the existing and future needs of organizations and companies.
- According to NIST the CC environments are characterized by:
  - **On-demand self-service** of resources without human interaction in order to achieve it.
  - **Broad network access** for the provision of end-service and access to CC resources through standard thin client mechanisms.
  - **Resource pooling** is made available due to a multi-tenant model which assign CC resources according to consumer demand.
  - **Rapid elasticity** offers the capability of unlimited resources for provisioning to its consumers at any time.
  - **Measured service** provides monitoring and control over the provisioned resources during the operation of an end-service.

Cloud Computing Environment

- The infrastructure of CC provider can be constructed following one of main deployment models according the needs of the end-service.
- The deployment models of the CC environments are:
  - **Private**
  - **Public**
  - **Community**
  - **Hybrid**
- Certain notable characteristics of the deployment models:
  - Private cloud is managed exclusively by an organization.
  - Hybrid cloud is characterized by the scalability of the public cloud and the level of security of the private cloud. There are several tradeoffs in how the hybrid cloud can be constructed according the main goals of the CC provider.

Cloud Computing Environment

- Through the CC environments three main service models can be used for the provision of the end-service according the type of clients and the business objective.



CC Service Models

Cloud Computing Environment

Software-as-a-Service (SaaS)

- Following the SaaS model, the end-service is an application. The software of this application operates by using the CC resources.
- The clients are not responsible about the underlying operation of the software.
- Clients:
  - have minimum responsibilities and liabilities concerning the software security.
  - are responsible about the data that manage by using the SaaS.

Cloud Computing Environment

Platform-as-a-Service (PaaS)

- The PaaS model offers to clients the capability to built their own applications by using a software platform and utilizing the CC resources.
- The clients use the development environment which is part of this type of service in order to write the core software of their application.
- The clients do not control the underlying CC resources, however they are responsible about the security of their code.
- The CC provider is liable about the software platform as well as about the CC resources and challenges (e.g. intranets, network traffic, type of servers).

Cloud Computing Environment

Infrastructure-as-a-Service (IaaS)

- In the IaaS model the provider offers virtualized resources such as servers, loadbalancers and firewalls which are hosted by CC environment.
- This type of service provides scalable capabilities to the IT sector of enterprises.
- In this type of service, the clients are responsible about the security of the virtualized resources as well the data which are managed in them.
- The CC provider is liable only about physical threats to the physical assets of its infrastructure.

Cloud Computing Environment

Security dependencies in service models:

- The PaaS and SaaS models are hosted in the CC environment by the IaaS model.
- The SaaS model can be exposed with two ways:
  - through the PaaS as an application constructed in the software platform
  - or directly though native cloud mechanisms which integrate the end-service with the CC resources.
- Security threats and vulnerabilities that exist in the IaaS model, exist also in the other models inductively.
- In the PaaS model exist two security challenges:
  - the protection of data which are collected by the SaaS that is constructed in the platform
  - the security level of the software platform

Cloud Computing Environment

Involved parties in the provision of the CC end-services:

In the Cloud, the responsibility is divided among potentially many parties including the:

- Provider
- Clients
- Third-party of Inspection

- The **clients** are entities which use the end-service of a CC provider.
- **Third-party of Inspection** is a governmental authority or a group of people with main goal the finding of security threats and mitigation of them. More specifically this party:
  - **audits** the CC environment
  - **defines** the level of security
  - **confirms** the fulfilment of the certain QoS and security attributes.

Cloud Computing Environment

- The competences of the **provider** are:
  - the uninterrupted provision of the end-service
  - the maintenance as well as the update of the CC resources which support the end-service
  - the security both of the physical assets and of the virtualized resources
- Moreover, the CC provider is responsible about the management as well as the privacy of Personally Identifiable Information (PII) that collects.
- The CC provider balances the consumer demands and the feasible provisions concerning the end-service at any time through the Service Level Agreement (SLA).

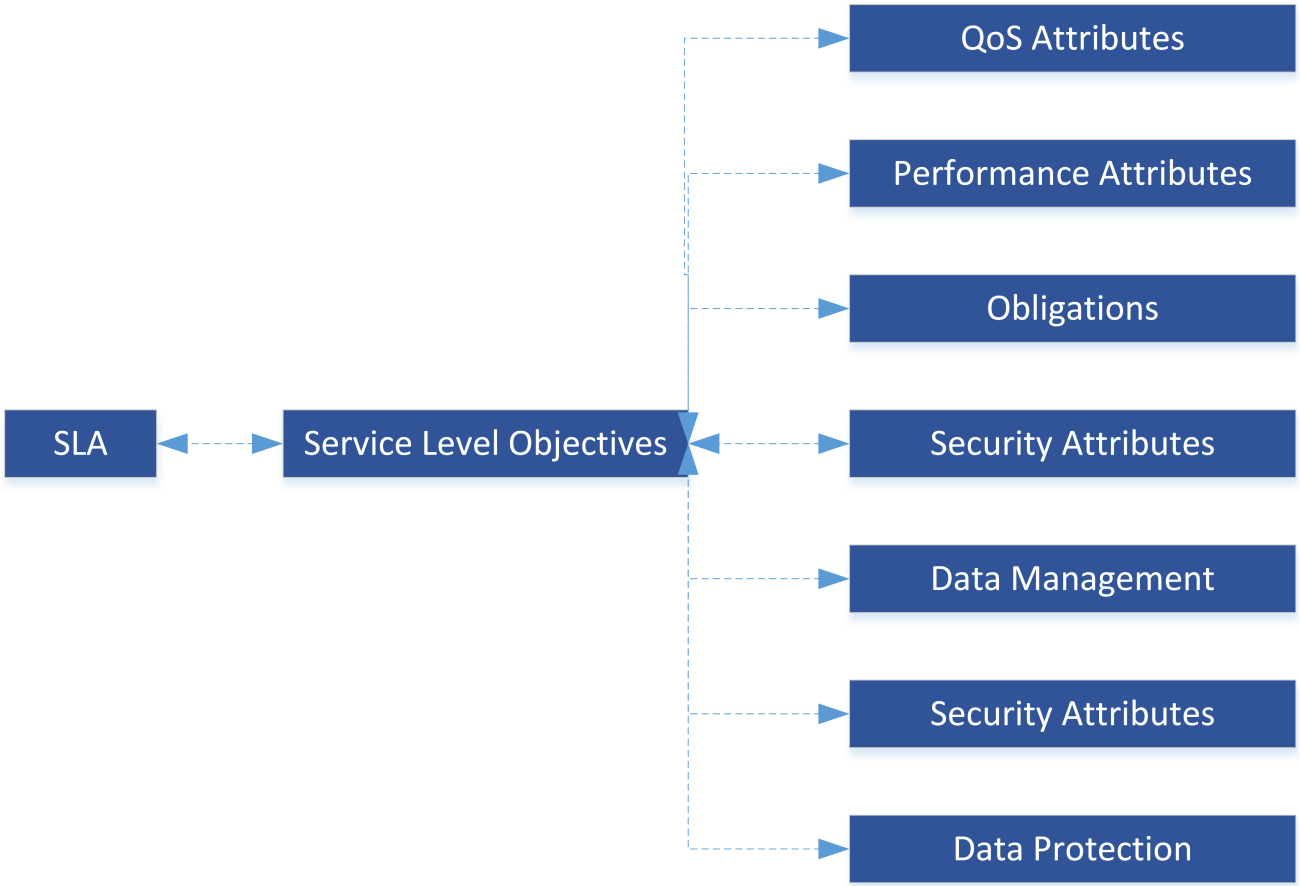
Cloud Computing Environment

Economic considerations about CC environments:

- Cloud environments facilitate:
  - elastic consumption
  - self-service
  - pay-as-you-go
- No need for an up-front acquisition cost in order to deploy an end-service; the cost is analog to the usage of CC resources
- Avoidance of phenomena such as building enough capacity for peak demand and then not using the capacity in non-peak periods.
- Multi-tenancy in CC environments reducing costs through sharing of applications.

Cloud Computing Environment

Between the provider and the clients, takes place a negotiation process which defines metrics that should be fulfilled by the end-service. The official form of this process is the Service Level Agreement (SLA).



1

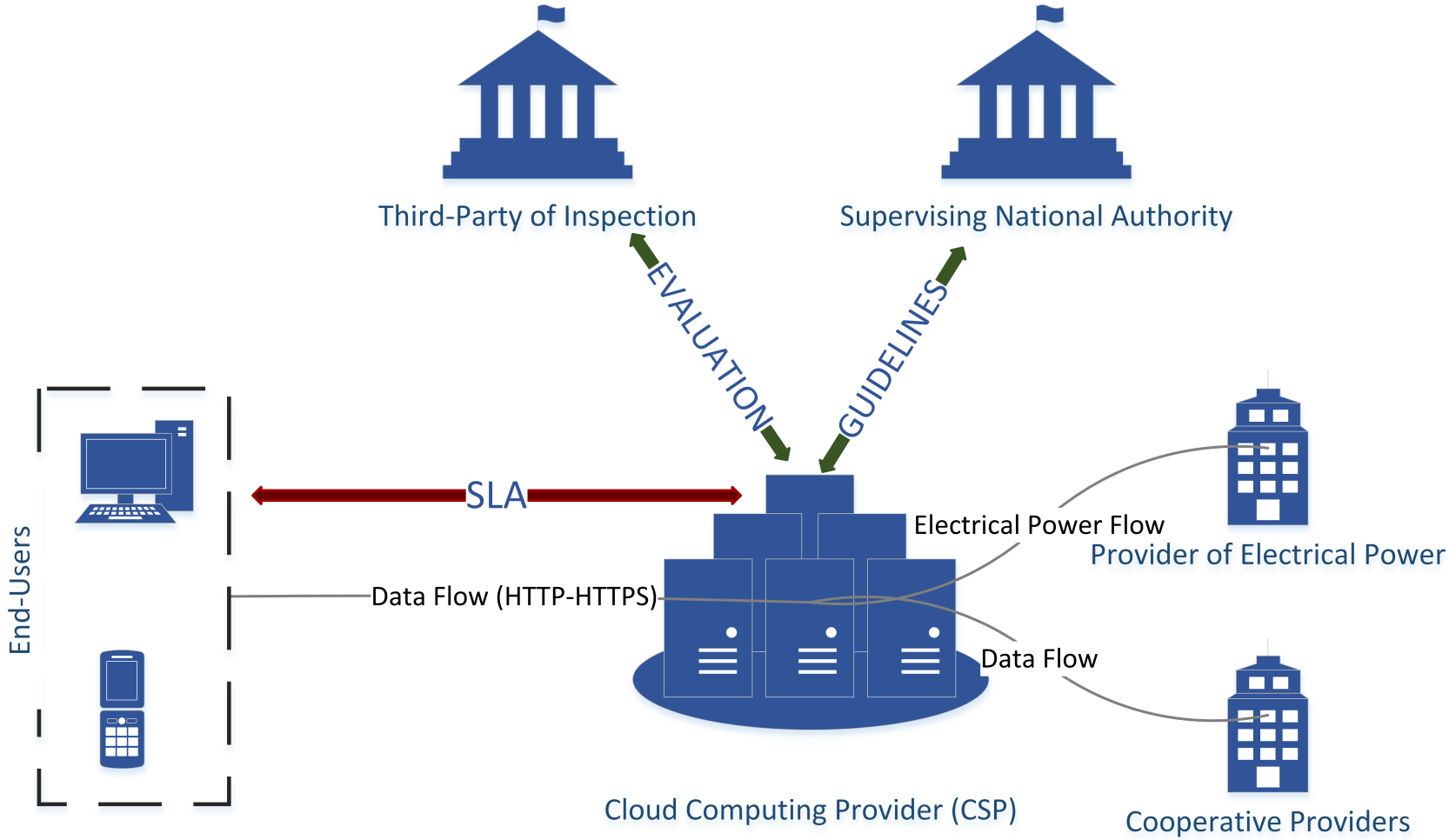
SLA Definition Procedure

Cloud Computing Environment

Service Level Agreement:

- The SLA consists of four phases:
  - the negotiation
  - the establishment
  - the deployment
  - the compliance
- The SLA is the foundation for the expected level of service between the clients and the provider.
- The CC environments deliver end-services which support scaling behavior concerning the CC resources.
  - So through the SLA the clients use an environment which supports Service-Oriented Architecture (SOA).
- The SOA enables new capabilities for the clients which leads to a bidirectional relation between provider-clients.

SLA incorporation in a cloud scenario:



Abstract presentation of the SLA-involved parties

SLA Assessment:

- The SLA compliance takes place by assessing the fulfilment of its objectives in regulatory and technical level.
- The SLA assessment should follow a dynamic schedule in order to evaluate:
  - the performance under the fast changing conditions
  - the response of the end-service in high load fluctuations
- The SLA should follow the legal framework which supervises the relation between provider-clients.
- The Third-Party of Inspection should perform the assessment independently, with obligation to the clients' interest.
- The Third-Party of Inspection should also evaluate the connection between the Service Level Objectives (SLOs) metrics and the CC environment.

SLA Violations:

- There are not standardized SLAs; so as the SLA is defined by the CC providers, the compensation clauses merely damage them.
- The third-Party of Inspection forces the CC provider to mitigate the violation.
- The fines in case of violation are defined in the SLA for transparency.
- In some cases the clients are responsible for monitoring SLA violations.
- SLA violations/fines depend on the model of services due to the type of data that are managed in each.
- The violations are not published publicly due to the damage that may cause to the reputation of the CC provider.

CC Case Study

Major parts of our work:

1. Address the security challenges of cloud environment taking into consideration the European legislation concerning the transaction of data with country outside EU.(e.g. 95/46/EC, contractual clauses C(2004)5271)
2. Create a custom SLA for a cross-border CC scenario.
3. Construct a custom CC environment based on the SLA which characterized by high level of security.
4. Perform risk assessment and analysis in order to manage it effectively.
5. Evaluate the CC environment both the regulatory and the technical level by using a SLA-based assessment methodology.
6. Construct a security architecture and match it to the network topology of this environment in order to mitigate the threats.
7. Design for this environment a regulatory framework aiming to fraud disclosure.

