Enterprise Transformation Projects-Cloud Transformation Concept Holistic Security Integration (CTC-HSI)

ANTOINE TRAD
IBISTM
Courbevoie
FRANCE

Abstract: This chapter presents the fundaments of the Cloud Transformation Concept (CTC) and this concept is a basic component of the author's transformation framework and in complex transformation projects, where a holistic security concept is a top priority. The implementation of CTC's Holistic Security Integration (CTC-HSI) is supported by the author's Applied Holistic Mathematical Model (AHMM) for CTC (AHMM4CTC) and his various research works on Holistic Security Integration (HSI), Business Process Management (BPM), Artificial Intelligence (AI), AI Services (AIS), Compute Services (CS), Mathematical Models, cross-functional transformations projects. The AHMM4CTC is based on cross-functional research on an authentic and proprietary mixed research method supported by his own version of an AI learning model, a search tree, combined with an internal heuristic algorithm. In this chapter, the focus is on CTC-HSI's integration concepts, requirements, services, data management, and corresponding transformation security strategies. The proposed AHMM4CTC-based CTC-HSI is a concept for secured environments, which use real-life cases of a transformation project, which needs scalable and secured Cloud Platform's (CP) infrastructure and services layer, that are supported by the alignment of CP services, standards, enterprise architecture paradigm, and security development strategies. In a CP-based transformation project, the author recommends integrating a Private CP (PCP); which can use commercial CPs like the Google CP (GCP). The GCP was chosen as a sample CP, but there is a need to define a standardized security architecture and concept/procedures so that the organization builds its own CTC-HSI-based PCP and has to avoid locked-in commercial products.

Key-Words: Cloud Security, HSI, Enterprise architecture, Artificial Intelligence, Mathematical Models, Strategic and Critical Business Systems, Business transformation projects, CSFs/areas, Performance Indicators, and Strategic Vision.

Received: February 7, 2022. Revised: October 27, 2022. Accepted: December 5, 2022. Published: December 30, 2022.

1 Introduction

The CTC-HSI is based on resources related to CP domains like services, processes, AI, CSs, and CP's infrastructure, to offer a set of CTC-HSI recommendations, which can be applied to build a PCP-based transformation. CTC-HIS's strategy is a generic CP security-driven approach that uses various security concepts, including Enterprise Architecture (EA), AI, Distributed or Cloud Computing Architecture (CCA), and BPM. This chapter uses the GCP to demonstrate CTC-HIS's capability to offer different types of generic, business, and Information and Communication Systems (ICS) security concepts. Security-related resources need different levels of provisioning, that depend on the used CP and the underlined ICS services. This chapter's background combines CTC-HSI, CP security (and various security domains), AI, Machine Learning (ML), Secure Development and Operations for CTC (DevSecOps4CTC) strategy, Knowledge Management System for CTC (KMS4CTC), EA, heuristics/mathematical models, secure ICS management, and cohesive business transformation technics. The CTC-HSI is a generic and cross-business concept that interacts with a learning process (AI/ML) that manages sets of Critical Success Factors (CSF) that can be used by a transformation project (or simply the Project). This chapter's experiment uses an insurance case, [1], and GCP Use Cases (UC); where the experiment is based on many years of Research and Development Projects adapted for CTC (RDP4CTC).

2 Research Process and Problem Formulation

The CTC-HSI is business driven and is agnostic to any Applied Problem Domain (APD) and is founded on the author's genuine research framework that in turn is based on many existing standards, like the Architecture Development Method for CTC (ADM4CTC), [2], [3], and the Sherwood Applied Business Security Architecture (SABSA), which can be coupled with The Open Group's Architecture Framework's (TOGAF) major components. The Business Transformation Manager, CP architect, or enterprise architect (or simply the Manager) can

integrate the CTC-HSI in the enterprise's (simply the Entity) EA's roadmap, where the CTC-HSI must deliver the path for integrating security components in the ADM4CTC. The RDP4CTC is based on: Literature Review Process for CTC (LRP4CTC), a Qualitative Analysis for CTC (QLA4CTC) methodology, and the experiment or the Proof of Concept (PoC), that is used to solve the Research Question (RQ), in which the management of processes has a crucial and his decisions are aided by using the Decision-Making System (DMS for CTC (DMS4CTC), [4]. Many CSFs influence CTC-HSI's integration, like 1) CP/ICS' interface mechanisms; 2) Managing Project security and other types of risks; 3) Entity resources mapping to CTC-HSI requirements and mechanisms; 4) CTC-HSI related skills; 5) PCP security, infrastructure and requirements support; 6) PCP security tests capacities; and 7) PCP security monitoring and control. The author's research project's keywords were introduced in the scholar engine (in Google's search) and the results clearly show the uniqueness and the absolute lead of the author's methodology, research, and works. Due to this fact, the author considers his works in the mentioned fields as successful and useful. The CTC-HIS-based PCP is optimal because it synchronizes Entity's processes, tasks, actions, and resources; and that is the chapter's main focus. CP based EA methods, like TOGAF and its adapted ADM4CTC, support the needed for an CTC-HSI. Actual PCP security technics focus on the Entity's isolated security tools, services, processes, and CSs. Minimal modelling technics are needed for the CTC-HSI which used standard ICS security frameworks to align with other CPs, ADM4CTC, and secured atomic Building Blocks (saBB). This chapter also illustrates how Projects can benefit from using the CTC-HSI and proposes an adequate RDP4CTC. The TDP4CTC RQ is: "Which PCP characteristics and support is needed for in the implementation of an Entity CTC-HSI?". Where the kernel of this research is based on the Heuristics Decision Tree (HDT), AI/ML and CSFs (and areas). A Critical Success Area (CSA) is a category (or set) of CSFs where in turn a CSF is a set of Key Performance Indicators (KPI), where a KPI maps (or corresponds) to a single CTC-HSI requirement. For a given CTC-HSI requirement or problem, the Project identifies sets of CSAs, CSFs and KPIs, to be used by the DMS4CTC and to be mapped to PCP's artefacts. Hence the CSFs are important for the mapping between CTC-HSI requirements, resources, and DMS4CTC, [41]. Therefore, CSFs reflect CSAs that must meet the Project's goals and constraints. Measurements technics, which are provided by the Transformation, Research, Architecture, and development framework (TRADf), are used to evaluate performance in each CSA, where CSFs can be internal or external. Once the initial sets of CSFs and CSAs have been identified, then the Project can use the DMS4CTC to deliver solutions for CTC-HSI problems. The CSF-based RDP4CTC uses the AI/ML/HDT based DMS4CTC, where in RDP4CTC's phase 1 (represented in automated tables), which form the empirical part of the RDP4CTC, checks eight CSAs and tables The tables' decision concept was influenced by the Object Management Group's (OMG) Decision Model and Notation (DMN), where DMN can be used for specification of business decisions and business rules. DMN is optimal for different engineer's profiles involved in decision management, [5]. The CTC-HSI delivers recommendations on how to align Project's CP resources by using TRADf.

2.1 The Framework-TRADf and the Empirical Engineering Research Model

This and other authors' research works are based on a polymathic model, which is a very complex approach. And it is recommended to refer to the *Using Applied Mathematical Models for Business Transformation,* [57]; to understand his approach. The CTC-HSI alignment strategies manage the Entity's PCP security, resources and Microartefacts' which used various types of technologies. The CTC-HSI is complex and is a risky approach because 1) The complexity of PCP's security and risks management; 2) Various security types and levels; 3) CTC-HSI synchronization for all processes and resources; 4) Mapping mechanisms; and 5) Implementation of security in existing PCP and ICS components. A system's approach, like TRADf's, is recommended for CTC-HSI-based Projects [6]. The CTC-HSI is generic and can be applied to any standard, public, or PCP. This chapter is a part of many years' research cluster that has produced a large set of articles and TRADf, and parts of previous works are reused for a better understanding of this complex iterative research. If all facts are only referenced, it would have been tedious to understand this RDP4CTC which is based on an Empirical Engineering Research Model (EERM), [2], [3], [7]. The EERM is optimal for engineering projects and it uses an authentic mixed method that is a natural complement to Quantitative Analysis for CTC (QNA4CTC) and QLA4CTC research methods, to deliver empirical concepts as a possible

holistic approach for mixed methods; in fact, both methods are compatible and the difference is the scope and depth of the research process. EERM's validity checks if the RDP4CTC is acceptable as a contribution to existing scientific (and engineering) knowledge. The author wants to convince the valuable reader(s) the proposed recommendations and the related PoC, are valid and applicable. In engineering, a PoC is a design and software prototype of a testable RQ (and hypothesis) where one or more CSFs (or independent variables, in theoretical research) are processed to evaluate their influence on the EERM's dependent variables. The PoC permits to evaluate precision of the CSFs and if they are related, whether the cause–effect relationship exists between these CSFs and CSAs. The CTC-HSI uses EA, AI/ML, and ICS standards, [2]. This EERM is based on the author's major related works.

