Auditing Hybrid IT Environments

Georgiana Mateescu
Computer Science and Automatic Control Faculty
Polytechnic University of Bucharest
Bucharest, Romania

Marius Vlădescu
Computer Science and Automatic Control Faculty
Polytechnic University of Bucharest
Bucharest, Romania

***Abstract*—This paper presents a personal approach of auditing the hybrid IT environments consisting in both on premise and on demand services and systems. The analysis is performed from both safety and profitability perspectives and it aims to offer to strategy, technical and business teams a representation of the value added by the cloud programme within the company's portfolio. Starting from the importance of the IT Governance in the actual business environments, we presented in the first section the main principles that drive the technology strategy in order to maximize the value added by IT assets in the business products. Section two summarizes the frameworks leveraged by our approach in order to implement the safety and profitability computation algorithms described in the third section. The paper concludes with benefits of our personal frameworks and presents the future developments.**

Keywords—audit cloud computing; cloud service safety; cloud governance

I. Introduction

Nowadays, the companies must continuously provide efficient innovation strategies, by making the IT environment more agile in order to support radical changes on the business process and information flows due to the economic instability and permanent changes in the market.

Together with the requirements of flexibility, scalability and elasticity, the IT environment mandates a new dimension that should ensure proper management of change and efficient operations on both existing and new IT assets. The technology manifests a trend of migrating from specialized "systems" to dedicated services, becoming more and more platform independent in order to get the maximum value from the information technology. This is how in 2003, a new concept was built – IT Governance that aimed to put together all the concepts, definitions, processes, procedures and methodologies that, by reassembling them into a common framework, are able to implements IT programs to deliver high profitability in the business dimension.

Enterprise governance of IT (EGIT) represents the conceptual and pragmatic definition and implementation of processes, structures and relational mechanisms that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments [1].

The six principles that define the Enterprise Governance of IT are [2]:

1) Responsibility – this principle refers to the people and the groups of people within the company that must be aware of their responsibilities regarding the supply of and demand for IT. Also, this principle supposes that those with responsibility for actions also have the authority to perform those actions.

2) Strategy – The organization's business strategy considers the current capabilities of IT, the value delivered by the information technology as related to the programs implemented and tries to address the business needs in the ongoing and future initiatives.

3) Acquisition – IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making based on practical business cases that demonstrate a proper balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

4) Performance – IT is able to support the organization, by providing the services, levels of service and service quality that meet current and future business requirements.

5) Conformance – IT complies with all mandatory legislations and regulations. Policies and practices are clearly defined, implemented and enforced.

6) Human Behavior – IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

In order to assess correctly the IT Governance, a proper audit process must be conducted that, starting from mature evaluation frameworks, analyses the specific company and offers a value of the IT Governance level.

In this paper we propose an efficient methodology to audit the hybrid IT environments that consist in both on premise and on demand systems, in order to evaluate the level of the cloud service safety and its profitability. Starting from two existing frameworks presented in Section II, we describe our personal approach in the thirds section of the paper. The paper concludes with the benefits of our approach and future works.

II. Auditing It Governance Frameworks

There are a lot of frameworks that evaluate the governance and the efficiency of IT environments from different perspectives, one of them is defined in [14]. In our approach, we want to offer a methodology of assessing the safety of the cloud service and its profitability. In order to do that, we start from the Cloud Security Alliance security model and, for each of the domains defined in [3] we specified security controls. The security controls compose the audit questionnaire. The audit process evaluates the control mechanisms using an algorithm based on the maturity level provided by COBIT. In this section, we made a summary of the main characteristics of the frameworks and standards leveraged by our approach.

A. CSA – Security Model

According to [3] the level of security measures within an organization is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), all the way to the information and applications (application security).

Cloud Security Alliance categorizes security domains as presented in Table 1.

TABLE I. : CLOUD COMPUTING SECURITY DOMAINS

Domain	Description
Governance and Enterprise Risk Management	The ability to govern and measure risk introduced by cloud computing
Legal Issues: Contracts and Electronic Discovery	Security breach disclosure law
Compliance and Audit	Evaluate how cloud affects compliance
Information Management and Data Security	Managing data stored in cloud
Portability and Interoperability	The ability to move data from a cloud provider to another
Traditional Security, Business Continuity and Disaster Recovery	How cloud affects the current security procedures
Data Center Operations	How to evaluate provider's data center architecture and operations
Incident Response, Notification and Remediation	Proper incident detection, response, notification and remediation
Application Security	Securing application that runs on different cloud deployment model
Encryption and Key Management	Identify proper key usage and key management
Identity and Access Management	Cloud-based IdEA (Identity, Entitlement and Access Management)
Virtualization	Risk associated with VM isolation, VM co-residence
Security as a Service	Third party security assurance including incident management and compliance attestation

Starting from this security domains classification for the cloud models [19], we defined for each of the areas mentioned in the table above, the required controls that lower the risk associated with the domain. This research activity was performed based on existing cloud practice and traditional security measures and concluded in the definition of most relevant mechanisms and procedures that must be evaluated during an audit process.