CC Case Study: Analysis

Points of interest about the scenarios in this CC case study:

- **In the first scenario**:
  - The data controller is a EU governmental authority (i.e. in Greece.). The data processor is the CSP.
  - The CSP is housed in a Member State of the European Union (i.e. Spain).
- **In the second scenario**:
  - The data controller is a EU governmental authority (i.e. in Greece.). The data processor is the CSP.
  - The CSP is housed in a third country (i.e. Turkey) outside the European Union (EU) and the European Economic Area (EEA).
- The type of data that are transferred during the usage of the CC end-service are **sensitive**. (e.g. personnal, governmental)
- The data belong to natural people who can be identified and their current habitat is inside EU.
- The natural people have only permission of usage of the end-service

CC Case Study: Legislation

Examined European legislation:

- According to Article 5 of the Greek national law 2472/1997, which harmonizes the Directive 95/46/EK in the national legislation, the processing of personal data is feasible when the data subjects give their consent and must be informed about any action carried out in their data.
  - This task is achieved through the SLA between the data controller, governmental authority and the clients.
- According to Article 4 of the Directive 95/46/EC, the data controller must take the necessary measures to ensure that each of its establishments complies with the obligations laid down by this Directive.
- According to Article 2 of the Directive 95/46/EC, the data controller must provide information about the identity of the **data processor** and the **purposes of the processing** for which the data are intended.
- The data controller should adopt a code of conduct intended to contribute to the proper implementation of the provisions defined in the

CC Case Study: Legislation

Examined European legislation:

- According to Article 25 of the Directive 95/46/EC, the third country (e.g. Turkey, Egypt) that was selected for the scenario did not provide adequate level of security concerning the processing of personal data.
- In order to accomplish the transaction of data, the legal framework that supervises the collaboration, between the CSP and the clients, has to be the articles of the Directive 95/46/EC.
- The transaction of data was feasible by following the Article 26 of the directive 95/46/EC and by defining the appropriate contractual clauses of the Commission decision C(2004)5271.
- The Hellenic Data Protection Authority (HDPA) then should approve the contractual clauses in order to accomplish legality of the data transaction.
- In the case of governmental data transaction, there is not competent authority to authorize this action as a result the HDPA approves it.

CC Case Study: Legislation

Examined European legislation:

- According to Article 13 of the directive 2000/31/EC, *"Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information."*
- According to Article 14 of the directive 2000/31/EC, *"Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service."*
- According to Article 15 of the directive 2000/31/EC:
  - *"Member States shall not impose a general obligation on providers to monitor the information which they transmit or store"*
  - *"nor a general obligation actively to seek facts or circumstances indicating illegal activity."*
- Because of these articles appear security challenges which should be addressed through the SLA and any commercial contract in general.

CC Case Study: Legislation

Examined Contractual Clauses:

- The contractual clauses adopted in this scenario, does not incorporate commercial business terms which are established by the main services contract.
- The personal data have been collected processed and transferred in accordance with the laws applicable to the data controller (e.g. Directive 95/46/EC).
- The data controller should be able to identify that the data processor, CSP, is able to satisfy its legal obligations.
- The data processor will have in place appropriate **technical** and **organisational** measures to protect the personal data against any event threatening the transferred data.
- The data processor should inform the data controller about the existence of any local laws that would have a substantial adverse effect on personal data under these clauses.

CC Case Study: Legislation

Examined Binding Corporate Rules (BCRs):

- Binding Corporate Rules consist a legal tool which enables the transaction of data in the corporate environment of a company or organization under specific provisions aiming to achieve a high level of security.
- BCRs:
  - **regulate** the cross-border transfer of data and
  - **apply** across the multi-domain environment of the CSP regardless the number of facilities and their position in high-risk countries.
- In the scenario of cross-border transfer of data, (EU-Third Country), the CSP should incorporate in the governance of its environment certain BCRs defined by the data controller.
- The BCRs will ensure that the Directive 95/46/EK and its provisions are adopted by the CSP's environment as long as the main services contract is in force.

CC Case Study: Legislation

Examined Legislation concerning Fraudulent Activities:

- Member States cover fraud cases by the criminal laws under the power of the competent authority and police body.
- In the scenario between Member States of the European Union, it is necessary that they have adopted in their national law specific Directives and their provisions prior to the transaction of data.These Directives are namely:
  - **Directive 2009/136/EC** amending **Directive 2002/22/EC** on universal service and users rights relating to electronic communications networks and services
  - **Directive 97/7/EC** on the protection of consumers in respect of distance contracts
  - **Directive 2005/29/EC** on Unfair Commercial Practices.
  - **Directive 93/13/EEC** on unfair terms in consumer contracts.

CC Case Study: Legislation

Examined Legislation concerning Fraudulent Activities:

- The **Regulation No 2006/2004** should be taken into consideration for the cooperation between the national authorities of the Member States concerning the consumer protection.
- In the cross-border scenario with third country outside EU, the Member State of the data controller must have already adopted the **Directive 2009/136/EC** amending the Directive 2002/58/EC.
- Due to the fact that the contractual clauses are governed by the law of the country in which the data controller is established.
- **NIS directive** and the revised **Payment Services Directive** reinforce the worldwide cross-border dimension of fraud crimes and in the same time lead to changes in criminal methods of frauds.

CC Case Study: Legislation

Examined Legislation concerning Fraudulent Activities:

- The data controller is responsible about fraudulent activities affecting the management and processing of personal data.
- The data controller should ensure that:
  - the data processor adapts technical and organizational measures so as to avoid negative effects in personal data,
  - the operation of the CC environment complies with the Directive 2009/136/
- The Member State should ensure that the relevant authority is able to block the access to service where this is justified by reasons of fraud.
  1. In case that the data processor, CSP, detects fraudulent activity has to block it in the technical, as well as, in the organizational layer as agreed by the the contractual clauses and the BCRs.
  2. In case the national authority of the Member State where it is established the data controller, detects fraudulent activity by the CSP's end-service, has the authority to block it.

CC Case Study: Fraud Disclosure

Theoretical Background concerning Fraud:

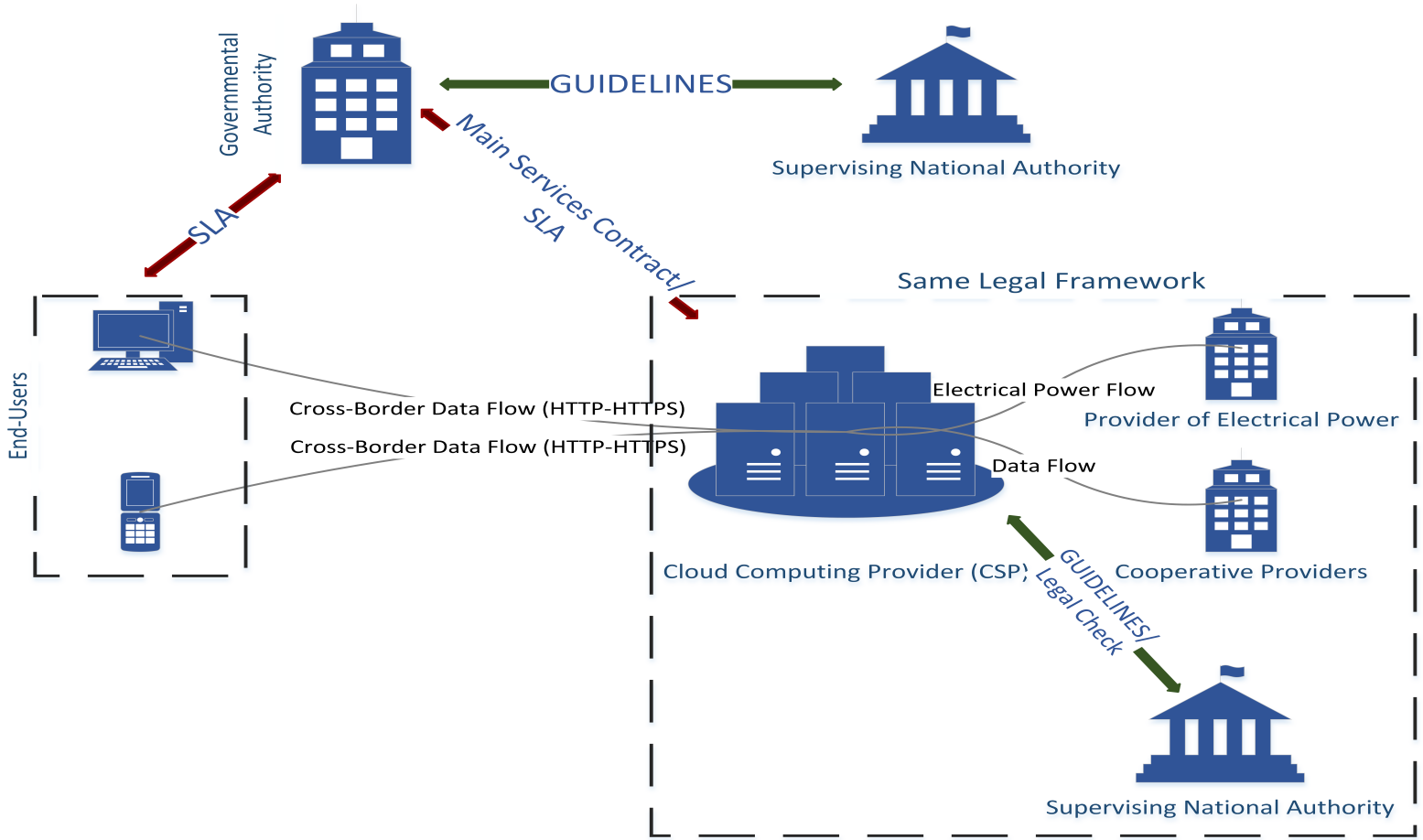
- Fraudulent activities are illegal actions according the legislation or prohibited by the SLA.
- Illegal actions depend on the regulation or directive which governs the management and processing of certain type of data. (e.g. personal data)
- Prohibited actions depend on the agreed SLA and the deviation of natural people by the authorized actions.
- In the event of a fraudulent activity, the perpetrator :
  - is prosecuted according the regulation in force or
  - pays a compensation according the SLA violations occurred.
- Fraud risk is of great significance to a CSP as it affects its financial status, reputation as well as regulations and regulatory compliance controls.

CC Case Study: Fraud Disclosure

Fraudulent Activities threatening the CC environment:

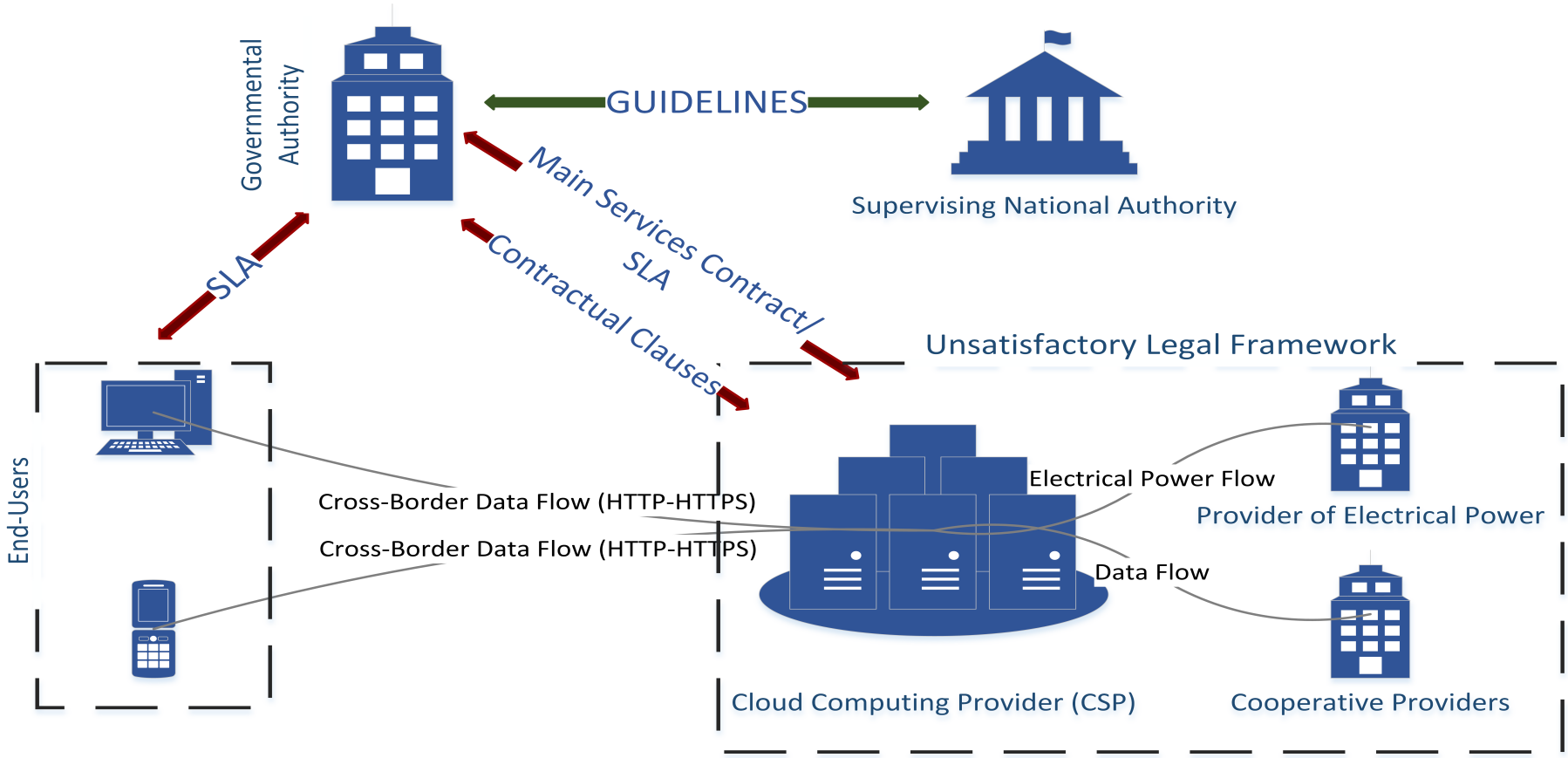
- CSPs that do not commit resources to fraud detection and prevention could ruin their reputation and expose collected data by the end-service.
- It should be noted that the CC environment is susceptible to fraudulent activities due to the level of security.
- In order to mitigate the threats by fraudulent activities in the scenarios of this case study:
  1. the level of security of the CC environment should be adequate so as to mitigate threats by numerous attacks in technical and organizational layer,
  2. assess the level of security by evaluating the results and improve the security mechanisms,
  3. in the secure environment match a regulatory framework aiming to fraud disclosure.