2.2 Major Related Works

CTC-HSI's main topics include: 1) The use of secured CP resources like BPMs, CSs, Virtual Machines (VM), Compute Engines (CE), App Engine, (AE) Standard (AES), AE Flexible (AEF), Kubernetes Engine (KE)/clusters…; 2) Secure interaction with external CPs and ICSs; 3) The use of secured components with Infrastructure-as-Code (IaC); 4) The use of secure services architecture; 5) security Risks (sRisk) management; 6) Basic security; 7) Complex PCP domains to be secured; and 8) Existing CP security concepts. CTC-HSI can be used with existing products, like GCP's Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) concepts and their core functionalities. CTC-HSI aspects when designing the secure PCP components are based on managing states in distributed systems' interactions, data flows, and monitoring and alerting, [8]. Besides the use of standard artefacts this chapter uses the author's major related works:

- *Projects* in the financial industry and ethics [9]: It analyses global financial, societal, and geopolitical security and crisis, which can be analysed by *TRADf*. *TRADf* identifies recurrent patterns of organized global financial misdeed models and related crimes. The CTC-HSI uses measurable CSFs and CSAs which characterize the evaluation of risk factors related to Global Predators' Misdeeds (GPM). Such GPMs are in general ranked as the most ethical organizations because such ranking organizations are chosen by GPM-related circles; here the main limitation is the ongoing ethical and regulatory organizations are corrupt. The CTC-HSI is aimed mainly to support the proactive detection of financial irregularities, locked-in traps, and major security and hence financial crimes, which can be fatal for an *Entity*. Some of the major states and financial powers are responsible for most GPM crimes, and they even enjoy excellent world-class reputations. In this article, various cases are mentioned because they are related to known financial centres, that enjoy a top worldwide position in transparency and ethical rankings, [10], [11], and who at the same time have committed major security/financial irregularities and crimes. The main reason for this global contradiction is that they have overwhelming legal, political, and financial advisory support, which blocks any attempt to divulge such unethical behaviour. Financial motives are the main reasons for security breaches and financial crimes.
- BUSINESS ARCHITETCURE AND TRANSFORMATION PROJECTS-ENTERPRISE HOLISITIC SECURITY RISK MANAGEMENT [12]: It presents a strategy that identifies and assesses possible CP and ICS security problems that can damage the *Entity's* assets and. *Entities* are using Cybertechnologies to become full *Entities*. *Entities*, face challenges, dangers and sRisks, when implementing their PCP. One of the most important sRisks is the stability of an *Entity* in an unsafe ecosystem. Cybersecurity is a major part of an *Entity's* EA roadmap. *Projects* have many tangible advantages and unfortunately have also many sRisks. These sRisks are related to data, assets and resources platform security, but there is a whole set of other types of CPs/ICSs and APDs sRisks. *Entities* are sensitive to Cyberattacks, depending on the volume of transactions, data management and the applied security concept. To identify security breaches like, data leaking, the CTC-HSI supports a systematic approach to CP's resources protection that includes classical and Cybersecurity mechanisms. Cybersecurity is essential for ensuring the *Entity*'s sensitive information, and resources protection from the use of personal information that can be

leaked and can be used by hackers. *Entities* are facing excessive requests to optimize their assets and minimize sRisks, to guarantee sustainability, optimize costs, support frequent transformation initiatives and to integrate legal, security and governance frameworks. sRisks may include CSFs related to reputation, routine operational procedures, legal and human resources management, financial, the risk of failure of internal controls systems related to the Sarbanes-Oxley Act (SOX) and global governance. A *Project* integrates various objects, like CTC-HSI managers and/or the creation of a department for risk management supported by a quality control team. Possible CTC-HSI risks are: 1) Hazard risks, which include risks that present a high level of threat to life, health or property; 2) Financial risks, which refer to risks that are directly related to money; 3) Strategic risks are risks that affect or are created by strategic decisions; 4) Operational and security risks are risks that influence the *Entity*; 5) CTC-HSI main fields and background.

- The *Entity* Transformation Projects: In the APDs related to military technology strategies, [13], conflicts, wars, and military investments are the backbone for major global economies' evolution, stagnation, or failure. *Entities* drive major technological transformation and innovation trends. Transformed *Entities*, have to face new challenges and geopolitical sRisks. One of the most important sRisks is related to finding the right balance between, military technology, military strategy, financial capabilities, security concepts, geopolitical knowledge, the status of combativity and the evolution of demography. Therefore, the stability of an *Entity*, depends on a holistic strategy to support the *Entity*'s transformation projects. The CTC-HSI includes a methodology and a concept to manage the *Entity*'s geological stability and tries to detect the main sRisk, which is that an *Entity* may lose the sense of reality, by thinking that only CTC-HSI and financial investments will solve all types of military conflict.
- *Entity* Transformation Projects: Security Management Concept, [14]: One of the most important sRisk is mainly based on the internet and its various services. Therefore, the security of an *Entity* must be a CTC-HSI to manage Cybersecurity. Cybersecurity is employed in the *Entity*'s EA processes. *Entity*'s PCP enables the processing of large groups of applications and their related data storages with optimal performance and sometimes in hyper-time, in order to serve clients and executive management, who are supported by a DMS4CTC, where CP's evolutions have enabled the transformation of legacy mainframe systems where most of the *Entity*'s transactions and data storages are found, [15].
- The Role of Cyber and Information Technology Security in Automated Business Environments: Proposes CTC-HSI procedures, to support automation pattern for secured transformation processes. Security controls for an *Entity* are a set of interrelated activities from various domains like security architecture, financial engineering, geopolitical influence, governance and legal conformance. All that can be used to avoid financial crimes, business disruptions and corruption. Complex transformation initiatives must be coherent with the *Entity*'s ethics, business, and security strategic planning goals, where the main strategic goal is to minimize the various types of financial criminal acts. Security controls are the fuel of the *Entity*'s sustainable business growth and its integration in global economies. Security control schemes can be supported by security and risk frameworks, standards, and legal controls that are necessary for the company's business strategy that is based on a Cybersecurity background.

2.3 RDP4CTC's CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 1. This chapter also related to author's works related CP topics, like: CTC-CS, CTC-AI, CTC-BPM…, which support ICS' interaction with the PCP.

Table 1. CSFs have an average of rounded 9.25.

3 ICS' AND PCP'S INTERACTION

3.1 ICS and CP Basics Interactions

ICS' evolution has enabled CTC-HSI to support PCPs, where the integration of various types of security challenges supports *the Entity's* business robustness, longevity, and sustainability. The CTC-HSI manages distributed security in complex APDs, which are used to improve the *Entity*'s Time To Market (TTM) activities. The CTC-HSI supports *Projects*, by applying the PCP, to synchronize and secure all its activities. The main problem for *Projects* is to unbundle their legacy ICS and use a secure PCP. A PCP is based on sharing of secured resources to support business coherence and uses the *pay-as-you-go* business model; such a model reduces capital expenses but can also generate unexpected operating expenses. A PCP includes a group of networked components providing services, which do not need to be individually located. The CTC-HSI provides a secure management environment for PCP components, which can be designed internally to support complex APD operations, [16]. The PCP enables the processing of its secured activities, which include a large set of applications and resources. The DMS4CTC and CTC-HSI support the *Entity*'s business capabilities to operate in various APDs. The CTC-HSI uses some central domains, like security & governance frameworks, EA, CP, and services coordination. This RDP4CTC will offer a set of recommendations to support the PCP's evolution. *Entities* have built their PCP or accelerated their use of CP providers, to become secure, and agile and the main differences between CP providers need strategic *Project's* HSI capacities. Where in the case of public CP's IaaS can offer Application Programming Interface (API) based services, [17]. … To support Business Transformation *R*eadiness (BTR).

3.2 The BTR

The CTC-HSI supports and secures all Project tasks, including the tools usage, processes, and PCP's management. Important advances are made in CPs' secured processes, discipline, skills, and methodologies to enhance Enterprise Capacity to Execute, which improves the Entity's ability to perform all the tasks including secure DMS4CTC operations in time constraints. PCP's security is important, and the Project defines how to design and implement CTC-HSI concepts. Today there are many security standards and they are applicable and help in the unbundling of legacy ICSs. An important CSF for Projects is to use saBBs based CTC-HSI strategy, [2]; where such a saBBs-based CTC-HSI must respect standards. Entity activities are achieved by combining various synchronized CSs to promote process automation. There are no precise recommendations for such a saBB-based CTC-HSI strategy, but there are some technics related to organizational processes, services, and PCP controls.

3.2 Main Components and Artefacts

The main ICS-related security activities are related to 1) Managing Passwords; 2) Firewalls; 3) DevSecOps; 4) Antivirus, Viruses, and Worms; 5) Emails; 6) Wireless Fidelity; 7) Malware; 8) Business rules for the handling of data/information assets; 9) Defined security policies; 10) Codified data/information assets' ownership and custody; 11) sRisk analysis documentation, and 5) Data classification policy documentation. The CTC-HSI manages the normal flow of ICS applications' fallout, abnormal flows, failure modes, and the possibilities in which the ICS and applications can be interrupted or attacked. All Entities have security concerns and they should dedicate a security architect to support the Entity's transformation process. In all ADM4CTC phases, recommendations are given on security-specific management. CTC-HSI decisions are traceable to business and policy decisions and their sRisk management. The areas of concern for the CTC-HSI are, [2], [9]:

- Authentication: The substantiation of the id Entity's secured environment.