In order to assess the level of conformity and the risk associated with the lack of mature implementation of the mechanisms, we used the capability model defined by COBIT.

B. COBIT

COBIT (Control Objectives for Information and Related Technology) [4] represents the framework implemented by ISACA in order to define the environment of a company that defines governance and management of enterprise IT from both business and management perspective.

This framework is based on five principles:

1) Meeting Stakeholder Needs – this principle describes the COBIT objectives from IT requirements perspective that must fulfill the business needs.

2) Covering the Enterprise End-to-End – this principle describes the approach used in this framework to address all the aspects related to IT components management and governance by relating them with the existing business processes and information flows.

3) Applying Single Integrated Framework – this principle describes the scope of COBIT to include all the functions and process that exists within a company in a single framework.

4) Enabling a Holistic Approach – this principle presents the IT Governance and Management in s systematic way by controlling them with a generic model proposed by ISACA. This model is driven by IT enablers that address all the existing resources and facts that lead to IT governance.

5) Separating Governance from Management – this principle describes the differences between the two processes and the mechanism that interconnects them.

Based on these principles, ISACA build a capability model able to evaluate the level of IT governance and management. This model consists of 6 different capability levels each control can implement. The next picture depicts the COBIT 5 Capability model leveraged by our approach:

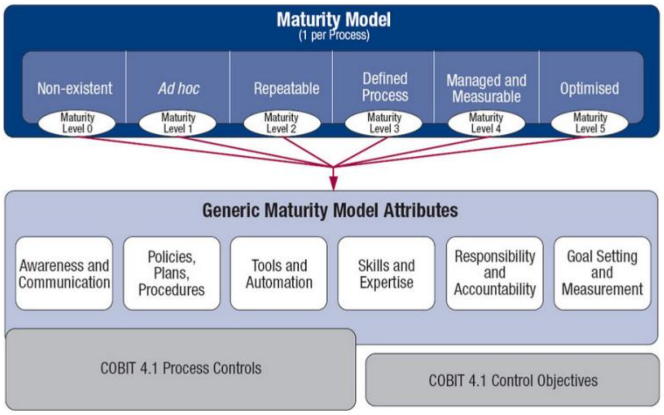


Fig. 1. COBIT Capability Model [4]

This capability level implements the restriction that each level can be achieved only after the previous one was successfully fulfilled. Also, there is a huge difference between the process that is in level 1 and the ones in superior levels because, once the process reached level 1, it means that all the performance attributes were achieved.

C. Val IT

ISACA describes in [5] an evaluation model for the value added to the enterprise by the IT programs. This framework is based on the following principles:

IT-enabled investments will:

1) Be managed by an investment portfolio

2) Include all the activities required in order to obtain the business benefits from the IT program

3) Be managed through their entire economical lifecycle Value delivery practices will:

4) Recognize there are different categories of investments that will be evaluated and managed differently

5) Define and monitor key metrics and respond quickly to any changes or deviations

6) Engage all stakeholders and assign appropriate accountability for the delivery of capabilities and the realization of business benefits

7) Be continually monitored, evaluated and improved

Val IT uses the following concepts in order to assess the maturity level of an enterprise in implementing IT programs [5]:

Project—A structured set of activities concerned with delivering a defined capability to the enterprise based on an agreed-upon schedule and budget

Programme—A structured group of inter-dependent projects that are both necessary and sufficient to achieve a desired business outcome and create value.. The investment programme is the primary unit of investment within Val IT.

Portfolio—Groupings of 'objects of interest' (investment programmes, IT services, IT projects, other IT assets or resources) managed and monitored to optimize business value. The investment portfolio is of primary interest to Val IT. IT service, project, asset or other resource portfolios are of primary interest to COBIT.

The maturity evaluation is implemented within Val IT using specific process metrics that analyze the information flows and business process from the following perspectives:

Value Governance - the goal of this domain is to ensure that value management practices are embedded in the enterprise, enabling it to secure optimal value from its IT-enabled investments throughout their full economic life cycle.

Portfolio Management – the goal of this domain is to ensure that an enterprise secures optimal value across its portfolio of IT-enabled investments.

Investment Management – the goal of this domain is to ensure that the enterprise's individual IT-enabled investments contribute to optimal value.