Practical Approach with Spain:



Abstract presentation of the European Scenario

Practical Approach with Turkey:



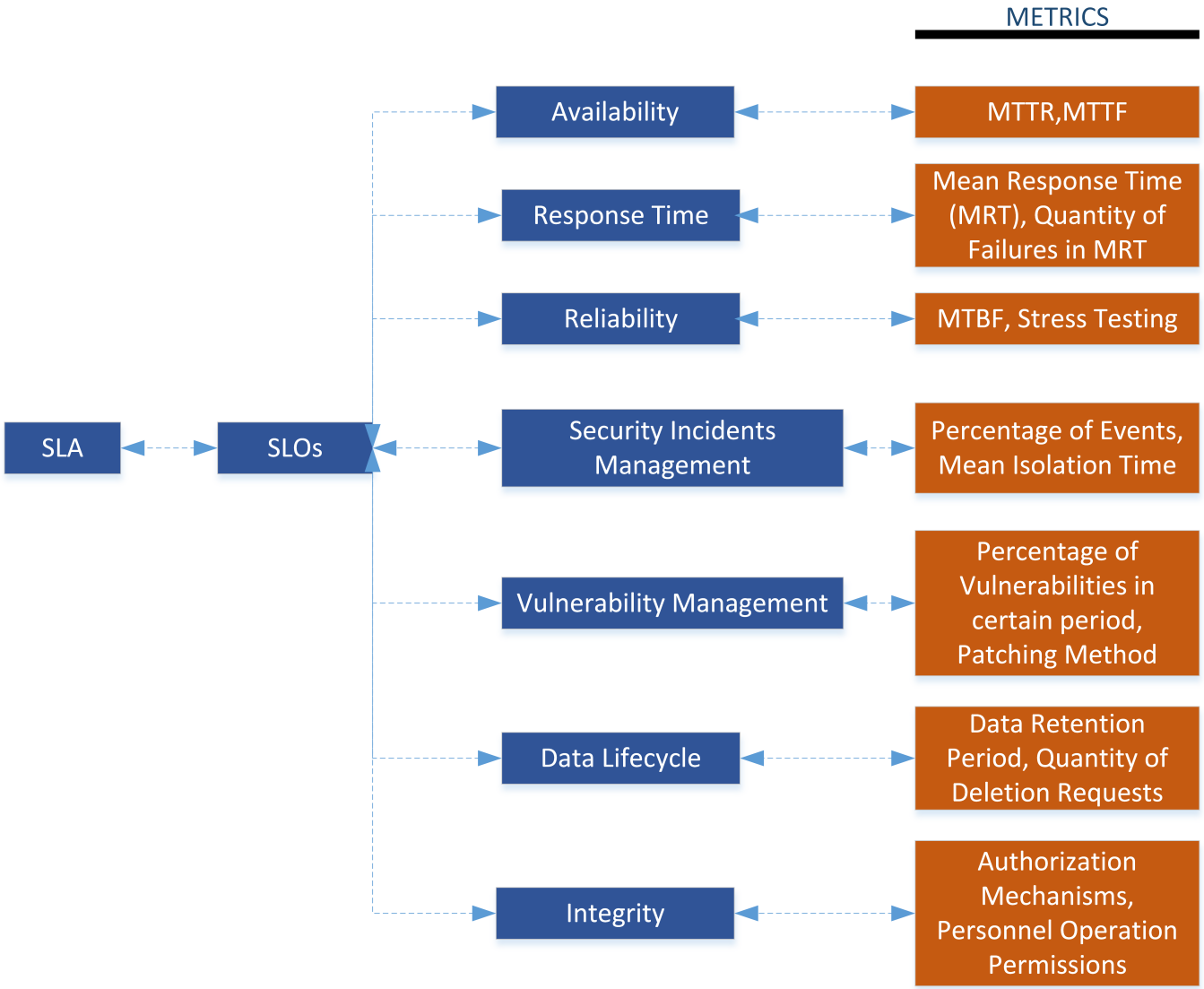
Abstract presentation of the Cross-Border Scenario

CC Case Study: SLA

Custom SLA:

- The SLA defines objectives which should be fulfilled in order to cover legislation gaps and misinterpretations.
  - Continuous monitoring of the intranets.
  - Evaluation of personnel actions concerning PII data.
  - Monitoring of data indicating **illegal and fraudulent** activities.
- The SLA consists of four SLO categories namely, Data Management, Functionality, Data Protection and Service Security.
- The SLA defines security SLOs which indicate technical specifications for the provider's environment.
  - IDS
  - monitoring systems for intranets
  - firewalls
- For each SLO, appropriate metrics would be defined in order to measure the effectiveness and control the performance of the environment.

SLA metrics:



SLOs-Metrics association

CC Case Study: SLA

SLA main objective:

- The main objective of SLA is to protect the personal data as well as the CC infrastructure against a wide spectrum of attacks.
- Attacks which are addressed through this SLA are namely:
  - Data Theft
  - Denial of Service Attacks
  - Economic Denial of Service
  - Hypervisor Attack
  - Insider Threats
  - Power Attack
  - Malicious Injection Attacks
- Vulnerabilities that exist due to the web architecture, (e.g. TCP fragmentation attacks), continue to threat the CC environment.
- The majority of the attacks which target the CC environment could be associated with fraudulent activities and be **enhanced** by them.

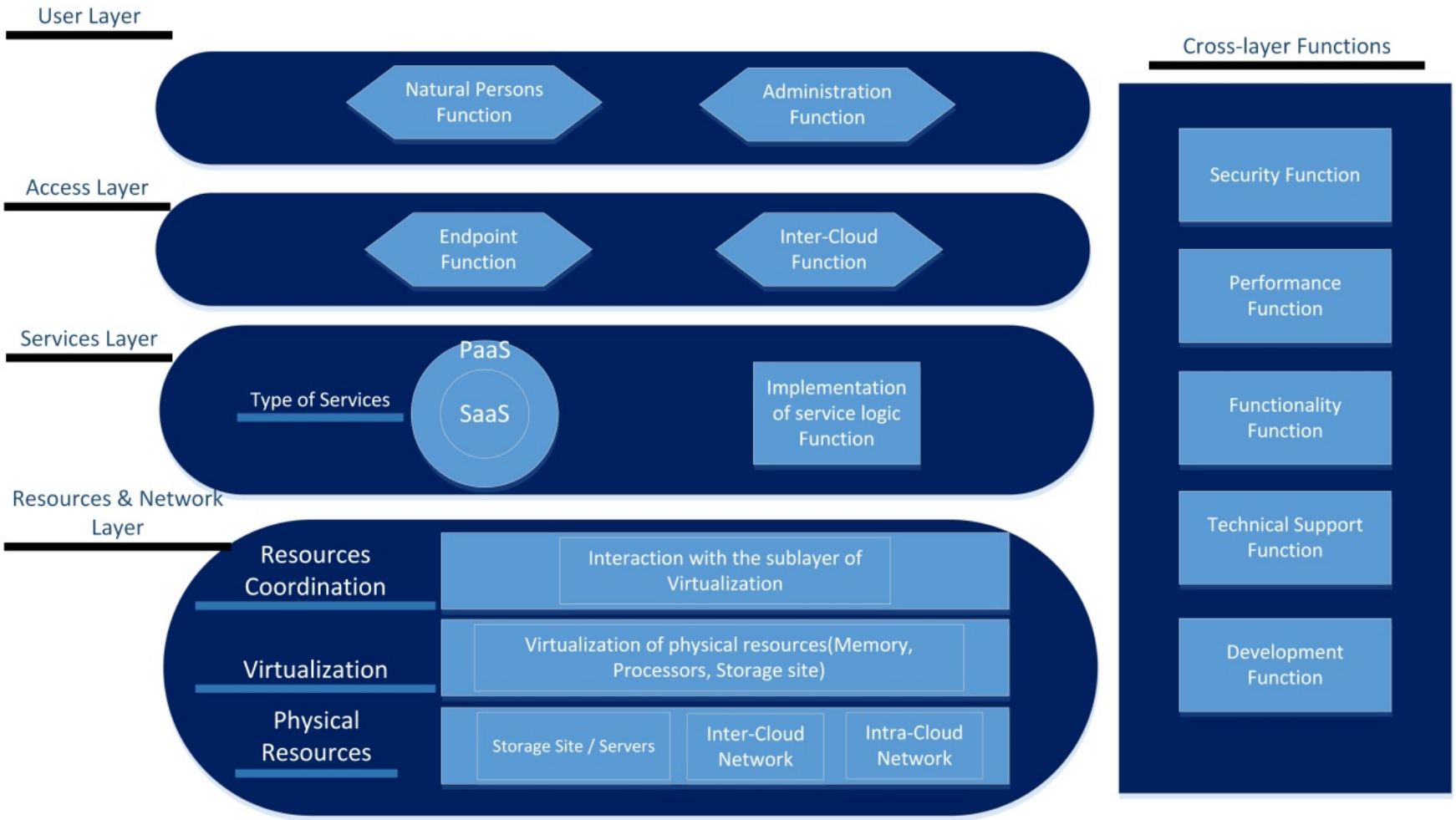
CC Case Study: Policies

Policies Design Strategy:

- This strategy aims to indicate objectives which should be accomplished and methods which should be followed by the policies in general.
- By following this strategy, there will be homogeneity in the performance of the provider's infrastructure.
- Main CC policies are namely:
  - Policy for the purpose of data collection
  - Credential creation policy
  - Data separation policy
  - Policy of accepted actions by personnel
  - Ethical policy
  - Failure restoration policy
  - Transparency policy
  - Fraud-related interviewing of personnel

CC Case Study: Functional Architecture

The organization of the CC provider's infrastructure is based on the functional architecture of ITU which consists of layers and functional blocks.



ITU Functional Architecture

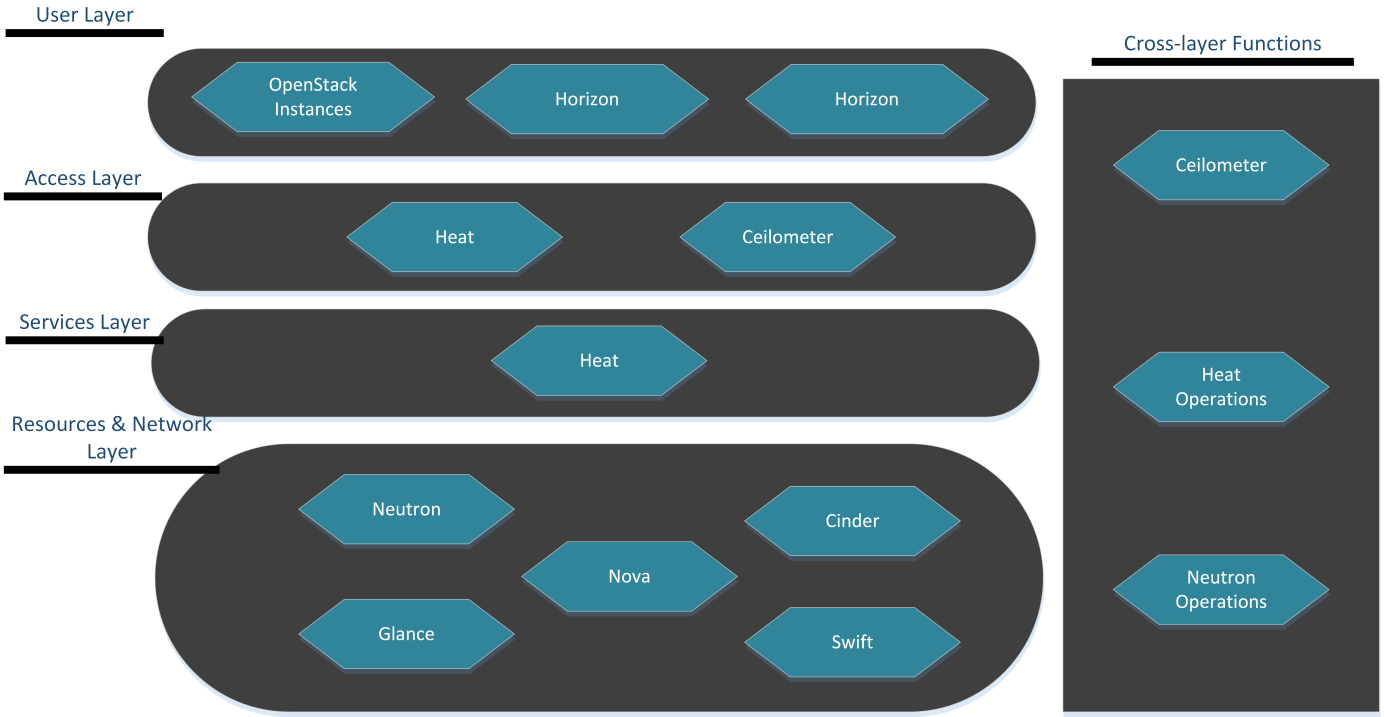
CC Case Study: Functional Architecture

Cloud Service Provider's Environment:

- The provider's environment delivers the end-service through the functional layers namely:
  - **User layer**, provides interaction with the end-users.
  - **Access layer**, controls the consumption of the end-service and by using the inter-cloud function the provider can allocate resources by another CC environment.
  - **Services layer**, provides the end-service fro each request that accepts.
  - **Resources and network layer**, manages and modifies the CC resources according to the needs of the end-service.
  - **Cross-layer functions**, in this layer exist functions that accomplish security of the end-service and specification fulfilment.
- The provider's environment is a custom **OpenStack** environment constructed by following the objectives which were set in the SLA.