- Authorization: The definition and enforcement of permitted capabilities for a person whose Identity has been established.
- confirming that the ICS has been used in accordance with CTC-HSI policies.
- Assurance: The ability to test the EA and its security attributes, which are required to support security policies.
- Availability: The Entity's ability to function without service interruption despite malicious events.
- Asset Protection: The protection of information and assets from loss and resources from unauthorized and unintended use.
- Administration: The ability to add and change security policies and to add or change the persons related to the ICS.
- sRisk Management: The Entity's attitude and tolerance for sRisks.

3.2 ICS's CSFs

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_ICS_PCP_Bases	Proven	From 1 to 10. **10 Selected**
CSF_ICS_Standards	Proven	From 1 to 10. **10 Selected**
CSF_ICS_saBBs	Complex	From 1 to 10. **08 Selected**
CSF_ICS_BTR	Possible	From 1 to 10. **09 Selected**
CSF_ICS_DevSecOps4CTC	Complex	From 1 to 10. **08 Selected**
CSF_ICS_CTC_HSI	Complex	From 1 to 10. **08 Selected**
CSF_ICS_ADM4CTC_Artefacts_Automation	Proven	From 1 to 10. **10 Selected**

valuation

Table 2. CSFs that have a rounded average of 9.0.

Based on the LRP4CTC, the most important CSFs are presented in Table 2.

4 EA AND CTC-HSI'S INTEGRATION

4.1 EA based PCP

The use of EA support for the CTC-HSI is crucial because of the following facts:

- ADM4CTC secures applications, [12]: This ADM4CTC supports Projects' integration and presents the influence of an CTC-HSI to support the Project. The CTC-HSI focuses on the design of security controls' integration for the PCP; so the security capabilities protect the Entity from attack by: 1) Localizing gaps in the infrastructures of partners; 2) Review of detection, and real-time security solutions; 3) Block cumulative attacks; 4) Defining a security strategy to locate potential weaknesses; 5) Build a robust defense; 6) Integrate security in transactions; 6) GPM attacks; and 8) Apply qualification procedures in the ADM4CTC, [24]. Without the use of the ADM4CTC based CTC-HSI, the PCP can: 1) Become siloed and have poor performance; 2) Lack scalability; 3) Fail, become un-usable and un-maintainable; 4) Fail in producing successful CTC-HSI functionalities. The CTC-HSI interfaces various market risk frameworks like the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is shown in Fig. 1.
- The Architecture Standards and the CTC-HSI: Legacy architecture layers represent a silo model where it is very hard to transform to a PCP. Moving to a standardized CP is the first step to a basic CTC-HSI. Using the CTC-HSI, the Project can transform the ICS into a dynamic and secured PCP, [2].

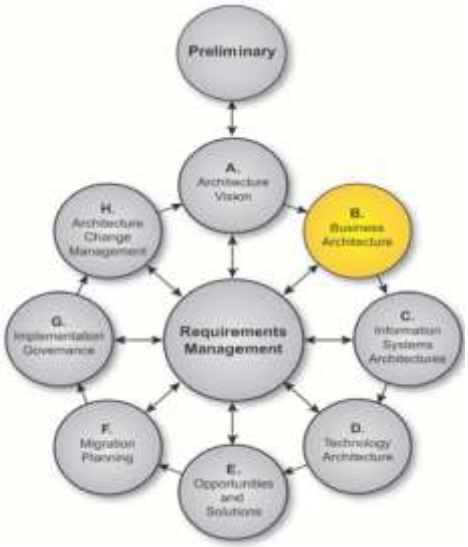

Fig 1. TOGAF' phases [2].

- ADM4CTC's integration with the CTC-HSI, enables the automation of the Project's secured processes, saBBs, Microartefacts, throughout its phases. The ADM4CTC encloses cyclic iterations, where information about all PCP operations. The ADM4CTC offers the management, control and monitoring of Project's Microartefacts' by using various types of tests and

integration concepts like: 1) Test Driven Developments (TDD); 2) The Acceptance Test Driven Development (ATDD); 3) Business process testing; 4) The Behavior-Driven Development (BDD) concept includes TDD, integration and ATDD; and 5) CP security testing uses different approaches like: Black box, Gray box, or White box. Where PCP's application cartography is essential.

4.2 Designing a Generic CTC-HSI based PCP for Various APDs

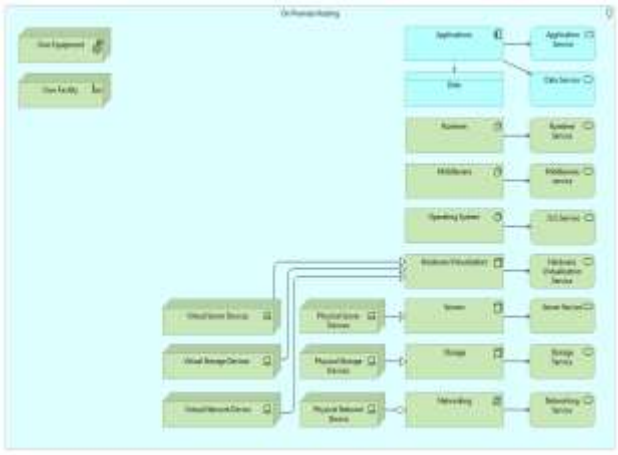

Fig. 2. On-Premises Hosting Model, [21].

The CTC-HSI-based PCP is designed as a set of hosted secured CP models by using EA and the *On Premises Hosting Model*, as shown in Fig. 2, where the *Entity* is responsible for its PCP and installed secured components, [21]. *The IaaS Hosting Model* represents hosting in both *On Premise* and in the *Cloud*, where the *Entity* manages its EA-based PCP and all its components like CSs and Operating Systems (OS). EA's support is needed to transform *Entity's* fragmented legacy components into secured and agile components in PCP's context and that in turn supports the defined *Project* strategy and the refinement of PCP's applications' cartography. EA modelling languages like Archimate can be used for CP's applications classification by using the Application Communication Diagram (ACD), to depict all used CP's applications, [50]. The use of an EA-based CTC-HSI concept is crucial because of the following reasons, [13]: 1) In delicate domains like defense and military, *Entities* are using technologies and methodologies as the kernel of their defense strategies, like the case of EA in the form of DoDAF, [26]; 2) In the actual age of secured CPs & ICSs, security issues, fast changes, AI, complexity, and technology, the EA based CTC-HSI becomes the *Entity's* major *Project* and security objective; 3) The CTC-HSI defines security capabilities to protect the *Entity* from attacks by: Localizing gaps in the CP's infrastructures, Review of detection and real-time security solutions, Block cumulative attacks, Defining a CTC-HSI to locate potential weaknesses, Build a robust EA based CTC-HSI; Integrate security mechanisms in all PCP components, Block GPM attacks, Apply qualification procedures in the ADM4CTC [24]. PCP security is different for different *Entities* and depends on various CSFs, but the National Institute of Standards and Technology (NIST) made a list of best practices that can influence the CTC-HSI. The NIST has created the necessary steps for an *Entity* to self-assess its PCP security preparedness and to apply adequate security measures. These principles are built on the NIST's five pillars of a cybersecurity framework: Identify, Protect, Detect, Respond, and Recover. Another framework is the Cloud Security Posture Management (CSPM) which is designed to address common CP flaws, [28]. Use security frameworks, like SABSA to interface EA-based CTC-HSI, to provide common ADM4CTC interfaces.

4.3 CTC-HSI and the ADM4CTC

Fig. 3. Integration of SABSA with TOGAF [33].

The EA-based CTC-HSI is based on EA methodology, which facilitates SABSA's integration; where the ADM4CTC supports the following characteristics, [33]: 1) sRisk management that uses CSFs for the selection of CTC-HSI's measures. SABSA's approach to operational sRisk management is the domain or business-driven rather than threat-driven, which is a purely technical approach; 2) During EA's

requirements management phase, CTC-HSI models are delivered; 3) The ADM4CTC, as shown in Fig. 3 delivers secured Microartefacts; 4) *TRADf* englobes the ADM4CTC; and 5) facilitates the use of the DMS4CTC and KMS4CTC.

4.4 The ADM4CTC and the CTC-HSI CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 3.

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_ADM4CTC_CP_Standards	Feasible	From 1 to 10, **09 Selected**
CSF_ADM4CTC_PCP_Interfacing	Complex	From 1 to 10, **08 Selected**
CSF_ADM4CTC_ACD_Integration	Feasible	From 1 to 10, **09 Selected**
CSF_ADM4CTC_HSI_Integration_Requirements	Complex	From 1 to 10, **08 Selected**
CSF_ADM4CTC_HSI-Standards_SABSA	Possible	From 1 to 10, **09 Selected**

valuation

Table 3. CSFs have an average of 8.60.

5 THE DMS4CTC AND KMS4CTC USAGE

5.1 CTC-HSI's Risk Assessment

Fig. 5. GCP's AI capacity, [29].