The picture below depicts the Val IT processes and domains:

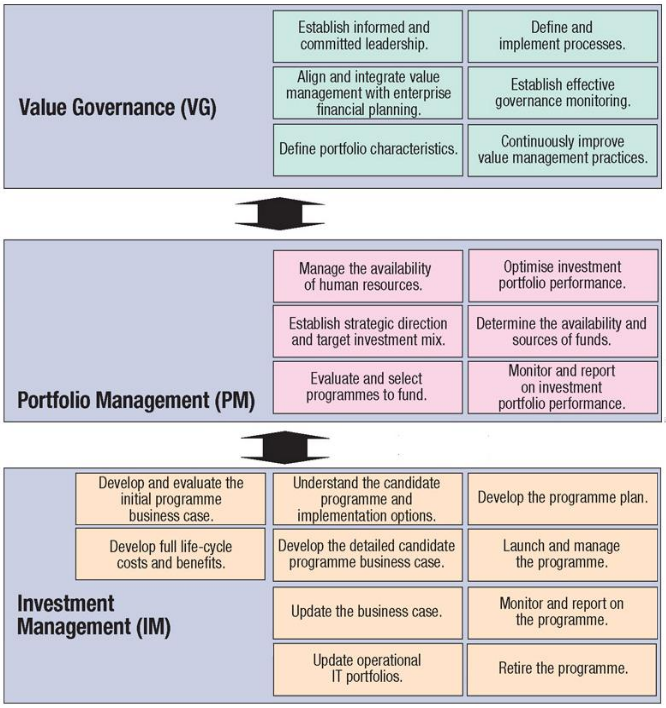

Value Governance (VG)
Establish informed and committed leadership.
Define and implement processes.
Align and integrate value management with enterprise financial planning.
Establish effective governance monitoring.
Define portfolio characteristics.
Continuously improve value management practices.
Portfolio Management (PM)
Manage the availability of human resources.
Optimise investment portfolio performance.
Establish strategic direction and target investment mix.
Determine the availability and sources of funds.
Evaluate and select programmes to fund.
Monitor and report on investment portfolio performance.
Investment Management (IM)
Develop and evaluate the initial programme business case.
Understand the candidate programme and implementation options.
Develop the programme plan.
Develop full life-cycle costs and benefits.
Develop the detailed candidate programme business case.
Launch and manage the programme.
Update the business case.
Monitor and report on the programme.
Update operational IT portfolios.
Retire the programme.

Fig. 2. Val IT Processes and Domains

In our approach we use this model in order to determine the level of the enterprise maturity related to the implementation of cloud programmes. Beside COBIT and Val IT, ISACA also issued a number of papers that describe general guidelines [6] regarding the evaluation of business continuity and the IT governance within cloud computing architecture [7][8].

Starting from these specialized opinions, we created an audit framework that quantifies the safety level of a cloud service based on the security measures implemented within the architecture analyzed. During our assess, we have a second indicator – the profitability level of the programme that invested in the cloud service, which is computed based on the maturity level of the company's practices used during the programme and on the risk manifested by the cloud service, evaluated in the safety section of the audit.

III. Personal Approach

A. General Approach

Our audit methodology is based on questionnaires consisting in security measures defined for hybrid TI environments that ensure a high level of safety, governance and operability within the infrastructure.

These controls and classified in domains according to the guidelines from [3] presented in the second section of this paper. They address the major aspects of each domain by analyzing both on premise and on demand specific controls and procedures.

The audit process can address one or multiple domains within one assessment [20]. Each control is evaluated using the capability model of COBIT presented in section 2 which represents the reference model in assessing the level of implementation of each security mechanism included in the audit questionnaire. The security measures [18] and procedures address both service provider and consumer assets. The safety level is computed against an assumed level of risk for each cloud service and an application sensibility:

- The assumed level of risk has direct impact in computing the safety level by addressing the difference between the actual level of security control implementation and the maximum one
- The application sensibility reflects in the correction factor inserted in the computation of risk, by the previously mentioned difference.

After computing the safety level, we offer an approach that quantifies also the level of conformity with the CSA [3] best practices and recommendation. This indicator is computed against the assumed risk level that is materialized in the minimum safety level that must be met by the domain in order to be classified as compliant. Once the domain is compliant, the conformity level is computed based on the safety level.

For the computation of profitability level, beside the analysis of the security measures realized using the approach we defined above, we use Val IT process measures to assess the level of company's maturity in implementing, governing and operating the hybrid IT programmes.

The evaluation that leverages the Val IT framework uses the 3 domains described in the previous section and evaluates the maturity of the metrics included in the audit questionnaire by comparing estimated maturity level with the one obtained after the assessment.

The profitability assessment can be conducted for a single programme or for the entire portfolio. In case the audit addresses the entire portfolio, the profitability factor algorithm takes into consideration the risk level of the audited programme within the portfolio, and for the other ones, it computes the profitability level by evaluating only the maturity level.

At the end of this methodology, we present a mechanism to compute the internal rate of return of the audit target – the portfolio or the programme addressed during the audit process.

In the next two sections we present our personal methodology of evaluating the safety and profitability level for an assessed cloud service contracted within a hybrid IT environment.

B. *Computation of Safety Level*

The safety level represents the level of security controls implementation as compared to the assumed risk defined for the application that is been evaluated.