CC Case Study: Functional Architecture

- The OpenStack environment consists of projects which should be matched to the functional architecture of the CC provider's infrastructure.

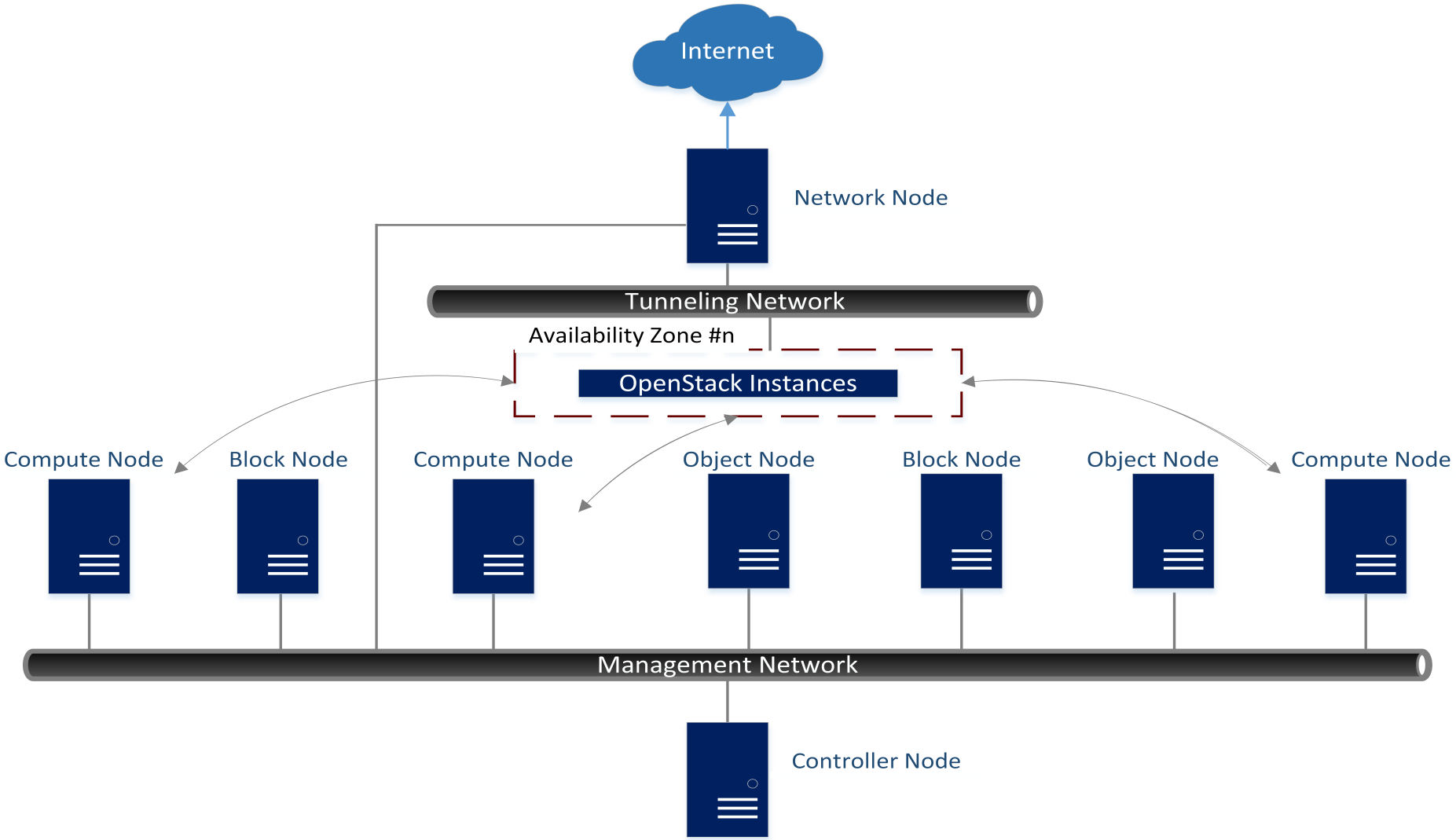


OpenStack-ITU Matching

- The provision of the end-service takes place according the functional architecture of the ITU after the matching between Openstack projects-ITU functional blocks.

CC Case Study: Environment

Custom OpenStack Environment:



CSP's Environment

CC Case Study: Environment

Characteristics of this environment:

- The end-service is a SaaS which is provided through the integration of it with the CC resources by the native CC mechanisms. (e.g. Heat project)
- The dynamic allocation of CC resources during the provision of the end-service takes place according a custom **OpenStack Flavor**.
- The deployment of the end-service takes place due to the Heat project and a custom **Heat template**.
- The Heat template:
  - orchestrates the CC resources which are necessary for the end-service.
  - sets alarms in the telemetry service in order to scale up/down according to the network traffic load.
  - defines scaling policies which interact with the telemetry alarms.

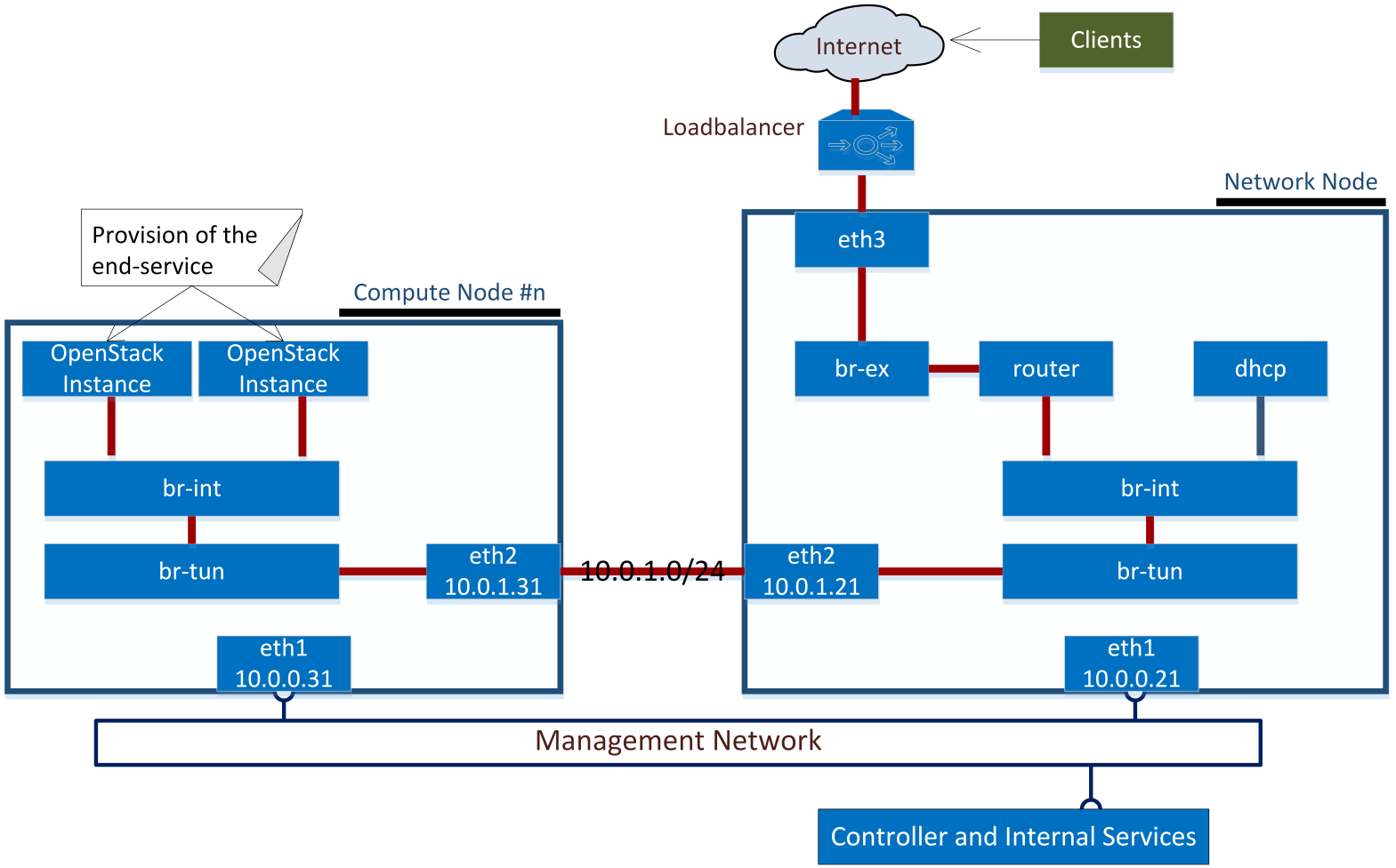
CC Case Study: Environment

```
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-up when the average CPU > 80% for 1 minute.
    meter_name: cpu_util
    statistic: avg
    period: 60
    evaluation_periods: 1
    threshold: 80
    alarm_actions:
      - {get_attr: [scale_up_policy, alarm_url]}
    comparison_operator: gt
cpu_alarm_low:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-down when the average CPU < 10% for 15 minute.
    meter_name: cpu_util
    statistic: avg
    period: 900
    evaluation_periods: 1
    threshold: 10
    alarm_actions:
      - {get_attr: [scale_down_policy, alarm_url]}
    comparison_operator: lt
network_alarm_high:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-up when the network incoming traffic is more than 10000 for 1 minute
    meter_name: network.incoming.packets
    statistic: sum
    period: 60
    evaluation_periods: 1
    threshold: 10000
    alarm_actions:
      - {get_attr: [scale_up2_policy, alarm_url]}
    comparison_operator: gt
network_alarm_low:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-down when the network incoming traffic is less than 8000 for 10 minute
    meter_name: network.incoming.packets
    statistic: sum
    period: 600
    evaluation_periods: 1
    threshold: 0
```

Heat template snapshot

CC Case Study: Environment

The CC environments are vulnerable to a large majority of attacks, greater than other environments (e.g. clusters, grid computing) due to the abstraction layer which is accessed by the clients.



End-service networking

CC Case Study: Risk

Theoretical background of CC Risk:

- According to Federal Information Processing Standards (FIPS)-Publication 199, risk is the combination of threats and vulnerabilities that exist in the corporate environment.
- Risk assessment is an activity involving management and operational personnel within the organization.
- In order to accomplish effective risk management the CIA model is orchestrated and aims to achieve high Confidentiality, Integrity and Availability in technical and organizational layer.
- Moreover, in order to identify and address the risk thoroughly, a classification of risk in certain categories takes place. These categories are:
  - Organizational and Policy Risks
  - Legislation Risks
  - Technical Risks

CC Case Study: Risk

Organizational and Policy Risks:

- SaaS lock-in, is the potential dependency for service provision on a particular CSP and the inability to transfer data in case an emergent event.
- Compliance challenges lead to risk during the end-service provision as the clients can not acknowledge the compliance of the CSP according the agreed SLA. This risk exist in two cases:
  - When the CSP can not provide evidence of their own compliance to the agreed SLOs.
  - when the CP does not permit audit by the CC.
- Multi-tenancy and resource sharing of an instance of the end-service by numerous clients introduces risk for the provision of the end-service.
- Termination or failure of the provision of the end-service which diverge by the SLA, have a critical impact on the clients ability to meet their duties and obligations to their own clients.

CC Case Study: Risk

Legislation Risks:

- The distributed environment of a CSP permits multiple facilities located across many countries and in some occasions in high-risk countries.
  - In high risk countries the national regulations do not define data protection guidelines as well as the privacy of data and the civil rights of natural people are not applicable.
  - Moreover, the national authorities in high-risk countries do not act according a framework and their actions may endanger PII.
- In case the CSP's environment collects and processes PII, then should be acting according specified data protection directives and regulations depending on the country.
- The CSP should follow changes in the national legislation framework concerning the process of personal data.
  - For example, in two years the directive 95/46/EC will be replaced by the regulation 2016/679 concerning the protection of personal data and then the SLAs should incorporate new security aspects.

CC Case Study: Risk

Technical Risks:

- The CC environment is characterized by the scaling mechanisms which permit fast resource allocation according the demand. Due to these mechanisms the environment is susceptible to resource exhaustion.
  - These certain mechanisms ease the task of DoS and DDoS attacks during the period in which they take place in order to damage the provision of the end-service
- Data leakage due to the actions of malicious insiders consist a critical risk as PII and data concerning the operation of this environment become available to attackers.
- In distributed environments, data must be transferred in order to synchronise multiple distributed virtual machines in order to accomplish data management and end-service provision.
  - So, large quantities of data are in transit both on the intranets and on the outside perimeter of the CC environment, creating attack vectors.