CTC-HSI's Risk Readiness Assessment and the CTC-HSI has the following characteristics, [2]: 1) It integrates TOGAF's *BTR Assessment* that supports the *Capacity to Execute* all PCP's secured processes; 2) Includes the *Enterprise Capacity to Execute* the tasks needed for the *Project*; 3) Its assessment process checks CTC-HSI's readiness to implement defined CTC-HSI's requirements; 4) To assess sRisks for each readiness CSF and identifies improvements of secured processes and actions to mitigate these sRisks; 5) Integrates *BTRs and Mitigation Activities*; 5) Relates CSFs and *Risks Estimations* by an AI/ML process, [56]. CTC-HSI can use AI Engine (HSIAIE), which is a suite of services used to integrate AI/ML models as shown in Fig. 5, these services are available for the following AI/ML operations, [29]: Prepare, Build, Validate, and Deploy. sRisks continuous evaluation is supported by implemented models and provides a continual return on PCP's security status.

5.2 Using an AHMM4CTC Instance

Basic Mathematical Model's (MM) Nomenclature

Iteration	= An integer variable "I" that denotes a *Project/ADM iteration*	
microRequirement	= (maps to) KPI	(1)
CSF	= Σ KPI	(2)
Requirement	= (maps to) CSF = $\bigcup$ microRequirement	(3)
CSA	= Σ CSF	(4)
microMapping microArtefact/Req	= microArtefact + (maps to) microRequirement	(5)
microKnowledgeArtefact	= $\bigcup$ knowledgeItem(s)	(6)
neuron	= action->data + microKnowledgeArtefact	(7)
microArtefact / neural network	= $\bigcup$ neurons	(8)
microArtefactScenario	= $\bigcup$ microartefact	(9)
AI/Decision Making	= $\bigcup$ microArtefactScenario	(10)
microEntity	= $\bigcup$ microArtefact	(11)
Entity or Enterprise	= $\bigcup$ microEntity	(12)
EntityIntelligence	= $\bigcup$ AI/Decision Making	(13)
BMM(*Iteration*) as an instance	= EntityIntelligence(*Iteration*)	(14)

Fig. 6. The AHMM4CTC nomenclature.

The AHMM4CTC that is presented in Fig. 6, is easily understandable on the cost of a holistic formulation of the CTC-HSI, which uses the AHMM4CTC as a formalized structure. As shown in Fig. 7, the symbol $\sum$ indicates the summation of all the relevant named set members, while the indices and the set cardinality have been omitted. The summation should be understood in a broader sense, more like set unions. The *Project*'s development and mapping processes are a part of the CTC-HSI which uses the DMS4CTC. The DMS4CTC, as shown in Fig. 7, is based on a light version of the ADM4CTC.

The Generic AHMM's Formulation

AHMM	= $\bigcup$ ADMs + BMMs	(15)

AHMM's Application and Instantiation for CTC (HSI)

Domain	= CTC	(16)
AHMM4(*Domain*)	= $\bigcup$ ADMs + BMMs(*Domain*)	(17)

Fig. 7. The AHMM for a domain.

The enterprise AHMM4CTC is the combination of an EA and Project methodologies. A Project (or a transformation) is the combination of an EA methodology like the TOGAF and the AHMM for a Domain (which in this case/chapter is the CTC-HSI), that can be modelled after the following formula for the CTC based Transformational Model (CTC-HSI-TM):

CTC-HSI-TM = EA + AHMM4CTC (18)

5.3 KMS4CTC's and DMS4CTC's CSFs

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_KMS&DMS4CTC_AHMM4CTC_Support	Possible	From 1 to 10: 09 Selected
CSF_KMS&DMS4CTC_Secured_Microartefacts	Complex	From 1 to 10: 08 Selected
CSF_KMS&DMS4CTC_AI_Support	Complex	From 1 to 10: 08 Selected
CSF_KMS&DMS4CTC_sRiskAssessment	Possible	From 1 to 10: 09 Selected
CSF_KMS&DMS4CTC_ComplexSystems_Design	Complex	From 1 to 10: 08 Selected

valuation

Table 4. CSFs that have an average of 8.40.

Based on the LRP4CTC, the most important CSFs are presented in Table 4 and can be used for CTC-HSI's sRisk Management.

6 CTC-HSI SRISKS MANAGEMENT

6.1 CTC-HSI'S Concept

Fig. 8. CTC-HSI's sRisk management concept [20].

This chapter proposes an alignment between the CTC-HSI, DMS4CTC, ICS, governance, and EA activities. Supporting an overall CTC-HSI for an Entity, Fig. 8 shows the main concept. Governance processes ensure control when moving from strategic planning to operative implementation activities and this demands guidance and transparency that is supported by the ADM4CTC. EA is used to discover deficiencies, and show complex and risky interactions between strategies, global processes, services, and infrastructure, providing a base for complex sRisk analysis. The concept proposes an integrated view of governance, CTC-HSI, and EA to support an Entity to be efficient and reliable. This enables the DMS4CTC to control sRisks optimally. Entities are modelled using EA which uses Microartefacts like data models, business models, strategy models, platform plans, and organizational structure…, [20].

6.2 The PCP, sRisk Management, and Frameworks

The CTC-HSI asses and governs PCP resources by using the CTC-HSI; and a global management concept of assets is optimal for the *Project*. The CTC-HSI is managed by ADM4CTC's phases, where each secured Microartefact circulates through its phases. *TRADf* interfaces various market sRisk frameworks, like COSO, which is shown in Fig. 9. The COSO framework defines basic important components, proposes a common language, and offers a roadmap for sRisks' management. Where CTC-HSI's objectives can have the following CSAs: 1) Strategic; 2) Operations; 3) Reporting; and 4) Compliance. And the following key CSFs: 1) Organizational design of business; 2) Establishing a CTC-HSI organization; 3) Performing sRisk assessment; 4) Determining overall sRisk possibilities; 5) Identifying sRisk responses; 6) Communication of sRisk results; and 7) Monitoring, [31].

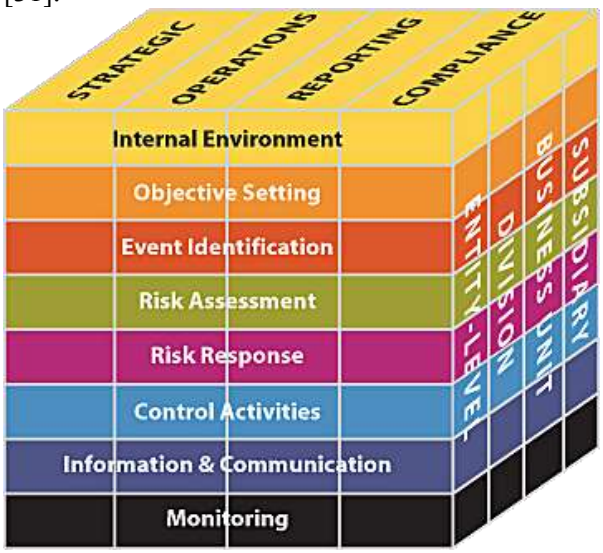

Fig. 9. The COSO framework, [31].

Accountant-oriented sRisks management promotes off-shoring and ruthless growth, which can have a negative effect on Projects, because they promote erroneous conclusions. Transformed Entities with an efficient CTC-HSI, automates sRisks' management, by using efficient security mechanisms which are in turn supported by the ADM4CTC. sRisks are, in most cases, difficult to discover and classify, due to their diversity and complexity. sRisks' neutralization is a technical, financial, and mathematical process based on the DMS4CTC. The CTC-HSI structures sRisks by using CSAs, weights them, and uses delimiters to select the related CSFs. The CTC-HSI analysis the CSAs by applying scenarios for mitigation. CTC-HSI system's key principles are: 1) the Principle of integration using a systemic and holistic approach; 2) the Principle of continuity using a set of procedures; and 3) the Principle of validity, which provides an analysis of the ratio of costs to reduce possible sRisks, [34].

6.3 CTC-HSI's sRisk Processes

Fig. 10. sRisk architecture, strategy, and protocols, [18].

CTC-HSI's sRisk processes are a set of coordinated activities, as shown in Fig. 10; which contain the descriptions of these processes and where sets represent the 7Rs and 4Ts of sRisks to be managed: 1) Recognition or the identification of risks; 2) Ranking or the evaluation of risks; 3) Responding to significant risks; 4) Tolerate; 5) Treat; 6) Transfer; 8) Terminate; 9) Resourcing controls; 10) Reaction planning; 11) Reporting and monitoring of risk performances; and 12) Reviewing risk management frameworks, [18]. Using CTC-HSI to discover sRisk aspects mitigation measures and is supported by an evaluation of the impact of sRisks using EA, DMS4CTC and KMS4CTC. This approach, starts in the *Project's* multiple points in ADM4CTC, where a phase includes the following actions: 1) To assess sRisks that cover discovered risk types, like Cyberattacks, technology, business-related risks; 2) To define CTC-HSI control measures, using a combination of sRisks and control measures; 3) To implement control procedures to control sRisks. EA based CTC-HSI is a step where the *Project* shifts from a simple design to a secure one; 4) To execute and monitor the implemented control procedures; 5) To analyze the vulnerabilities, monitoring delivers insights on the effectiveness of implemented controls, like, pen-testing. This activity determines which vulnerabilities (or CSFs) are dangerous and the link is implemented between the vulnerabilities and identified sRisks, by using EA-based CTC-HSI models; 6) To identify external and internal sRisks; and 7) Define governance procedures, [35], Trad, 2022a).