In order to compute the safety level, the audit process must address the entire audit questionnaire for the domain being evaluated. Based on the responses, we define the application risk as the uncertainty rate reported to the cloud vulnerabilities from the analyzed security domain, materialized in the implementation level of each control:

$$AR_i = c_{NSA} + \sum_{k=1}^{n}(5 - s_k)\cdot c_A \quad (1)$$

Where:

- AR_i is the application risk for the evaluated domain i
- c_{NSA} is the correction risk constant computed based on the existing cloud community experience. Its value is 0.01 and it is introduces for practical reasons because there is no domain with zero risk.
- s_k is the implementation level for control *k* from the domain *i*
- c_A is the correction constant applied to the risk defined for the control. This constant depends on the industry the target belongs to, and on the sensitivity rate of the cloud service.
- *n* is the number controls being evaluated in the audit process

Each cloud service analyzed has associated with it the assumed level of risk ranked from 1 to 3 – 1 meaning that the service should be very secured and 3 meaning that, providing the type of data and the business process and information flows being implemented in the cloud, the balance between security and costs should go on the cost savings side. The risk level is defined by the strategy team during the documentation of the business case that leads to the programme implementation. The assumed level of risk is evaluated using the following expression:

$$AR'_i = RL\cdot n\cdot c_A \quad (2)$$

Where:

- AR'_i is the assumed risk for the evaluated domain i
- RL is the risk level defined in the programme business case
- c_A is the correction constant applied to the risk defined for the control. This constant depends on the industry the target belongs to, and on the sensitivity level of the cloud service.
- n is the number controls being evaluated in the audit process

Using the two measures presented above, the safety level is computed using the following expression:

$$SL_i = \frac{5n(1-c_A) - {AR_i}/{AR'_i}}{5n} \cdot 100 \quad (3)$$

Where:

SL_i is the safety level for the evaluated domain *i*

c_A is the correction constant applied to the risk defined for the control. This constant depends on the industry the target belongs to, and on the sensitivity level of the cloud service.

AR'_i is the assumed risk for the evaluated domain *i*

AR_i is the application risk for the evaluated domain *i*

n is the number controls being evaluated in the audit process

For the scenarios when the audit process evaluates multiple domains, the safety level is the arithmetic mean of the safety levels of the individual domains:

$$SL = \frac{\sum_{i=1}^{n} SL_i}{n} \quad (4)$$

Where:

- SL is the safety level of the audit process
- SL_i is the safety level for the evaluated domain *i*
- *n* is the number of domains in scope for the audit process.

Based on the safety level and on the assumed risk level, the conformity level is computed using the following expression:

$$CL_i = \frac{1+(-1)^c}{2}(SL_{\min} + \frac{SL_i - SL_{\min}}{SL_{\min}}) \quad (5)$$

Where:

- CL_i is the compliance level for the evaluated domain *i*
- SL_i is the safety level for the evaluated domain *i*
- *c* is the compliance factor that ensure that the compliance level is zero if the minimum safety level is not reached. This factor is computed using the following expression:

$$c = \begin{cases} 1, SL_i < SL_{\min} \\ 2, SL_i > SL_{\min} \end{cases} \quad (6)$$

- $SL_{\min}$ is the minimum safety level that must be obtained by a domain in order to be compliant and it is computed based on the assumed level of risk:

$$SL_{\min} = 1 - RL \cdot c_c \quad (7)$$

Where:

- $SL_{\min}$ is the minimum safety level
- RL is the assumed risk level for the application
- c_c is the conformity constant and its value depends on the assumed risk level according to the following table:

TABLE II. CONFORMITY CONSTANT VALUES

Risk Level = *RL*	Conformity Constant = c_c
1	0.001
2	0.25
3	0.33

The conformity level is the measure of the security and governance measures and controls implementation within the audit architecture evaluated against the best practices recommended by the standards used as references when we defined the audit framework.

Therefore the two levels computed by our approach in the safety section of the audit process, offer a realistic view of the contracted cloud service by analyzing the entire integration context.

Our methodology analyzes cloud provider and consumer controls in order to evaluate the level of performance, governance, risk, management and operation of the IT domain by including in the audit questionnaire assets from both parties.

C. Computation of Profitability Level

The profitability level represents the rate of capitalization of the financial investments engaged for a programme.

In order to compute the profitability level, our approach starts from the maturity level of programme evaluated using specific process metrics. All the processes and flows metrics are classified into the Val IT specific domains and address the following topics:

- Level of leadership agreement on value governance principles
- Level of leadership engagement
- Degree of implementation and compliance with value management processes
- Level of satisfaction with IT's contribution to business value
- Percentage of IT expenditures that have direct traceability to business strategy
- Percentage increase in portfolio value over time
- New ideas per investment category, and percentage that are developed into detailed business cases
- Completeness and compliance of business cases (initial and updated)
- Percentage of expected value realise

After the audit process assesses all the audit questionnaire items, the maturity score is computed:

$$MS = \frac{\sum_{i=1}^{m} ms_i}{m} \quad (8)$$

Where:

- MS is the maturity score of the programme being analyzed
- ms_i is the maturity score of the metric *i*
- m is the total number of metrics that are evaluated during the audit process