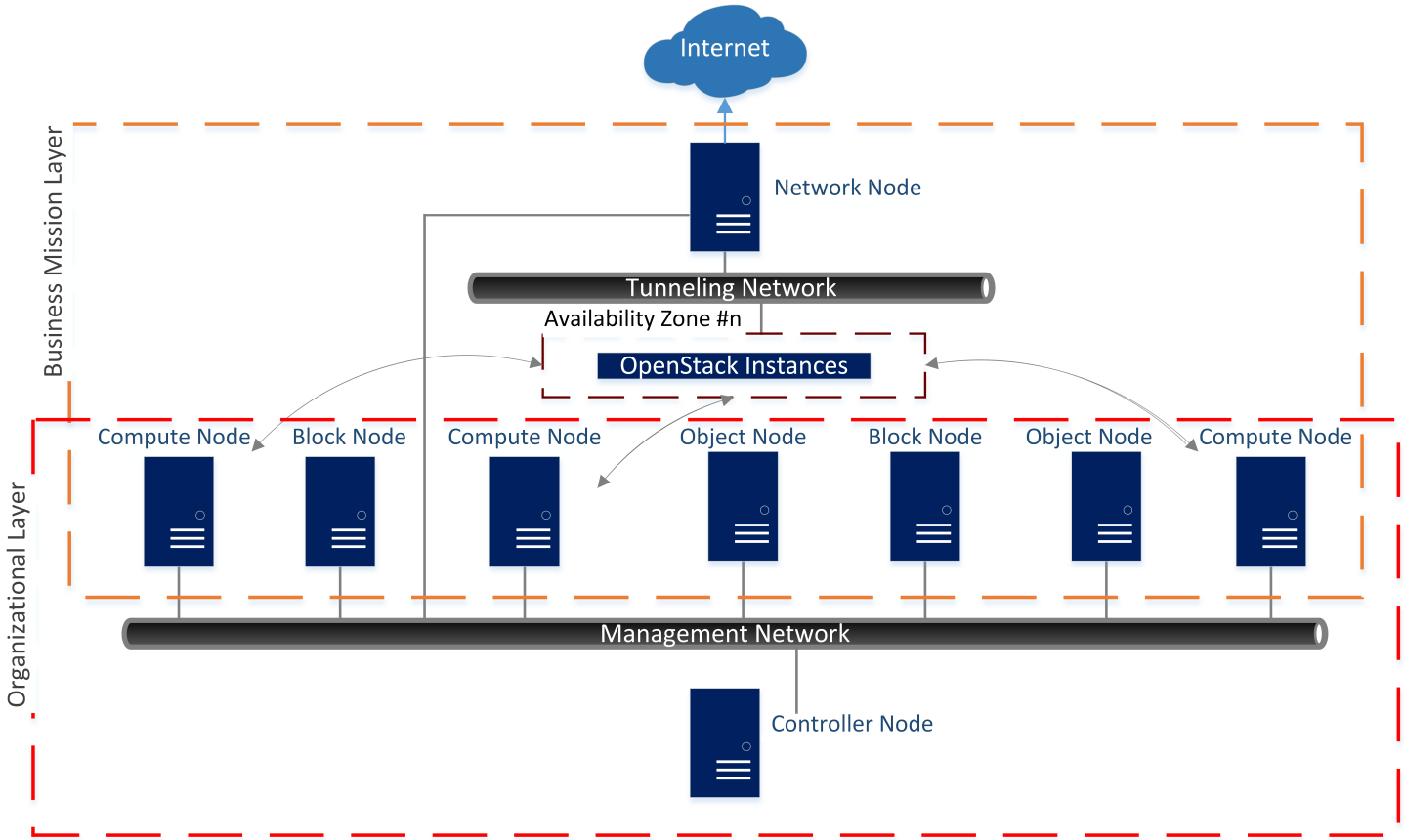
CC Case Study: Risk

Risk Management:

- In order to achieve management of the risks described, two distinct layers of risk defined and matched to the network topology of the CC environment:
  - **Organizational Layer**
  - **Business Mission Layer**
- Then, in those two layers performed classification of the data which are collected and managed. The classification categories are:
  - **Confidential**, PII and data concerning the natural people.
  - **Sensitive but unclassified**, data concerning the operation of the CC environment.
  - **Unclassified**, data concerning the provisioned SaaS.
- Moreover, every attack performed in each layer has a certain impact. Three categories of impact are defined:
  - Low
  - Moderate
  - High

CC Case Study: Risk

- The definition of risk layers permits association between the attacks and the impact of them against the CC environment by identifying the type of data which are affected. The organizational layer is the high risk layer as data by all every category are hosted there.



Risk layers

CC Case Study: Security Assessment

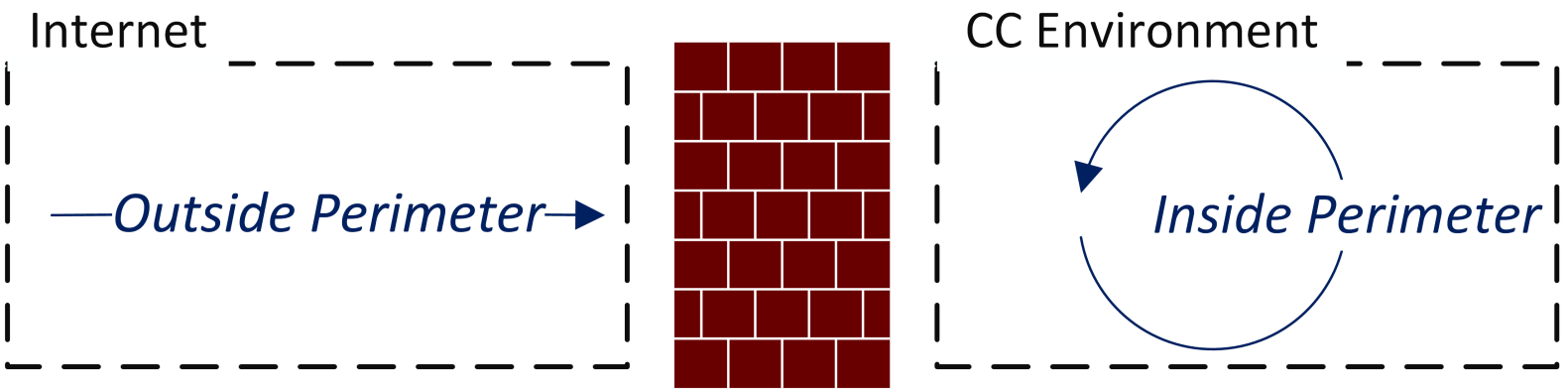
Security Assessment Methodology:

- The scope of the security assessment is to define the minimum information the attacker could gain so as to exploit the cloud boundary.
  - Moreover, security assessment identifies, Personally Identifiable Information (PII) and system information that can be leaked.
- The aggregation of the assessment results leads to the vulnerabilities definition that can be leveraged for exploitation.
- In the OpenStack environment, many computing entities with different characteristics interact and various technologies are combined (e.g. RPC-SDN), creating a diversity of vulnerabilities.
- A wide spectrum of tools and methods are orchestrated in order to identify the vulnerabilities and the attack vectors in the context of this security assessment. (e.g. Nmap, OpenVAS, Metasploit, Nessus)

CC Case Study: Security Assessment

The Cloud Boundary is divided into:

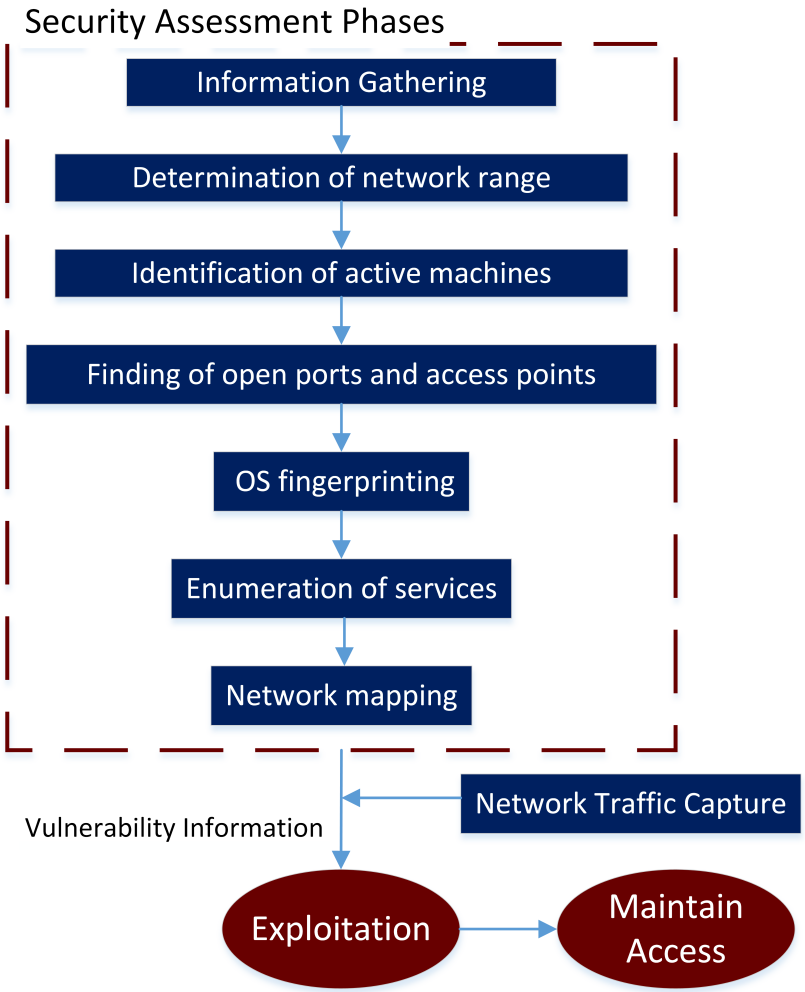
- The **Outside Perimeter** extends among the computing entities that are visible to the end-users. The business mission risk layer belong to this perimeter.
  - There exist limited PIIs and information about specified CC systems.
- The **Inside Perimeter** extends among the intranets of the environment. The organizational risk layer belongs to this perimeter.
  - There exist PIIs and critical operational data.



Inside and Outside Perimeters

CC Case Study: Security Assessment

- The security assessment phases are necessary to identify the environment's vulnerabilities in the technical layer.



Security Assessment Phases

CC Case Study: Security Assessment

The Inside Perimeter:

- The captured network traffic reveals that the attacker acquires access to critical data about the CC environment and the PII.
- The Controller Node has a critical vulnerability that allows NTP reflection and a DoS attack to a spoofed IP address inside the CC environment.
- The CC administration dashboard is vulnerable to a vector of attacks that allows password attacks.
  - The dashboard is only visible inside the CC environment and it is used for the configuration of the end-service delivery.
- The importance of the **insider threat** is identified due to the combination of the particularities of this type of environment and the impact of the attacks.

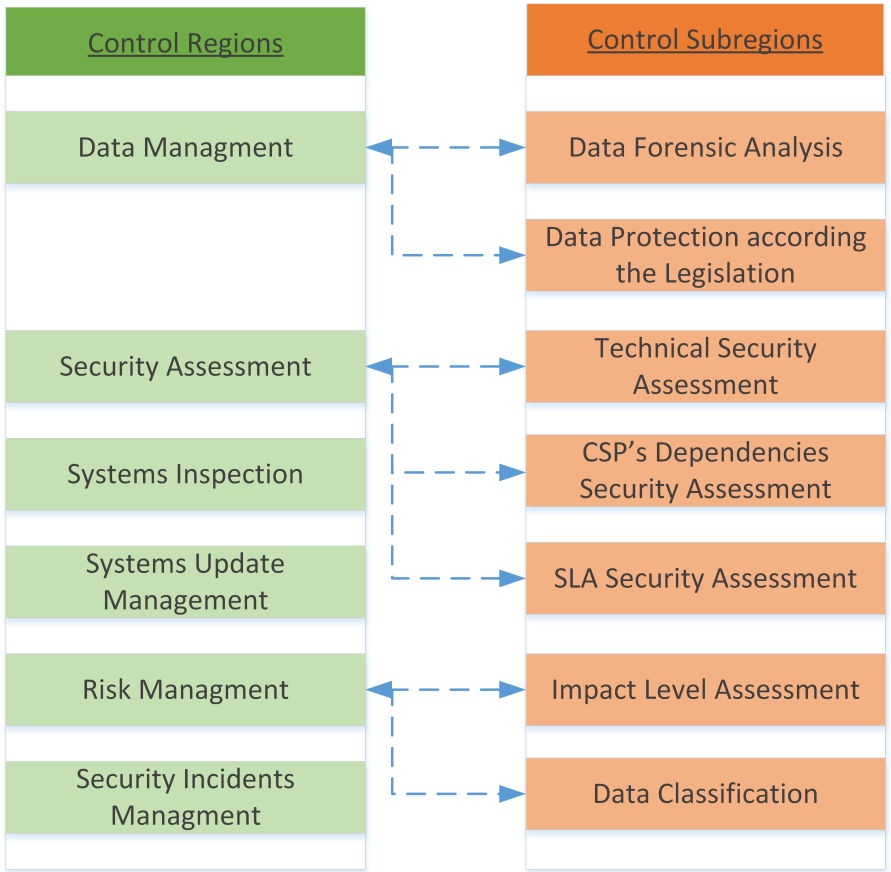
CC Case Study: Security Assessment

The Outside Perimeter:

- A DoS attack performed on the loadbalancer IP address of an Availability Zone may lead to resource exhaustion and damage the end-service availability.
  - The attack is performed by 100 virtual users and each of them perform 300 HTTP GET requests in a period of 1 minute.
  - This attack damages the provision of the end-service due to the fact that affects the response time of the end-service for the clients.
- In the outside perimeter attacks performed in the data in transit by following the man-in-the-middle attack and sslstrip method, the leakage of PII is achieved.
  - By this type of attack, it is identified that the CC environment is susceptible to vulnerabilities of the network protocols.

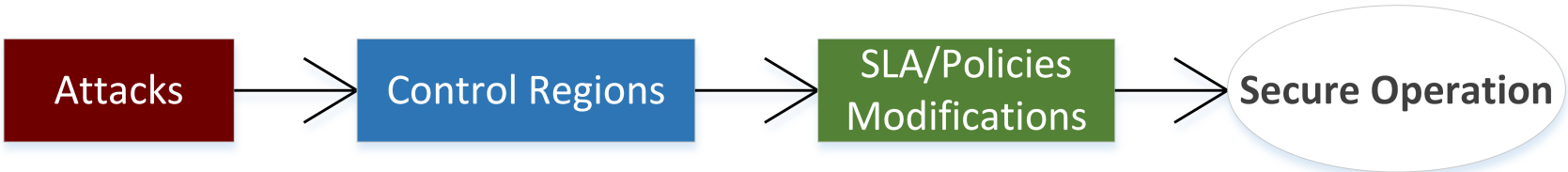
CC Case Study: Control Regions

- Control regions and subregions are the association link between the attacks which are performed and the functional layer of the CSP's environment. There areas identify the attributes of the SLA which are affected by the attacks.