6.4 CTC-HSI's Governance

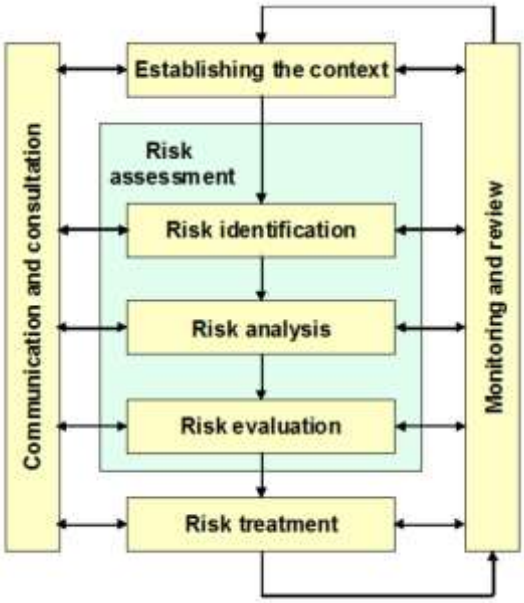

Fig. 11. sRisk management process [20].

6.5 Risk Response Strategies for Enterprise Asset Risk Management

Projects' Managers, select the optimal CTC-HSI strategies and are the following types: 1) Risk avoidance; 2) Risk reduction, where mitigation of the severity of losses; 3) Alternative actions to offer possible actions to reduce risks; 4) Share the actions of transferring risks to third parties; and 5) Risk acceptance, is the willingness to accept their consequences. CTC-HSI critical capabilities include, [42]: 1) sRisk analysis; 2) sRisk remediation; 3) Compliance content mapping; 4) Workflow design; 5) User experience; 5) Board and

senior executive reporting; 6) Basic and advanced integrations; 7) Digital asset discovery; and 8) Near-real-time assessment. Fig. 12, shows the major trends concerning CTC-HSI, which has to apprehend the levels of possible damages.

Fig. 12. The magic quadrant for sRisk management, [42].

6.6 The Levels of Possible Damage

The levels of security damages are immense and USA's Federal Bureau of Investigation (FBI) estimated that attacks caused 1.7 billion United States Dollars (USD) in damage; therefore *Entities* are dependent on CSI/CP technologies like: 1) Direct internet; 2) Communication (Email…); 3) Commerce (e-commerce and other); 4) Control and management systems; 5) Information and entertainment services; 6) PCP's sensitive data; 7) PCP's usage of transactions; 8) EA based CTC-HSI policies; and 9) Internet of Things (IoT) domains, like .com, with having replaced legacy domains. The scale of security damages is immense because related GPM misdeeds, which is the main motive, are never condemned and huge amounts of money and assets are hidden, [44], [12]. *Project's* first iteration must transform basic security concerns.

6.7 CTC-HSI's sRisks' Management CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 5, and can be used for CTC-HSI's sRisk Management.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_sRisksManagement_Concept_Frameworks	Complex	From 1 to 10. **08 Selected**
CSF_sRisksManagement_Processes	Possible	From 1 to 10. **09 Selected**
CSF_sRisksManagement_Governance	Complex	From 1 to 10. **08 Selected**
CSF_sRisksManagement_Strategies	Complex	From 1 to 10. **08 Selected**
CSF_sRisksManagement_Damages	Complex	From 1 to 10. **08 Selected**

valuation

Table 5. CSFs that have an average of 8.20.

7 CTC-HSI BASIC SECURITY

7.1 Fundamentals

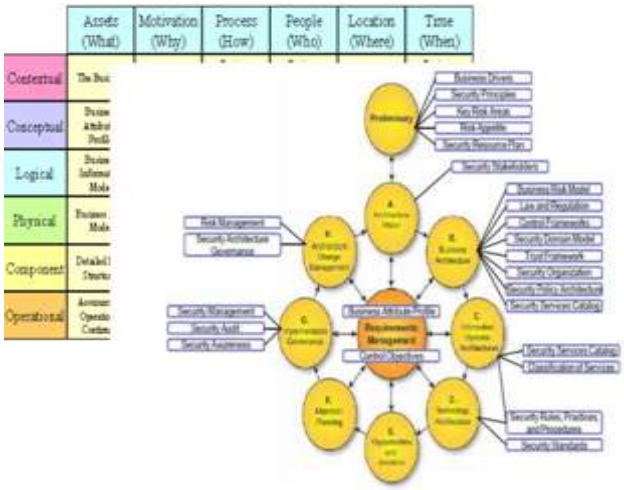

Fig. 13. The architecture interface with security modules [55].

CTC-HSI's constraints and characteristics are, [12]: 1) Security, which includes the protection of the Entity's information against unauthorized actions; 2) According to H.R. 4246, Cyber Security Information Act, Cybersecurity is: The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means …; 3) According to S. 1900, Cyberterrorism Preparedness Act of 2002, Cybersecurity is: Information assurance, including information security, information technology disaster recovery and information privacy… The CTC-HSI supports governance which defines the interaction between various PCP components that use: 1) Data; 2) Technology resources; 3) Networks; 4) IoT, Web and Internet infrastructure; 5) Service oriented applications' DecSecOps4CTC; 6) PCPs, policies; 7) GPM aspects; and 8) EA. As already

mentioned, TRADf supports TOGAF/ADM4CTC which includes the interfaces for frameworks like the SABSA to handle security requirements, [55]. The CTC-HSI supports network management that can be divided into the following sub-domains: 1) Fixed network; 2) External interfaces; and 3) Mobile or ad hoc networks; concerning Cybersecurity can be defined as the PCP's state that is prone to threats. The CTC-HSI delivers a PCP that is designed to provide maximum security. The CTC-HSI depends on the following fields: 1) Cyber technologies; 2) Global and national security requirements; 3) International security requirements; 4) Organizational security requirements; and 5) Financial security and regulations. The CTC-HSI encloses frameworks, like SABSA to handle classical Cybersecurity requirements, as shown in Fig. 13, [40], [52], [54], [55]. That needs a holistic design process.

7.2 The Holistic Design Process

Creating the classification domains (or CSAs) for the holistic design process is to reduce complexity in defining CTC-HSI objectives, like, security requirements, sRisks, threats, GPM financial dangers, and controls. Other objectives can be: 1) *Project* costs and finance; 2) Performance and speed; 3) Maintainability; 4) Use of saBBs; 5) Backward compatibility; 6) Use of CSFs and KPIs as metrics; 7) *Entity's* Cyberspace is global and international; and 8) GPM attacks. Classifying CTC-HSI CSAs can be complex because many APDs overlap. CTC-HSI's design process is done by applying the following phases, [15]: 1) Phase I - Preparation for defining security requirements; 2) Phase II - Security vulnerability analysis; 3) Phase III - Threats' modelling; 4) Phase IV - Determination of security requirements; 5) Phase V - sRisks assessment; 6) Phase VI - Categorization and prioritization; and 7) Phase VII - Preparation of documentation. In all these phases monitoring and logging must be supported.

7.3 Monitoring and Logging.

CTC-HSI logging enables central logging for all PCP resources, where logged data is essential for maintaining, measuring, and optimizing performance and security. It is complex to leverage logged data from heterogenous ICS and multi-CPs. Simplicity is critical for supporting PCP logging and it is important to use a multi-CP logging strategy that includes: Tooling, Organizational structure, and Implementing PCP logging processes. The CTC-HSI supports leveraging log-based insights to improve PCP's performance and billing activities. PCP's log media includes: Event logs, Security logs, Transaction logs, Message logs, and Audit logs. To achieve a cohesive collection and robust aggregation process, the PCP implements a log management environment to ingest, process, and correlate logged data. The CTC-HSI needs to build a *Multi-Cloud Logging Strategy* that includes where logging operations can be complex. *Multi-Cloud Logging Strategies* enable cohesive operations and unify incompatible services and data media. The CTC-HSI is not dedicated to any specific CP and it offers to support: 1) Performance and availability; 2) Reliability and recovery; 3) Attack tracing; 4) CP activities; and 5) Cybersecurity fundaments. The CP is controlled and monitored in real-time, using a unified logging system that supports distributed environments CTC-HSI's main activity is to Consolidated Audit Trail (CAT), and to use regulatory reporting obligation(s), which will increase PCP's power and storage requirements, [30]. GCP's Stackdriver is the service for collecting metrics, logs, and events; and it contains applications for debugging and tracing. Application-specific events can inform application performance and DevSecOps4CTC with respect to *Project* constraints.

7.3 CTC-HSI and DevSecOps4CTC

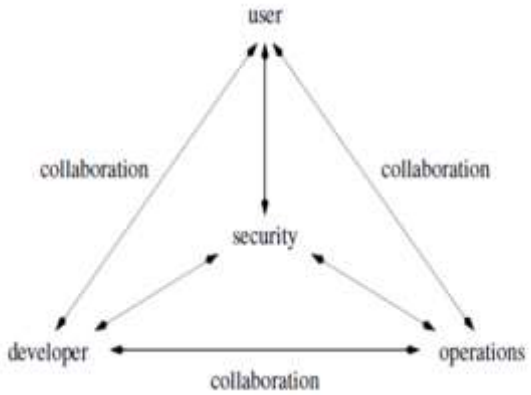

Fig. 14. DevSecOps relationships between stakeholders [39].