Using the maturity score computed using (8) and the expected maturity level defined within the business case of the audited programme, we defined the indicator of achievement:

$$i_a = \frac{MS}{ML} \cdot 100 \quad (9)$$

Where:

- i_a is the indicator of achievement of the analyzed programme
- MS is the maturity score of the programme being analyzed
- ML is the expected maturity level defined for the programme being analyzed

Based on the achievement indicator, we compute the underperformance index:

$$ui = \frac{1 + (-1)^{c_j}}{2} \cdot (1 - i_a) \quad (10)$$

Where:

- ui is the underperformance index of the programme
- i_a is the indicator of achievement of the analyzed programme
- c_f is the completion factor of the programme:

$$c_f = \begin{cases} 2, i_a < 1 \\ 1, i_a \geq 1 \end{cases} \quad (11)$$

Where:

- c_f is the completion factor of the programme
- i_a is the indicator of achievement of the analyzed programme

The underperformance index has direct impact on the update rate used to compute the Net Present Value which classifies an investment as being profitable or not.

The update rate is the method that provides a measure to the comparison between the economical parameters and financial indicators accomplished in different periods of time allowing in this way the classification of the program/investment as profitable.

In order to compute the update rate in the hybrid IT environments audit process we use the following expression:

$$u_r = f(ui, c_i, R) \quad (12)$$

Where:

- u_r is the update rate used in order to compute the profitability of the programme
- ui is the underperformance index of the analyzed programme
- c_i is the cost of the investment in the programme
- R is the risk indicator associated with the cloud service implemented in the analyzed programme

For the audit processes that address the entire portfolio, without assessing the safety evaluation for the all the programmes, the update rate is computed as the arithmetic mean of the updates rates of all the programmes. If the programme was not assessed for safety, the update rate is computed using the expression:

$$u_r = c_i + ui \quad (13)$$

Where:

- u_r is the update rate used in order to compute the profitability of the programme
- ui is the underperformance index of the analyzed programme
- c_i is the cost of the investment in the programme

For the programmes where the safety evaluation was conducted, the update rate is:

$$u_r = ui + c_i + R \quad (14)$$

Where:

- u_r is the update rate used in order to compute the profitability of the programme
- ui is the underperformance index of the analyzed programme
- c_i is the cost of the investment in the programme
- R is the risk indicator associated with the cloud service implemented in the analyzed programme

The risk indicator is the arithmetic mean of the risks associated with all the domains being addressed by the safety assessment:

$$R = \frac{\sum_{i=1}^{n} 1 - SL_i}{n} \quad (15)$$

Where:

- R is the risk indicator associated with the cloud service implemented in the analyzed program
- SL_i is the safety level for the evaluated domain i
- n is the number of domains in scope for the audit process

The Net Present Value (NPV) represents an investment evaluation method that is dependent on the total amount of costs and incomes for a programme. NPV makes comparisons between cash flow of the program and investment effort involved in doing so. The formula for calculating this is:

$$NPV = I_T - C_T \quad (16)$$

Where:

- NPV is Net Present Value of the programme
- I_T is the total income
- C_T is the total cost

The total income is defined by:

$$I_T = \sum_{k=1}^{y} \frac{I_E}{(1+u_r)^k} \quad (17)$$

Where:

- I_T is the total income
- I_E is the estimated income for year k
- u_r is the update rate
- y is number of years the programme lasts

The total costs are computed based on:

- Initial investments
- Operational costs during the programme
- The programme period
- The update rate

$$C_T = TI + \sum_{k=1}^{y} \frac{C_O}{(1+u_r)^k} \quad (18)$$

Where:

- C_T is the total cost
- TI is total investment in the programme
- C_O is the operation cost for year k
- u_r is the update rate
- y is number of years the programme lasts

Considering (17) and (18), the NPV is:

$$NPV = \sum_{k=1}^{y} \frac{I_E}{(1+u_r)^k} - (TI + \sum_{k=1}^{y} \frac{C_O}{(1+u_r)^k}) \quad (19)$$

For the audit processes that address the entire portfolio, the NPV is computed for each programme the portfolio contains. In this way we are able to assess the profitability of each of the portfolio components. In order to evaluate the overall profitability, the update rate for the portfolio NPV is computed using the mean update rate of all programmes included in the portfolio.

Based on NPV, we defined the profitability level as:

$$PL = \begin{cases} 0, NPV < 0 \\ 1, NPV \geq 0 \end{cases} \quad (20)$$

Where:

- PL is the profitability level
- NPV is Net Present Value of the programme

In order to determine the profitability level of the portfolio we use the same expression, but the update rate is computed by considering the individual update rates for each programme with the portfolio.