CC Case Study: Control Regions

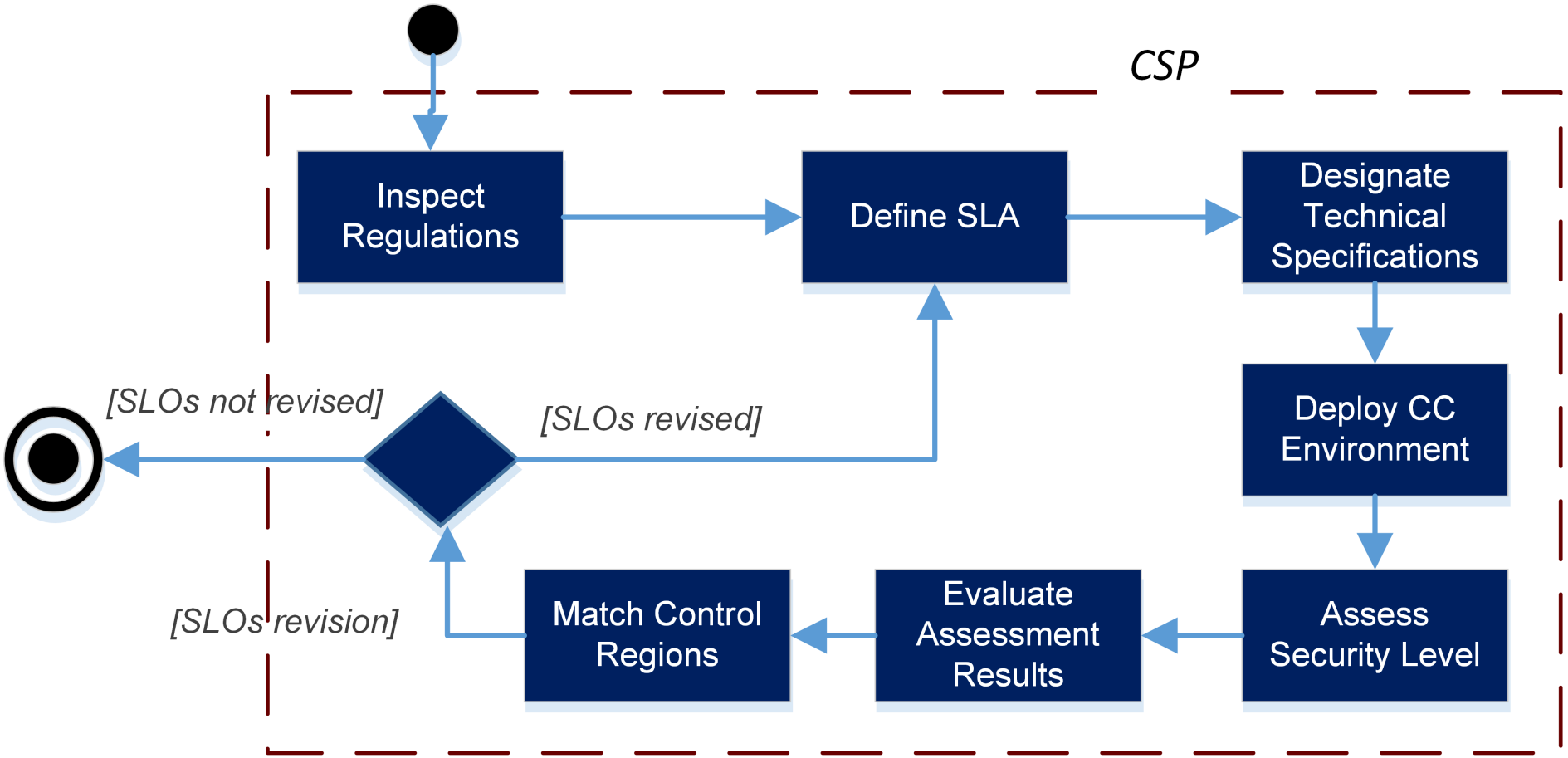
- Control regions and subregions facilitate detailed analysis for every identified attack and integrate the impact of every attack in the functional layer of the CSP's environment.
- The exploitation of a vulnerability is matched to a certain area of the CC environment. Then the operations of the SLO, *vulnerability management*, repair it.
- In case of a successful attack, the classification of the affected are is feasible and then the CSP can identify critical areas of its environment in order to reinforce them.



Control regions integration process

CC Case Study: Assessment Methodology

SLA-based assessment methodology:



- The SLA-based assessment methodology identifies also vulnerabilities in the functional layer.

CC Case Study: Security Architecture

The proposed CC Security Architecture is defined by a set of distinct functional layers namely:

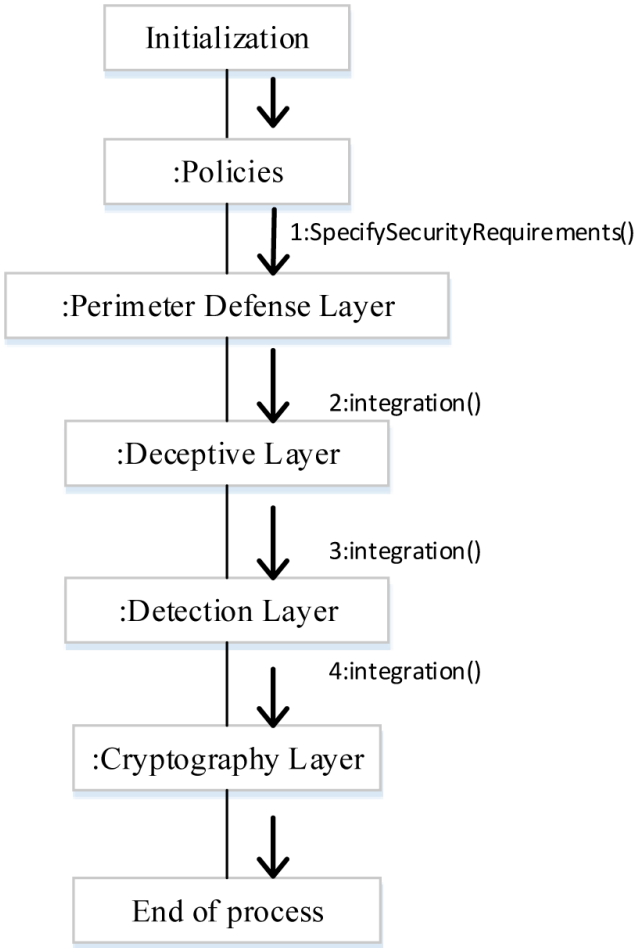
- the perimeter defence
- the deceptive
- the detection
- the cryptography

Prior to the adaptation of the security mechanisms of each layer, a sequence of policies should be defined. The policies will maintain the balance between:

- productivity
- functionality
- security

CC Case Study: Security Architecture

The following collaboration diagram presents the priority among the layers of the architecture concerning the incorporation of their security systems.



Collaboration Diagram

CC Case Study: Security Architecture

Perimeter Defence Layer

- This layer divides the CC environment into defence zones so as to protect the classified data with suitable security mechanisms.
- First Defence Zone
  - It extends between the border router and the first stateful inspection firewall.
  - The main security mechanism of the deceptive layer,honeynet, will be emplaced in this zone.
- Second Defence Zone
  - It extends among the first stateful inspection firewall, the security groups of instances and the second stateful inspection firewall.
  - Security groups act as virtual firewalls and control the bidirectional network traffic on the Autoscaling Groups.
- Third Defence Zone
  - It extends behind the second stateful inspection firewall and the security groups.

CC Case Study: Security Architecture

Deceptive Layer

- In this layer reside the deceptive systems which operate in every defence zone.
- A honeynet is emplaced in the first defence zone so as to lure the attackers and detain them enough to detect them.
- Honeynet consists of:
  - the honeywall
  - high interaction honeypots
- A number of high interaction honeypots are set up in key points of the second defence zone.
- A deceptive network of high interaction honeypots is created in the third defence zone, emulating the operations of the legitimate nodes.
- Under normal conditions, any ingress or egress traffic captured in honeypots should be considered malicious.

CC Case Study: Security Architecture

Detection Layer

- In this layer, the Intrusion Detection System (IDS) resides which analyses the network traffic with a predefined ruleset identifying attempts of attacks.
- The IDS adopted in the security architecture is the open source tool, SNORT.
- In the proposed security architecture, remote sensors are placed in every defence zone in specific points capturing the bidirectional network traffic so as to:
  - increase the accuracy of detection and
  - decrease the false positives.
- The management server which controls the logs and alerts, is placed in a secure location behind the second stateful inspection firewall.
- The efficiency of intrusion detection is highly connected with the predefined ruleset of the remote sensors.

CC Case Study: Security Architecture

Cryptography Layer

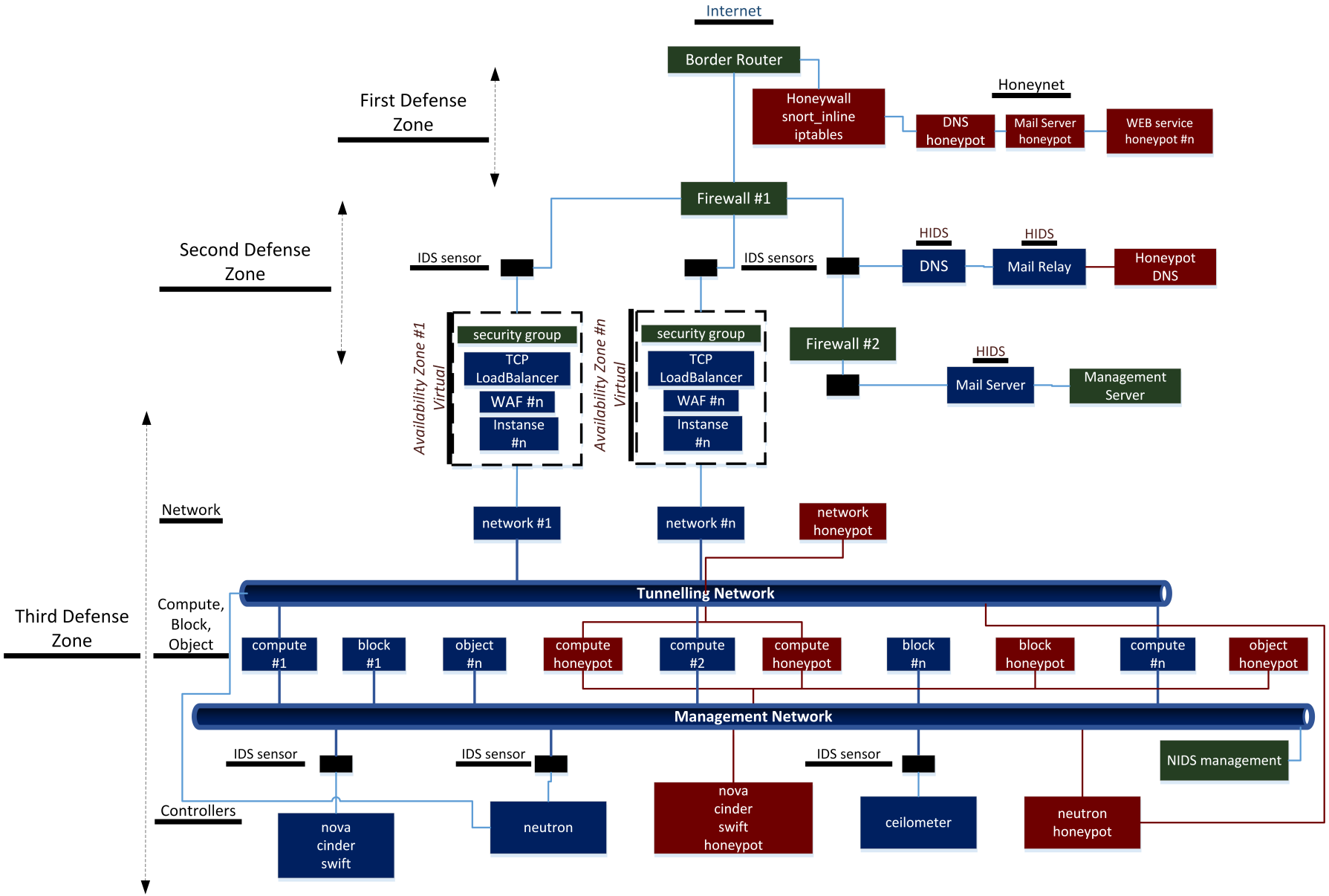
- Cryptographic methodologies are incorporated into the CC environment such as elliptic curve cryptography.
- The procedures and function of cryptography should not contradict with the operations of the other layers.
- In case the encrypted data harden the operation of IDS, then their emplacement should be avoided.
- The detection of an intrusion is more important than the concealment of data.
- The TLS protocol and its suite of cryptographic algorithms should be used to achieve end-to-end encryption between the clients and the web servers on the OpenStack instances.

CC Case Study: Security Architecture

Functional Layers	**Security Systems**
Perimeter Defense	OSSEC, ModSecurity, Openstack Security Groups
Deceptive	Second Generation Honeynet, Honeyd
Detection	Snort
Cryptography	Elliptic Curve Cryptography

Table: *Potential Security Systems in Each Layer*

CC Case Study: Security Architecture



Custom Security Architecture

CC Case Study: Security Architecture

Security Architecture Provisions:

- DoS, DDoS and flood attacks are strictly connected to embryonic connections and ip spoofing and can be treated by the systems of the perimeter defence layer.
- Web Application Firewalls (WAFs) provide HTTP protection against HTTP DoS attacks, cross-site scripting attacks and SQL-injection.
- WAFs offer Trojan protection, Webshell detection and Anti-Virus scanning of file attachments.
- IDS protects the CC environment against:
  - buffer overflow attacks
  - stealth port scans
  - OS fingerprinting
  - vulnerabilities scans
  - viruses and worms
- The honeynet has the ability to identify new vectors of attacks, malicious behaviour and 0-day exploits.