DevSecOps4CTC are coordinated processes that manage developers, operations, and security for Project members, as shown in Fig. 14. DevSecOps4CTC procedures are used to identify patterns for managing transformation requirements, [39], which would hinder violations.

7.2 Violations, Types of Dangers and Attacks

Entities' Cybertransactions are orthogonal to Cybersecurity requirements, where the business environment roles define the responsibility for their resources. Cybertransactions outcomes must be asserted, traced, and their periodic summaries are reported to the executive management, [27]. The most common motivations for violations and attacks are: Financial greediness, Lack of ethics, Immoral education, Geopolitical interest, and others. Financial greediness can drive major criminal acts, like gigantic financial irregularities, which are related to fraud and money laundering that damage many countries, and this case it is related to major global financial institutions, like the Union des Banques Suisse (UBS), [45], in which 32 trillion US dollars are hidden.. Under the cover of bank secrecy… GPM is behind major Cyberattacks like [12]: 1) Denial-of-Service (DoS) and Distributed DoS (DDoS); 2) Man-in-the-Middle (MitM); 3) Phishing and spear-phishing; 4) Drive-by attack; 5) Passwords theft; 6) Structured Language Query (SQL) injections; 7) Cross-Site-Scripting (XSS) ; and 8) Eavesdropping attack. GPM-backed attacks need CTC-HSI protection concepts.

7.3 Protection Against Attacks

Attacks are mainly due to global connectivity, GPM bank secrecy, and the usage of complex distributed CP/ICS services. CTC-HSI blocks threats and closes doors for Cyberhackers. A Cyberhacker is a criminal who steals access to the CP/ICS, usually by getting access to administrative part of the ICS to access controls; and where he hides his stolen assets in GPM banks. An Entity may counter these types of threats: 1) Cybercrime, which includes a single Cyberattacker or groups, attacking Entities for financial gains or to cause damage; 2) Cyberattack, often involves GPM/financial and/or politically motivated information gathering for various ideological purposes; and 3) Cyberterrorism, it is used to undermine the ICS and to cause panic; it originates from various anonymous groups. The CTC-HSI proposed actions and predispositions used to support the Entity's security and to reduce sRisks of possible attacks and offer protection, like spreading information and knowledge to all Entity's organizations, units, and personnel related to sRisks of Social Engineering Attacks (SEA), GPM banks, and common social scams. An attack is enabled by gaining access right to attack, which can be hindered by: 1) Systemic password management; 2) Using screen lock and face recognition when mowing away; 3) Block the use of email attached files from anonymous email addresses; 4) Not using anti-virus software, 5) Sharing personal info (and client or server nodes); 6) Not reporting security loops to the company; 7) Not using proper paper Documents; 8) Non-secured digital Data (while at rest and in motion); 9) Unsecured way of Information handling; and 10) Providing of information over the phone. CPs need strict governance and legal constraints to achieve this legal support, CSFs are selected and asserted, to monitor the used artifacts in complex security domains, [9].

7.2 Basic Security CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 6, and can be used for CTC-HSI's basic security approach.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_BasicSecurity_Concepts_Frameworks	Complex	From 1 to 10, 08 Selected
CSF_BasicSecurity_Holistic_Design_Processes	Possible	From 1 to 10, 09 Selected
CSF_BasicSecurity_DevSecOps4CTC	Complex	From 1 to 10, 08 Selected
CSF_BasicSecurity_Violations_Attacks	Complex	From 1 to 10, 08 Selected
CSF_BasicSecurity_Protection_Concepts	Complex	From 1 to 10, 08 Selected

valuation

Table 6. CSFs have an average of 8.20.

8 CTC-HSI COMPLEX SECURITY DOMAINS

8.1 Motivation, Capacity and Competence Development

The CTC-HSI tries to detect risky GPM misdeeds even if predators offer attractive financial conditions and perfect locked-in traps. It is an unwritten concept that can at any moment sweep out an Entity of its wealth. Such a case is the fraud scandal of the bank UBS that was hit with a historic fine and the incredible delict was openly supported and protected by the Swiss Federal Court that makes the Swiss banks' a major security threat [19]. The ADM4CTC supports CTC-HSI for capacity building enforcement, best practices, and Entity-specific PCP capabilities, mainly to evaluate PCP sRisks. CTC-HSI uses existing CSs' policies which include [3]: 1) Services-based security; 2) Management of viewpoints; 3) To design internal non-normative security scenarios; 4) To design single-purpose secure process instances; 5) To develop coordinated and secure application models, and 6) Defined security aspects. The CTC-HSI manages single-

purpose components and measures the security levels of used artifacts, by: 1) Using AI/ML for the handling of data/information resources; 2) Defined CTC-HSI policies, 3) Codify data/information management policies; 4) Enable PCP sRisk analysis; 5) To support secured VM, load balancers and other artifacts management; 6) Support secured IoT artifacts management; and 7) Support secured data classification policy documentation. The CTC-HSI manages the services flow's fallout, abnormal flows, failure modes, and the possibilities in which CP's applications can be interrupted or attacked. All Entities have security concerns and they should dedicate a CTC-HSI to support the CP, [47], which uses avantgarde ICS.

8.1 Avantgarde ICS

Major avantgarde ICS used in nuclear modernization has become one of the least priorities and the actual priorities are: Hypersonics; Directed energy; Command, control, and communications; Space offense and Defense, Cybersecurity; AI/ML; Missile Defense; Quantum science computing; Microelectronics; Autonomy and other. AI/ML and autonomy are of high priority for any CTC-HSI. CTC-HSI must prioritize CSAs to enable a systematic and holistic approach and should adopt an N-tiered strategy. The CP uses standard complex artifacts like in the case of a GCP and technology types: 1) CSs which offer configured processors, memory, disk, and OSs; 2) Kubernetes clusters, used to automate management; 4) AE is a fully managed serverless platform; and 5) PCP functions which are event-driven serverless function, [8], [30], [9].

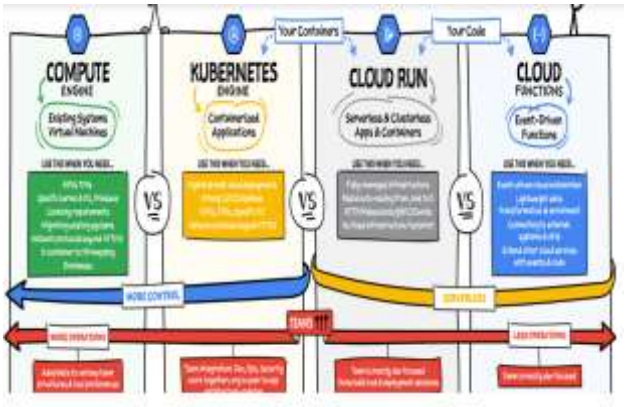

Fig. 15. PCP CS types, [30].

Stateful PCPs may present major challenges, when designing PCP's main block.

8.2 CTC-HSI Main block

The Identity and Access Management (IAM) service are designed to allow the PCP to specify which operations can be used by a user on its resources. The main IAM's elements are: Identities and groups, Resources, Permissions, Roles, and Policies, [9]; where:

- Identities and groups are objects that are used to grant access permissions to users, where an Identity is an object that represents a PCP actor that executes actions. There are various types of objects, like: Account, Service, and Identity domain. An account is used by an actor who interacts with the PCP, like developers or administrators.
- Resources are PCP objects and can be accessed by users; there is a large category, like: Projects, VMs, AE applications, Storage buckets, ….
- Permissions are the rights to perform an action on a PCP resource and permissions vary by the type of resource with which they are associated.
- Roles are sets of permissions and by using the IAM is that administrators grant roles to Identities, and not permissions. It is impossible to grant permission directly to a user, and it is granted by assigning an Identity. Roles can be granted to Identities, where an Identity can have multiple roles.
- Policies enable the association of a set of roles and permissions with PCP resources. A policy is a set of statements that define a combination of users and associated roles.
- Data security in a PCP, provides multiple mechanisms for securing data in addition to IAM policies, which control access to its data, by using encryption.
- Security design principles supports PCP needs to enforce security design principles, like the Separation of Duties (SoD), least privileges, and defense in depth. SoD is the practice of limiting the responsibilities of a PCP user to prevent malicious actions.
- General Data Protection Regulation (GDPR) is used to standardize privacy protections across the European Union (EU), by granting controls to individuals over their private information, and to specify security controls required for Entities managing private information of EU citizens.

- CTC-HSI resources can be optimized by using the DMS4CTC.

8.3 DMS4CTC's Integration

The CTC-HSI's DMS4CTC uses logs which inputs from various subsystems and these inputs depend on the defined level of tracing. If the Project's team signals a security problem to be solved, then the DMS4CTC is activated to propose a set of possible solution(s). CTC-HSI's AI/ML/HDT model includes scenarios of interactive services. These services make DMS4CTC's integration flexible and support the Project by offering saBBs. CTC-HSI's saBBs interact with other Projects Microartefacts in a synchronized manner and uses the ADM4CTC to assist in their management of various APDs using Digital Transformations (DT), [2].