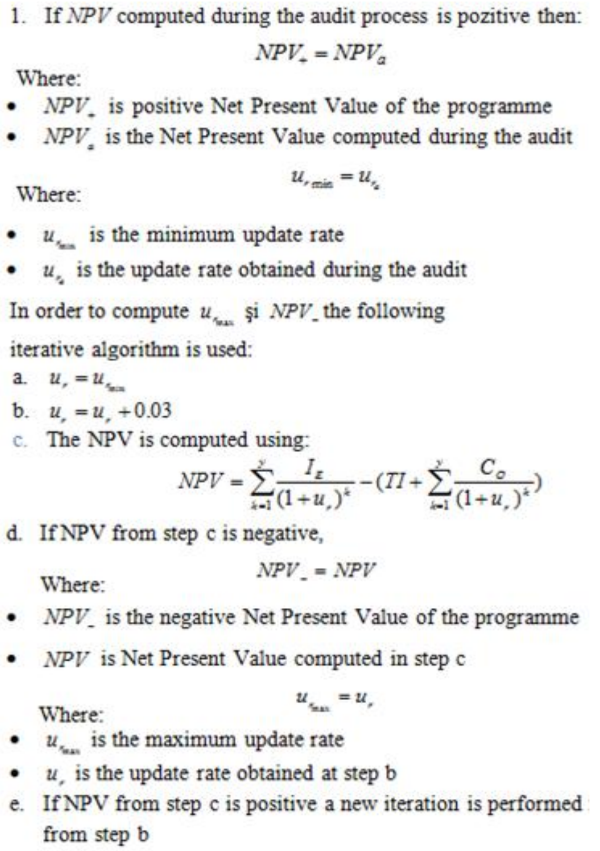
In order to evaluate another specific economic factor, the internal rate of return, we use the following expression:

$$IRR = u_{r_{\min}} - (u_{r_{\max}} - u_{r_{\min}}) \cdot \frac{NPV_+}{NPV_+ - NPV_-} \quad (21)$$

Where:

- IRR is the internal rate of return
- $u_{r_{\min}}$ is the minimum update rate – this rate ensures a positive NPV which classifies the investment as profitable
- $u_{r_{\max}}$ is the maximum update rate – this rate ensures a negative NPV
- NPV_+ is the positive Net Present Value of the programme – this value classifies the investment as profitable
- NPV_- is the negative Net Present Value of the programme

In order to compute the required measures for the internal rate of return, we use the following algorithms:



1. If NPV computed during the audit process is pozitive then:

$$NPV_{+} = NPV_{a}$$

Where:

- NPV_{+} is positive Net Present Value of the programme
- NPV_{a} is the Net Present Value computed during the audit

$$u_{r_{min}} = u_{r_a}$$

Where:

- $u_{r_{min}}$ is the minimum update rate
- u_{r_a} is the update rate obtained during the audit

In order to compute $u_{r_{max}}$ şi NPV_{-} the following

iterative algorithm is used:

a. $u_r = u_{r_{min}}$

b. $u_r = u_r + 0.03$

c. The NPV is computed using:

$$NPV = \sum_{k=1}^{y} \frac{I_E}{(1+u_r)^k} - (TI + \sum_{k=1}^{y} \frac{C_O}{(1+u_r)^k})$$

d. If NPV from step c is negative,

$$NPV_{-} = NPV$$

Where:

- NPV_{-} is the negative Net Present Value of the programme
- NPV is Net Present Value computed in step c

$$u_{r_{max}} = u_r$$

Where:

- $u_{r_{max}}$ is the maximum update rate
- u_r is the update rate obtained at step b

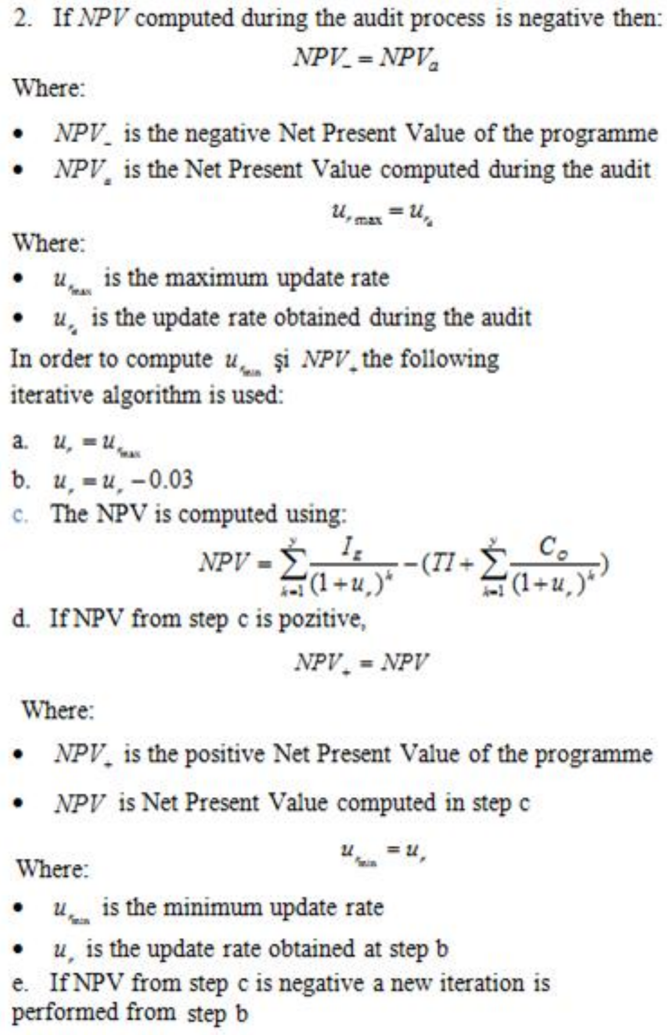
e. If NPV from step c is positive a new iteration is performed from step b