CC Case Study: Security Architecture

The following figure presents attacks that target CC environments and the security systems of the proposed security architecture which mitigate them.

Attacks	Security systems: Border Router	Firewall #n	Honeypots	IDS	Security Group	WAF
Intranets IP address spoofing	✔	✔			✔	
Tiny fragment attacks		✔				
Buffer Overflows			✔	✔		
Port scans	✔	✔	✔	✔	✔	
OS fingerprinting			✔	✔	✔	
Web attacks				✔		✔
Trojan attacks						✔
Viruses and Worms				✔		
Insider Threat			✔	✔		
Attacks on virtualization						✔
DoS and DDoS attacks		✔		✔		
HTTP DoS and DDoS				✔		✔
0-days exploits			✔			

Attacks and Security Systems

CC Case Study: Security Architecture

Security Architecture Evaluation:

- All attempts for DoS attacks created from systems of the third defence zone targeting systems on the second defence zone failed due to security groups protection.
- DoS attacks from the second defence zone targeting systems on the outside network failed due to the first firewall.
- The success of an external DoS attack is highly dependant by the capacity of the targeted Availability Zone.
- In case of interception of legitimate traffic on the third defence zone, no identification by the security systems can be achieved.
  - For that reason the administrator should assess the network behaviour of the CSP's employees.
  - The assessment should take into consideration each employee's authorization type and rights and compare them with the performed actions.

CC Case Study: Operational Specifications

- According to ENISA, organizations and companies should follow specific regulations and standards that govern the operation of a CC environment. These standards are about:
  - Data Protection
  - National Regulations
  - Payment Card Industry Data Security Standard (PCI-DSS)
  - Corporate Governance
  - Payment Application Data Security Standard (PA-DSS)
- The risk-based approach proposed in this case study:
  - **integrates** data protection guidelines in the functional layer of this environment
  - **incorporates** national regulations concerning the management of personal data
- By following this approach, the CSP creates harmony between legal and regulatory requirements as well as accomplish differentiation between the responsibilities and liabilities associated to the provision of the SaaS

CC Case Study: Operational Specifications

PCI-DSS Requirements:
The CSP maintains and verifies the PCI-DSS requirements of the environment. According the SLA, the CSP informs the clients about the results of the verification process.

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Encrypt transmission of cardholder data across open, public networks.
4. Protect stored cardholder data.
5. Restrict physical access to cardholder data.
6. Assign a unique ID to each person with computer access.
7. Track and monitor all access to network resources and cardholder data.
8. Regularly test security systems and processes.
9. Maintain a policy that addresses information security for all personnel.

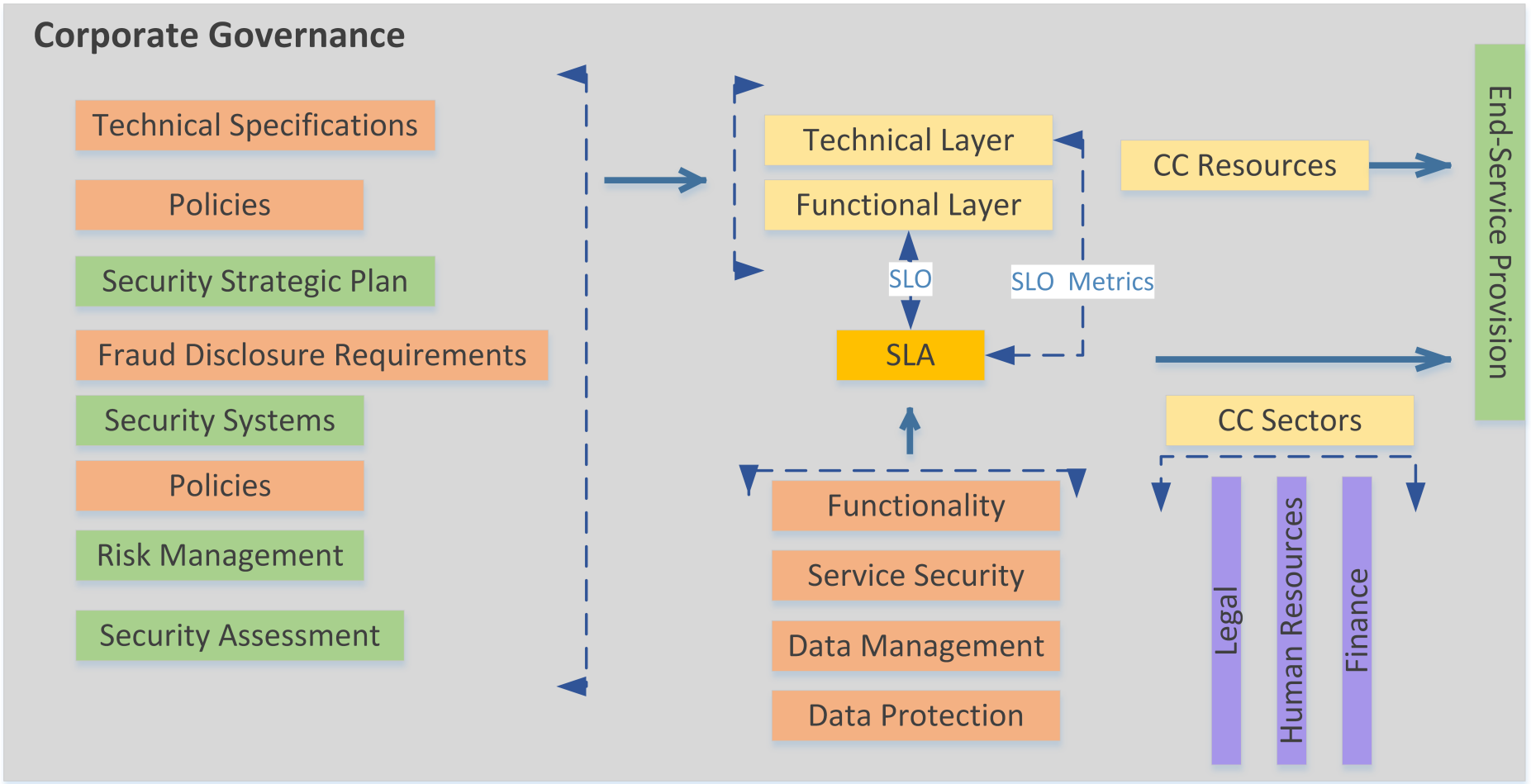
CC Case Study: Operational Specifications

PCI-DSS Compliance:

- Minimize reliance on third-party CSPs for protecting payment card data.
- Ensuring that clear-text account data is never accessible during the management of cardholder data in any operation which is performed at them.
- The client must have a detailed understanding of any security requirements associated to the PCI-DSS.
- the client also must maintain compliance for all of their own operations concerning the payment and their actions should be legal.
- The CSP should ensure that evidence is provided to verify that PCI-DSS controls are maintained continuously.
  - The **Attestation of Compliance** (AOC) proves that monitoring and validation controls are in place and work effectively.

CC Case Study: Operational Specifications

Corporate Governance:



Custom Governance Framework

CC Case Study: Fraud Regulatory Framework

Fraud Challenge in CC Environment:

- According to International Vice President of ISACA, Jeff Spivey:
  - *"All of the advantages of the cloud for enterprises are [also] the advantages for the bad guys."*
  - *"It is the anonymity and scale that is attractive to the fraudsters."*
- The clouds characteristics, such as rapid elasticity, on-demand provisioning, high availability, high scalability and pay-as-you-go model of pricing, are all as appealing to cybercriminals as to ordinary users.
- The **Operation High Roller** was a high risk fraud case accomplishing damage between 75 million and 2.5 billion dollars.
  - The entire fraud took place by the cloud computing environment.
  - This fraud case was combined with malware injection probes which were used for stealing the necessary information to perform the fraud.

CC Case Study: Fraud Regulatory Framework

Fraud in CC environment:

- The **fraudulent activities** in a CC environment are addressed by the information security sector.
- The fraud-related regulatory framework begins by a **strategic security plan** which will be embedded in the corporate governance of the CC environment.
- This specific strategic security plan consists of elements which enumerate actions in order to **initialize** the environment in an acceptable state.
- This state of the CC environment permits to the CSP to perform fraud risk management operations. Such operations namely are the following:
  - **Fraud Risk Assessment**
  - **Fraud Detection**
  - **Fraud Prevention**
- The task and objectives entrusted in those operations as well as the strategic security plan constitute the **proposed regulatory framework**.

CC Case Study: Fraud Regulatory Framework

The Regulatory Framework aims certain Fraud Forms:

- Firstly, the fraud perpetrators by exploiting one of the following methods, acquire information and data in order to perform a fraud by using the CC resources of the CC Client.
  - **Skimming** is one of the most common forms of non-cash payment fraud in which criminals copy the information stored on a payment card by means of a small device attached to an Automatic Teller Machine (ATM).
  - **Phishing** scheme is a common form in which a user receives an email by fraud perpetrators that purports to be from his or her bank and contains a link to an infected website designed to appear legitimate.
  - **Pharming** occurs when attackers hijack a banks URL and manage to divert traffic to a site of their own that looks legitimate and similarly seeks to harvest credentials and other personal data.
  - **Phishing scams**, is a form in which consumers receive fraudulent emails pretending to come from government bodies or financial institutions which claim that consumers data is not valid and asks that this be corrected.

CC Case Study: Fraud Regulatory Framework

Startegic Security Plan Elements:

- Operational Management
- Technical Security and Controls
- Monitoring
- Reporting
- Log management
- Asset classification
- Incident management
- Audit and Compliance activities
- Physical security

CC Case Study: Fraud Regulatory Framework

Fraud Operator in CC environment:

- The CSP should not outsource the fraud risk management operations to third-party enterprises in order to isolate frauds and achieve the optimum result with controlled negative effects.
- The operator of fraud in the CC environment are the **anti-fraud teams**.
- Anti-fraud teams are housed in any independent facility of the CC environment.
- They are characterized by coordination and cooperation in the distributed environment of the CSP.
- Moreover, they cooperate with the national authorities which are responsible for such events.
- The anti-fraud teams consist of personnel with a variety of skills and knowledge in order to evaluate any fraud attempt by different perspective.

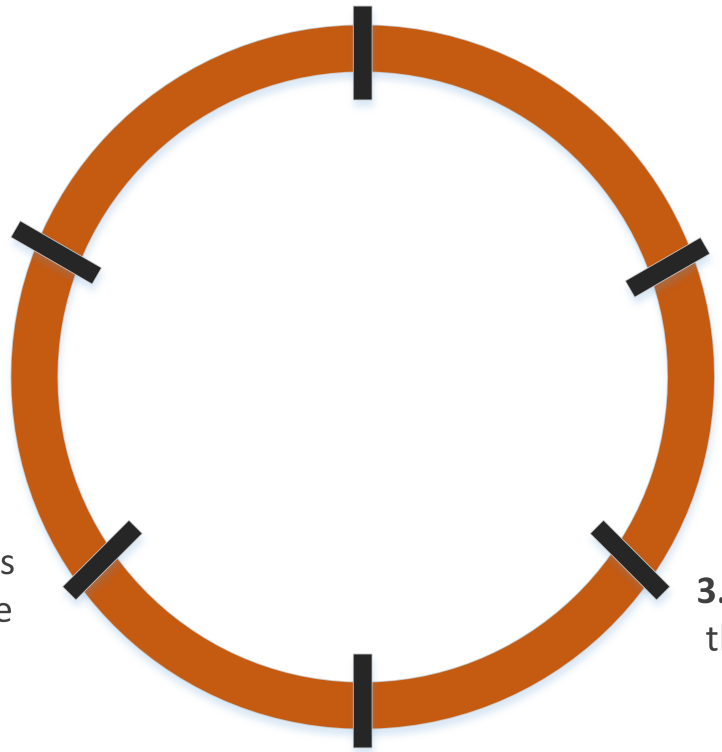
CC Case Study: Fraud Regulatory Framework

Fraud Assessment:

- During the risk assessment process firstly the anti-fraud team identifies opportunities and vectors to commit fraud.
- The fraud risk identification is performed both on the inside and outside perimeter of the environment.
- Moreover, the anti-fraud team should accomplish deep understanding of the processes and principles of corporate governance and gather information about potential fraud attempts.
- Two main fraud risks for the CC environment are:
  - The **misappropriation of assets** by interacting entities (e.g. clients, personnel) due to the distributed nature of assets.
  - The **corruption** is the process of exposure of confidentiality and misuse of cardholder data for private gain by the perpetrator.