8.4 Complex Security Domains' CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 7, and can be used for CTC-HSI's basic security approach.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_ComplexSecurity_Motivation_Capacity	Complex	From 1 to 10, 08 Selected
CSF_ComplexSecurity_Avantgarde_ICS	Possible	From 1 to 10, 09 Selected
CSF_ComplexSecurity_MainBlock	Possible	From 1 to 10, 09 Selected
CSF_ComplexSecurity_DMS4CTC_Integration	Complex	From 1 to 10, 08 Selected
CSF_ComplexSecurity_ADM4CTC_Integration	Complex	From 1 to 10, 08 Selected

valuation

Table 7. CSFs have an average of 8.40.

9 CTC-HSI FOR APDs

9.1 Digital Transformation, PCPs, and Security Concepts

The CTC-HSI is a set of procedures and technology concepts used for external and internal threats and Entitles need a CTC-HIS to finalize a DT. PCP-based DT support a global and agile change to optimize their operational processes, productivity, and security. The Project must find the right balance to integrate CP components in its PCP. PCP-based DT challenges are [28]: 1) Lack of visibility; 2) Multitenancy; 3) Access management and shadow IT; 4) Compliance; 5) Misconfigurations; 6) IAM capability; 7) Data Loss Prevention (DLP); 8) Security Information and Event Management (SIEM) capability; and Business continuity and disaster recovery, which protect various business aspects.

9.2 Business Aspects

Fig. 16. PCP models, [25].

The PCP has five main characteristics: On-demand internal self-service, Entity wide network access, resources planning & pooling, rapid elasticity, and optimized services. CTC-HSI has main backbone services models: IaaS, PaaS, and SaaS; and has four deployment models: PCP, public CP, community CP, and hybrid CP. CPs have important potential, to confirm that potential, an Entity must use the form of CP that is the most suited to its needs to improve its business advantage. A PCP supports financial models presenting revenue, capital and operational expenditure, and costs are the models from which Return On Investment (ROI). Using a PCP, CSFs of an ROI (or business advantages) are evaluated, these CSFs are: utilization, time compression, scale, and quality. PCP-based services offer scalable, secure, and reliable infrastructure that is specifically implemented to streamline business performance, support development, and growth; PCP's main advantages are Flexibility, Business continuity, Cost efficiency, Improved collaboration, Scalability, and performance, Automatic software updates, Environmentally friendly, Automatic software integration, Usability and accessibility of secure information, Streamlining applications and processes, Compliance and security, and PCP business models. The major and real disruptive power of CTC-HSI-based platforms lies in their ability to manage innovative businesses and operate PCP models. Applying rapid scaling of innovative capabilities and concepts, supported by the CTC-HSI The major CSFs that can be mapped to innovative PCP models, as shown in Fig. 11, can support the Project by the use of CP: Business model, Operating model, Technology, and enrichment of shopping experience, and artifacts, [46], [51], [25]. PCP models are supported by legal controls.

9.3 Legal Controls

International law on classical and Cybersecurity is inefficient, and some major states are hesitant to integrate such laws that are based on the emergence of non-government norm-making initiatives. States insist on their traditional central legal system that marginalizes the inter-state governance of Cyberspace, [38]. Cybertransactions are influenced by the Uniform Law Commissioners who promulgated the Uniform Electronic Transactions Act in 1999. It is the first adaptable effort to prepare a Cyberlaw for Entities. The Uniform Electronic Transactions Act represents the first effort in providing some standardized rules to govern Cybertransactions, [49]. The integration of the CTC-HIS is done with the use of standardized legal controls and supports data protection laws, contract law, procurement law, fraud law, and many other legislation domains to counter GPM crimes. A country, like Switzerland, where illegal money cannot be transparently audited and traced, can provide security breaches and is a safe cave for dubious investors and criminals; unfortunately, such countries serve as a role model for honesty. GPM financial havens have been the main leaders in worldwide financial scandals, misdeeds, and criminal acts that include: 1) Libor manipulations; 2) Criminal currency manipulations; 3) Credits manipulations; 4) Arms dealing transactions; 5) Hijacking people's wealth and documents falsification; 6) Financial and tax frauds; 7) Geopolitical confiscations, like in Gadhafi's case; 8) War victim wealth confiscation, like in the World War WWII and many other conflicts; 9) Drug dealing transactions; 10) War support against future financial competitors, like the case of Lebanon; 10) Forced confiscations; 11) Drastic and unjustified fines; 12) CP/ICS security breaches which stolen resources are transferred to GPM safe havens, [53]; the major problem with combating such GPM backed security breaches that some countries, like Switzerland, have hermetically closed systems which no ethics.

9.4 Predators and Ethics

The Nobel prize winner, the British economist, Angus Deatoon, warns about the destructive GPM's professional graduating business schools and to stop financial and hence security brutalities. The leading schools with such perceptions are the Chicago school, and the Swiss HEC, and many others, [36]. Such profiles can be classified as major GPM profiles which are the biggest threats to Entity's security. The probable motivation is extreme cupidity which is destroying Europe's industrial, societal, and engineering capacities. Revelations of the Swiss Leaks affair, the Swiss HSBC condemned for tax avoidance show the need for evolution towards ethical banking and that future generations of students in finance, economics, and management, must be aware of ethical values. GPM-based states tend to become leaders in Finance and Technology (FinTech) domains who are responsible to security standards?! The International Organization of Securities Commissions (IOSCO) identified eight domains that constitute FinTech. Before applying a CTC-HIS-based FinTech strategy a Project must consider ethics, financial crimes, and irregularities, like in the cases of:

- Tax fraud, where corrupt transparency organizations and politicians make it impossible to mitigate sRisks; where GPM accountancy financial flows and disable any type of transparency.
- Financial regulation, where GPM institutions do not respect ethics, security controls, and regulations.
- Perfect financial crime model, which supports brutal dictators like neo-Nazi brigands has a special status in states where the ownership of substantial financial assets can remain anonymous. Some Third World dictators maintain strong financial relationships with banks in financial havens.
- The major problem with combating such a GPM-based system or country, is that some Entities have a hermetically closed system and have an important geopolitical influence and reach.

9.5 Geopolitical Influence and Reach

The selection of CTC-HIS's CSFs is based on the following facts [12],[14]: 1) PCP/ICS resources; 2) Actors and boundaries; 3) Used and connected components; 4) Technical and functional security requirements; 5) Precisely defined Project's strategies, objectives, and goals; 5) Applied basic and complex security policies; 6) Sustainability and competition; 7) Geopolitical and geoeconomical contexts; 8) Behavioral sciences and parapsychology mirage; 9) GPM motivated Cyberattacks, and 10) Global security considerations. Determination and the evaluation of major sRisk is affected by many CSFs and their relation/correlation is therefore essential. Entities must defend their assets, resources, critical

processes, and data storage; so that external criminals or Cyberhackers using a GPM stronghold can be detected and deterred to access to its PCP. Such unauthorized access can be fatal and very difficult to prove. The Entity must be capable to defend its PCP main components' robustness, like data consistency, accuracy, reliability, and must build its own CTC-HIS to identify and block any Cyberhacker who attempts to damage the Entity. Therefore, the main objective is to block and to have CTC-HIS controls that identify GPM (or other types of attack patterns) attempts, like unauthorized and even criminal activities. Besides classical security and Cybersecurity, the GPM must be aware of other types of organized asymmetric attacks like: 1) Cyberwarfare; 2) Cyberterrorism; 3) Cyberhooliganism; 4) Cyberfinance attacks; and others. The CTC-HIS handles also various types of FinTech-related sRisks. GPM based institutions have a culture of financial secrecy and plundering and would be tempted to use FinTech to obfuscate the origins of illegal money and other assets, like in the concrete cases: 1) Paula Ramada estimated the amount of lost money due to the benchmark of interest rates debacle is estimated at $300 trillion in financial instruments, ranging from mortgages to student loans, [43]. FinTech would make security breaches more embedded, abstract and undetectable; 2) FinTech transforms the legacy financial environment in the delivery of embedded services; 3) Blockchain is a FinTech framework that supports cryptocurrency like Bitcoin, which is challenging for security; and 4) GPM based security breaches tactics can be used to destroy Entity's assets, in various APDs like Defense.

9.6 Defense and Security

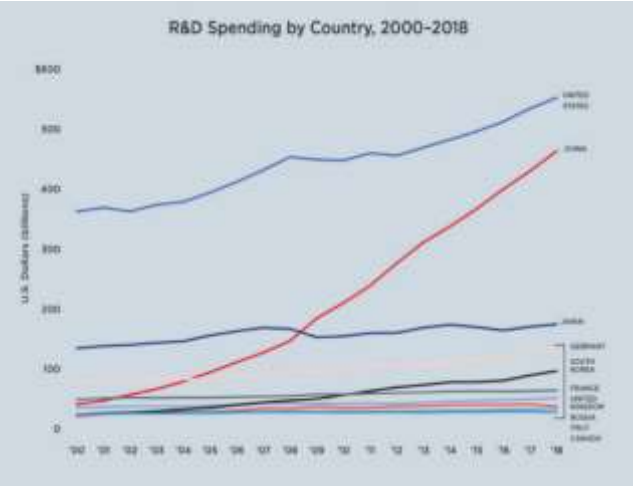

Fig. 17. Spending by major players.