Fig. 3. Algorithm to compute IRR measures if the audited NPV is pozitive

The picture above depicts the method used to find the measures required in order to compute the internal rate of return if, after conducting the profitability audit according to the methodology we proposed, the result of NPV is positive.

The picture below depicts the method used to find the measures required in order to compute the internal rate of return if, after conducting the profitability audit according to the methodology we proposed, the result of NPV is negative. Usually, in this scenario, the IRR obtained will be less than the one expected by the investors providing that a negative NPV during the audit highlights a lack of profitability for that programme.

In these scenarios a deep analysis must be performed in order to see if the risks and maturity levels assessed during the audit must be fine-tuned which means the expectations for the programme were not properly set, or if the programme did not reach the maturity expected and its security and governance mechanisms and controls do not prove enough capabilities.



2. If NPV computed during the audit process is negative then:

$$NPV_{-} = NPV_{a}$$

Where:

- NPV_{-} is the negative Net Present Value of the programme
- NPV_{a} is the Net Present Value computed during the audit

$$u_{r_{max}} = u_{r_a}$$

Where:

- $u_{r_{max}}$ is the maximum update rate
- u_{r_a} is the update rate obtained during the audit

In order to compute $u_{r_{min}}$ şi NPV_{+} the following

iterative algorithm is used:

a. $u_r = u_{r_{max}}$

b. $u_r = u_r - 0.03$

c. The NPV is computed using:

$$NPV = \sum_{k=1}^{y} \frac{I_E}{(1+u_r)^k} - (TI + \sum_{k=1}^{y} \frac{C_O}{(1+u_r)^k})$$

d. If NPV from step c is pozitive,

$$NPV_{+} = NPV$$

Where:

- NPV_{+} is the positive Net Present Value of the programme
- NPV is Net Present Value computed in step c

$$u_{r_{min}} = u_r$$

Where:

- $u_{r_{min}}$ is the minimum update rate
- u_r is the update rate obtained at step b

e. If NPV from step c is negative a new iteration is performed from step b

Fig. 4. Algorithm to compute IRR measures if the audited NPV is negative

In this section we presented an efficient mechanism of economical rates evaluation by considering during the analysis both financial and technical aspects from the IT programme being assessed. In this way we offered a relevant representation of the contracted cloud service for both technical and non-technical representatives from company being evaluated. We managed with our approach to translate the security measures and procedures in business figures able to classify the investment as profitable or not. Also, based on the Val IT maturity level leveraged in our framework, we measured the governance and management capabilities of the company in operating the analyzed IT asset. This offers an important decision support for the strategy team regarding the development direction and new cloud adoption roadmap.

IV. CONCLUSIONS

The information security and knowledge profitability are some the most important aspects within an organization that ensure business continuity and minimization of risk [13]. Their maximum benefits can be achieved by leveraging the IT assets capabilities in order to ensure data availability, business process and information flow high performance, sensitive data protection and business agility. All these characteristics can be obtained only if the company implements a proper IT governance and efficient management and operational processes and procedures.

A proper IT Governance strategy ensures the following benefits [9]:

- Cost reduction;
- Performance improvement;
- Ability to react quickly to market changes;
- Increased customer satisfaction;
- More sustainable practices;
- Increased revenue per dollar cost;
- General workplace benefits for the board, management and staff.

By combining technical aspects [10] [12] divided into main security drivers with governance and operations related factors, our approach offers a full evaluation analysis of cloud system that quantifies the overall safety of the cloud safety [11] from both technological and operational perspective. In this way, the audit process can be a key decision support for the IT strategy roadmap.

After the safety evaluation, we implemented a methodology to quantify the profitability of the IT programme that implemented the cloud service, offering in this way an economical representation of the service risk related to the operational, governance and security aspects analyzed during the first step of the audit process.