CC Case Study: Fraud Regulatory Framework

Fraud Assessment Cycle in the Scenarios:



Fraud Assessment Activities

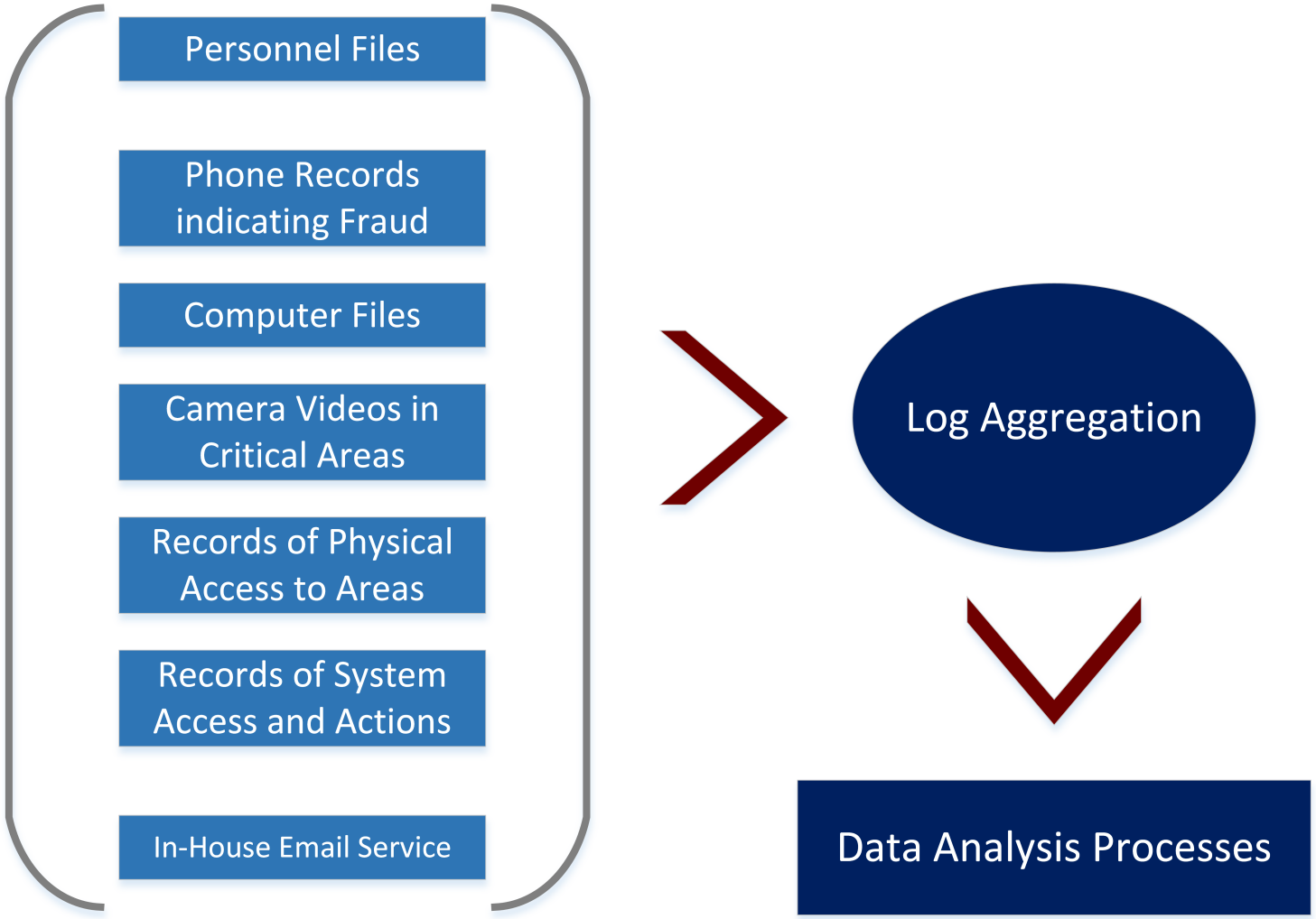
CC Case Study: Fraud Regulatory Framework

Fraud Detection:

- Fraud detection techniques should be combined with data analysis techniques and the auditing process.
- A data analysis technique could be used to construct the appropriate machine learning algorithm depending on the environment.
- The machine learning algorithm:
  - **consists** and automated process which would search for patterns, of fraudulent behaviour,
  - **gets** raw data by the log mechanisms of the environment (e.g. MySQL databases) ,
  - **performs** certain algorithmic features so as to create tidy data
  - and **applies** a statistical model with specific parameters to the tidy data.
- Moreover, the incorporation of fraud detection techniques in the auditing process which consists part of the agreed SLA creates certain dependencies. (e.g. time periods, authorized personnel)

CC Case Study: Fraud Regulatory Framework

Fraud Detection Logs:



Log Aggregation and Data Analysis

CC Case Study: Fraud Regulatory Framework

Fraud Detection Requirements:

- The detection techniques consist of processes in personal data and as a result according the regulations should be acknowledged to the natural people.
- Receiving and responding to complaints related to possible fraudulent activity by personnel or clients.
- The data analysis process should take place in real-time basis to achieve rapid provision of countermeasures in the environment.
- Continuous monitoring and auditing are necessary to identify and isolate fraud attempts effectively.
- Assessing the fraud detection mechanisms to identify correct operation under the conditions of the environment.
- The anti-fraud team should develop an approach regarding the fraud detection plan and its implementation.

CC Case Study: Fraud Regulatory Framework

Fraud Prevention:

- Fraud prevention techniques should be orchestrated in order to avoid fraud events to take place.
- Fraud prevention techniques consist of:
  - **Policies**, will balance the association of customer privacy and prevention of illegal activities.
  - **Personnel background checks**, performed prior to their recruitment and during their placement in the CC environment.
  - **Personnel interviewing**, will be performed in case of detection of a fraud attempt by the personnel.
  - **Internal procedures**, concerning the configuration of the systems which are responsible for the detection and prevention operations.
  - **Anti-fraud training**, consists of a period of courses and practical assignments to the personnel of the CC environment.
- Preventive control activities should be designed and implemented across the CC distributed environment in every independent facility.

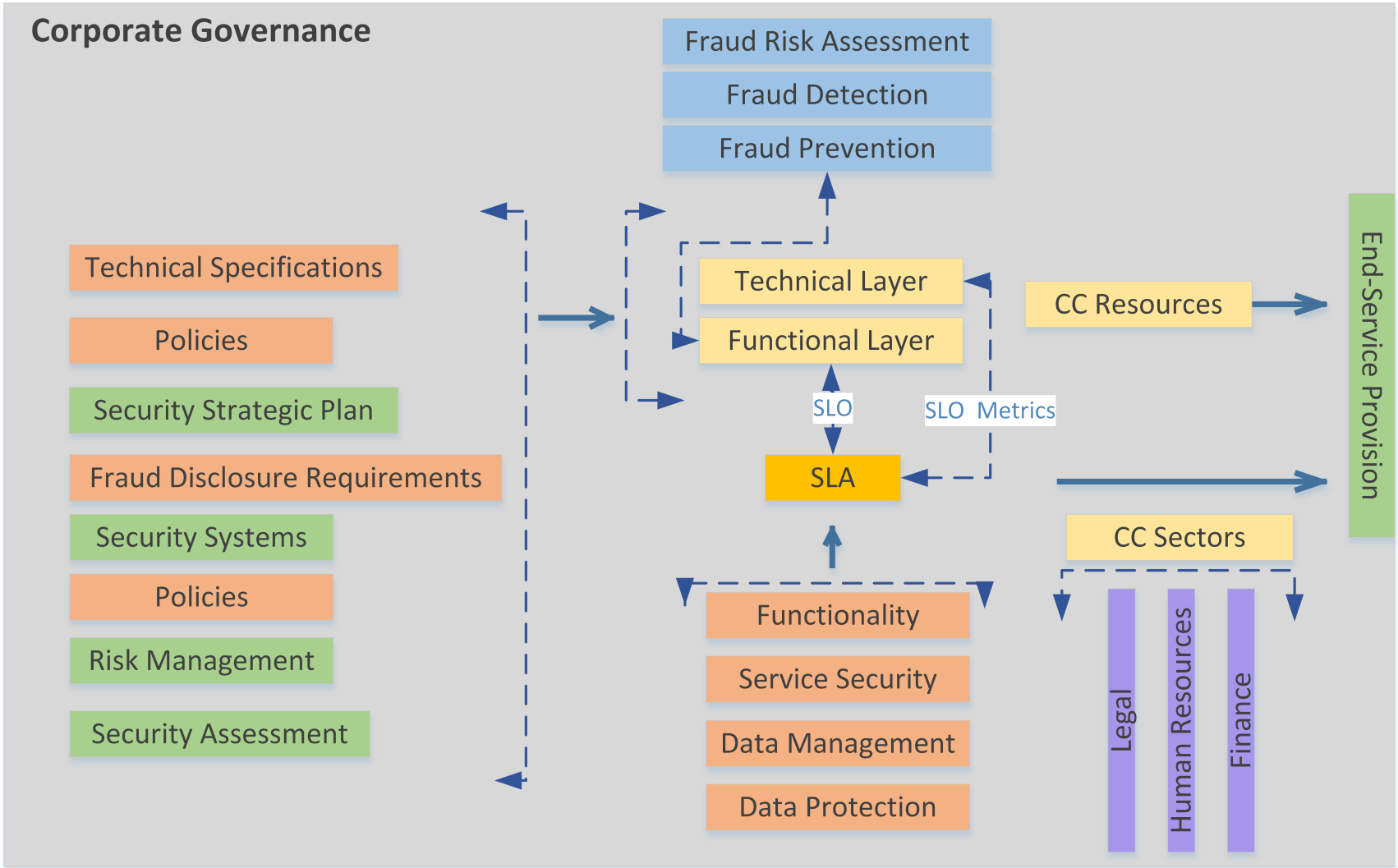
CC Case Study: Fraud Regulatory Framework

Fraud Disclosure Regulatory Framework Objectives:

- Perform data analysis and continuous auditing efforts should be based on assessment of the types of fraud schemes to which CC environments are susceptible.
- Ensure that the detection processes, procedures, and techniques remain confidential.
- Create a comprehensive documentation of fraud detection processes, procedures and techniques so that fraud detection vigilance is maintained over time.
- Train the personnel of the anti-fraud teams following professional standards in order the personnel to possess the appropriate competencies to support the regulatory framework.
- Periodically assess the effectiveness of fraud detection processes, procedures and techniques then document these assessments and revise so as to improve the framework.

CC Case Study: Fraud Regulatory Framework

Fraud Regulatory Framework:



Incorporation of the Fraud Disclosure Regulatory Framework in the Functional Layer

Conclusions

Synopsis

The proposed Regulatory Framework aiming to fraud disclosure:

- **assess** the cloud-based service and its infrastructure
- **determines** the outcome in case the underlying environment is constructed based on the SLA,
- **orchestrates** detection techniques in order to identify fraud attempts and
- **proposes** fraud prevention guidelines in organizational level so as to mitigate the association of fraud-insider threats

- The Member State in which the data controller is housed should embody to its national legislation the Directives defined by the European Commission concerning fraudulent activities.
- The Cross-Border regulations that are used to define the SLA force the CSP to operate legally but without adequate security constraints.

Conclusions

- The CSP should reinforce its environment with a security architecture in order to mitigate the vast majority of threats in technical level and then face the fraudulent activities.
- The presented CC security architecture propose the adaptation of the concept of defence in depth in a CC environment.
- The evaluation of the multi-layered security architecture established that leads to mitigation of serious threats of this environment.

Future Work!

- Work needs to be done on Governmental or Regional legislation to strengthen the Cross-Border guidelines for the transfer of PII in the context of CC.
- It is necessary to standardize a Fraud related Regulatory Framework in European level so as it can be outsourced by the data controller to the data processor during a cross-border scenario.

Thank you for the attention! Questions?

Dimitrios D. Vergados and Theodoros Mavroeidakos

Department of Informatics, University of Piraeus
80, Karaoli and Dimitriou St., GR-185 34, Piraeus, Greece
Email: vergados@unipi.gr
Tel: +30 210 4142479
Fax: +30 210 4142119

Hellenic Telecommunications and Post Commission (EETT)
60, Kifissias Avenue
GR- 151 25 Maroussi, Greece

National Technical University of Athens, Greece
Heroon Polytechniou 9, GR-15780 Zografou, Greece
Email: mavroeidakos.theodoros@gmail.com

References I

- Focus Group on Cloud Computing Technical Report (2012). Part 2: Functional requirements and reference architecture Telecommunication Standardization Sector of ITU, pp.5-32.
- Focus Group on Cloud Computing Technical Report (2012). Part 3: Requirements and framework architecture of cloud infrastructure Telecommunication Standardization Sector of ITU, pp.37-37.
- European Union law and publications (1995). Directive 1995/46/EC of the European Parliament and of the Council.
- Article 29 Working Party (2005) Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.
- European Union law and publications (2009), Directive 2009/136/EC of the European Parliament and of the Council.
- European Union law and publications (2010) Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.
- Halpert J., Dyson A., Van Eecke P., Umhoefer C., Jansen T., Ramos D., Van Schaik R., Alec C., Thiel S. (2014). Data protection laws of the world, DLA Pipers Data Protection, Privacy and Security group, pp.386-390

References II

- Catteddu D. and Hogben G. (2009). Cloud Computing: Information Assurance Framework European Network and Information Security Agency.
- Catteddu D. and Hogben G. (2009). Cloud Computing: Benefits, risks and recommendations for information security, European Network and Information Security Agency, pp.23-52.
- Computer Security Division, Information Technology Laboratory, (2004). Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication, pp. 5-8.
- Wayne J. and Timothy G. (2011). Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of Commerce, Special Publication 800-144, pp.7-36.
- Kandias M., Virvilis N., Gritzalis D. (2013). The Insider Threat in Cloud Computing, Critical Information Infrastructure Security, Volume 6983, 2013, pp.93-103.
- Brough D., (2003), Second Generation Honeynet Honeywall. GIAC Security Essentials Certification, SANS Institute, pp. 2-14.
- Michael P. Brennan, (2002). Using Snort For a Distributed Intrusion Detection System. SANS Institute, pp. 2-12.
- Jianhua C., Yamin D., Tao Z. and Jie F., (2011), Study on the security models and strategies of cloud computing. Procedia Engineering, 23, pp. 586-593, ISSN: 1877-7058.
- Migl A., Jaun D., Ann N., Caroline C. and Jana H. U., (2013) ECC-Net Fraud in cross-border e-commerce.
- Danezis G., Domingo-Ferrer J., Hansen M., Hoepman J., Metayer D., Tirtea R. and Schiffner S. (2014). Privacy and Data Protection by Design-from policy to engineering, European Network and Information Security Agency, pp.13-42