Our approach offers the following benefits:

- Quantifies the safety score based on security measures and controls that are compliant with cloud standards by comparing the implementation rate of key security controls with the assumed risked for the cloud service. In this way we managed to implement an efficient algorithm that takes into consideration all key contextual factors from the cloud service implementation and adoption process.
- Measures the conformity level for the standards used as reference in defining the audit framework. The main standard leveraged is the CSA Security model [3], but when we defined the specific controls to be evaluated, we included the best practice and state of the art of the security measures implemented in the traditional architecture and adopted also by the cloud community.
- Computes the conformity level based on the assumed risk and it is evaluated on each analyzed domain, emphasizing in this way the domains that require improvement [17].
- Offers an efficient methodology for complex analysis that shows strengths and weaknesses of the analyzed cloud service [16] in the enterprise architecture [18]
- Offers decision support for future cloud adoption by evaluating the rate of company maturity and adaptability to change by assessing the entire stack of mechanisms, controls, process and procedures defined within the company in order to obtain an efficient governance and management process.
- By using as a reference model an international standard, we ensure that the principals, best practices and mature recommendations are part of the audit process. Also, by leveraging an existing framework for initial assessment of the implementation level, we obtain all the benefits of a framework that proved its value during the experience.
- Offers a business relevant measures of the IT assets, by quantifying the profitability level of the programme based on the cloud service risk
- Offers a financial overview of the IT programme that implements the cloud service which can be used as decision support for future IT innovation strategies
- Assesses the level of the organization adaptability to the new trend of cloud computing
- Assesses the maturity and efficiency of the existing governance and management procedures for the new type of IT environment: the cloud computing architecture
- Assesses the integration between on premise and on demand systems by evaluating key security factors. This is possible due to the holistic representation of the audit process that assesses the control measures on domain basis.

By providing all the advantages mentioned above, our methodology helps the company gain visibility on their own IT environment by evaluating the governance, management and operations maturity levels using a holistic approach together with the security aspects [15].

This approach suffers permanent changes as the cloud practice keeps on gaining more and more maturity and adopters. Considering this, our set of controls must be permanently updated and adapted on the specificity of the system and business processes being analyzed.

In order to optimize our evaluation method, we want to fine tune the security measures being assessed by specializing the audit process based on industries and types of companies. In this way we can evaluate particular controls imposed by specific standards and regulations. Other improvement would consist in leveraging the approach for cloud providers specific environments, in order to offer a measure of the provider itself instead of addressing the cloud service in the consumer context.

REFERENCES

[1] Wim Van Grembergen and Steven De Haes , Business Strategy and Applications in Enterprise IT Governance, 2012, IGI Global ISBN:9781466617797

[2] Wim Van Grembergen, Steven De Haes, Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value, 2008 , Springer ISBN:9780387848815

[3] Cloud Security Alliance, Security Guidance for critical areas of focus in cloud computing v3.0, 2011 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[4] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012, ISACA ISBN:9781604202373

[5] ISACA, Enterprise Value: Governance of IT Investments: The Val IT Framework 2.0, 2008 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx , ISACA ISBN:9781604200669

[6] ISACA, Monitoring Internal Control Systems and IT: A Primer for Business Executives, Managers and Auditors on How to Embrace and Advance Best Practices, 2010, ISACA ISBN:9781604201109

[7] ISACA, Business Continuity Management Audit/Assurance Program, 2011, ISACA ISBN:9781604201864

[8] ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011, ISACA ISBN:9781604201826

[9] A. L. Holt, Governance of IT: An Executive Guide to ISO/IEC 38500, 2013,BCS,ISBN:9781780171548

[10] Chris Davis, Mike Schiller, Kevin Wheeler, IT Auditing: Using Controls to Protect Information Assets, Second Edition, 2011 McGraw-Hill/Osborne ISBN:9780071742382

[11] Ben Halpert, Auditing Cloud Computing: A Security and Privacy Guide, 2011, John Wiley & Sons ISBN:9780470874745

[12] Brian J.S. Chee, Curtis Franklin, Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center, 2010, Auerbach Publications ISBN:978143980612

[13] Kurt J. Engemann and Douglas M. Henderson, Business Continuity and Risk Management: Essentials of Organizational Resilience, 2012, Rothstein Associates ISBN:9781931332545

[14] Robert R. Moeller, COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition, 2011, John Wiley & Sons ISBN:9780470912881

[15] Jatinder N. D. Gupta, Sushil K. Sharma, Handbook of Research on Information Security and Assurance, 2009, IGI Global, ISBN:9781599048550

[16] Charles Babcock, Management Strategies for the Cloud Revolution: How Cloud Computing Is Transforming Business and Why You Can't Afford to Be Left Behind, 2010, MgGraw-Hill ISBN:9780071740753

[17] Perhuru Raj, Cloud Enterprise Architecture, 2012, Auerbach Publications ISBN:9781466502321

[18] Lee Newcombe, Securing Cloud Services: A Pragmatic Approach to Security Architecture in the Cloud, 2012, IT Governance ISBN:9781849283960

[19] Alberto M. Bento, Anil K Aggarwal Cloud Computing Service and Deployment Models: Layers and Management, 2013, IGI Global ISBN:9781466621879

[20] Tim Mather, Subra Kumaraswany, Shahed Latif, Cloud Security and Privacy. An Enterprise Perspective on Risk and Compliance, O'Reilly United States of America, first version2009.