Defense specialists have formulated the most important strategic, security, and tactical concepts of warfare, using principles like: Offensive surprise initiatives, Security concepts, Unity of command, Economy of force, mass, maneuver, … CTC-HIS's control of command and cooperation, is crucial to follow these objectives, the capacity to use Entity's forces effectively and to optimization critical phases. Maneuver consists of secured manners on how troops can be deployed and moved to support offensive, mass and surprise activities, [23], [46]. USA's Department of Defense (DoD) constant technology priorities jeopardizes its capacity to win a long-term technology competition, it needs a systematic and holistic approach, where an CTC-HIS is the kernel. Today's PCP/ICS' evolution is the leading trend and the highest DoD's priority is CTC-HIS for digital technologies developed by the private sector. Technology is the artifact needed to achieve military superiority, but alone it cannot give a decisive advantage and is an enabler for gaining superiority. Combined with the right organization, training and concepts for war activities, technological advantages can make combats asymmetric, but the human factor is the decisive CSF. The CTC-HIS must incorporate the mentioned trends to outcompete adversaries, [44]. The most important changes in the military competition will come partially from CTC-HIS capabilities. CTC-HIS is a crucial CSF for economic competitiveness and financial benefits, which is supported by political and military capacities; but also, by mammothlike companies like Google and others. As shown in Fig. 17, China will overtake the USA in national Research & Development (R&D) activities, knowing that China is already a leader in various ICS domains, like: AI/ML, genomics, and quantum technologies. The CTC-HIS must support a national technology concept that manages the Entity's government and private sectors. Between the years 1998 and 2018, China's national R&D spending had an average of 15 percent annually and it is closing the gap with the USA. USA's R&D spending was 13 times that of China's in 1998 and China surpassed the USA in 2020. The CTC-HIS recommends setting priorities on: 1) Increasing security R&D spending; 2) Improving human capital through education; 3) Accepting high-qualified immigration; 4) To improve the security of data, processing resources; and 5) Integrating existing security standards. Partnerships and alliances are needed for a global CTC-HIS to prepare for sophisticated Cyberwarfare.

9.7 Cyberwarfare

Since WWII, the primary ICS, security, and tactical advances is the emergence of amphibious warfare. The development of nuclear warfare, which continued after WWII, introduced a new security concept based on nuclear strategy and tactics; that introduced immense destructive possibilities, which meant also that warfare had limited traditional security goals. The use of conventional tactics with technologically very advanced arms would predominate in limited wars that followed WWII. That resulted in the need to keep wars limited and that has produced a global security CTC-HIS pattern based on: small, mobile special forces, armed with light but sophisticated weapons and trained in guerrilla tactics, that can be rapidly used and rapidly withdrawn from hostile regions, [23]. But the emergence of sophisticated Cyberwarfare CTC-HIS-based systems become a priority. Complex APDs need advanced DevSecOps4CTC.

9.8 Advanced DevSecOps4CTC for APDs

The CTC-I recommends the DevSecOps4CTC to automate Continuous Integration and Continuous Deployment (CI/CD) methods, distributed serverless architectures, and ephemeral assets like Functions as a Service and containers. That present advanced security challenges and sRisk like: 1) Increased Attack Surface; 2) Lack of Visibility and Tracking; 3) Ever-Changing Workloads; 3) DevOps, DevSecOps, and Automation; 4) Granular Privilege and Key Management; 5) Complex Environments; and 6) Cloud Compliance and Governance. Entities need highly automated DevSecOps4CTC to ensure that appropriate CTC-I controls are embedded in software components. CTC-I-related changes implemented after a component has been deployed can jeopardize the Entity's security structure which needs a holistic APD approach, [22].

9.9 A Holistic APD Approach

CTC-I holistic approach unifies the protection against sRisks, by setting PCP security policies, implementing best practices, and eliminating silos and that permits the Project's team to be proactive about PCP security. By implementing CTC-I best practices, an Entity can manage sRisks, where authorized users can damage the PCP. Clearly defining access and roles, limiting use, and remembering that no PCP is completely independent of human error can facilitate sRisks management. A security plan can be shared by Entity's employees to reduce human error. The CTC-HIS strategy is based on: 1) To gain awareness and visibility of PCP's structure; 2) Set security standards before automation; 3) Security skilled engineers implement software components; and 4) Establish security in all ADM4CTC phases. Adopting a holistic approach the Project team will be capable of tracking benchmarks, verifying security decisions, and more effectively protecting the PCP, [37]. sRisks related to a holistic approach are, [32]: 1) Internal threats due to human error; 2) Interconnectedness; and 3) Convenience over security.

9.10 CTC-HIS for APDs CSFs

Based on the LRP4CTC, the most important CSFs are presented in Table 8.

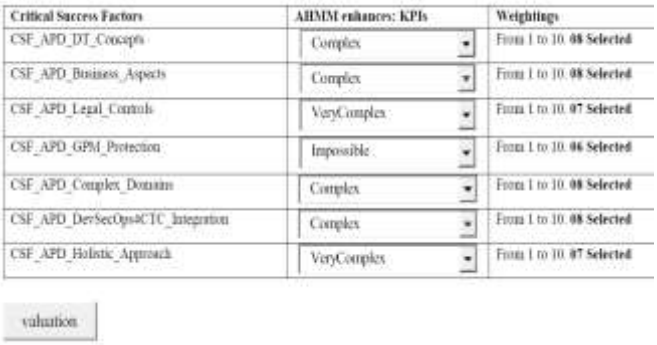

Table 8. CSFs that have a rounded average of 7.5.

10 THE POC'S IMPLEMENTATION

This PoC uses an *Entity* using *CloudEcoSource* and other GCP UCs, where the CTC-HIS-based solution, needs to engage several external *Cloud Service Providers and Partners,* to build a PCP; and also to support its critical business needs. The *Entity* uses EA practices and saBBs, which are used to manage its CTC-HIS-based services. *CloudEcoSource* has three distinct CTC-HIS-specific initiatives which are based on the following sub-systems: IaaS, PaaS, and SaaS; these sub-systems are for basic *CloudEcoSource* secured operations. This PoC describes how *CloudEcoSource* plans to use the CTC-HIS to create and evolve initiatives [48]: 1) The IaaS initiative, to secure the infrastructure; 2) The PaaS initiative, is related to the concept of development with DevSevOps4CTC; and 3) The SaaS initiative, concerns secure collaboration among service providers. The PoC's development uses CTC-HIS in an adapted implementation environment.

10.1 The LRP4CTC's

The LRP4CTC (or Phase 1) outcome supports the PoC's background, using an archive of an important set of references and links that are analysed using a specific interface. After selecting the CSA/CSFs tag is linked to various PCP-secured Microartefacts scenarios; where all its details are defined; this concludes Phase 1. In this DMS4CTC-related PoC (or Phase 2), the HDT delivers solutions. The empirical part is based on the AHMM4CTC's instance and the PCP Microartefacts mechanics', which uses the internal initial sets of CSFs' that are used in phases 1 and 2.

10.2 From Phase 1 to Phase 2

The *Project's* enumeration of CSAs are: 1) The RDP4CTC; 2) The ACS4CTC Integration; 3) The Usage of the ADM4CTC; 4) The CP, CSs, and security; 5) The AHMM4CTC's Integration; and 6) The DMS4CTC and the KMS4CTC. Where Tables 1 to 5, were presented and evaluated in this chapter and they are this chapter's empirical part.

10.3 The PoC

The PoC was implemented using the research's *TRADf* using its Natural Language Processing 4 CTC (NLP4CTC) and the selected CSFs', which are related to CTC-I requirements. The PoC was achieved using *TRADf's* development environment and the mapping/linking actions are activated by: 1) Choosing an HDT node that contains the requirement; 2) Choosing the CTC-I Microartefact(s) to be linked; and 3) Choosing a CTC-I problem to be solved. When the setup is achieved, from the front end the CTC-I requirements development initiation interface which is shown in Fig. 18, was launched.

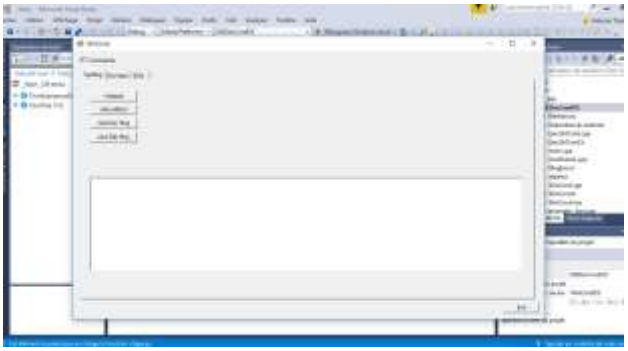

Fig. 18. The TRADf's setup interface.

The CTC-I uses the HDT which is the DMS4CTC to solve problems and offer solutions, whereas the NLP4CTC scripts that make up the DMS4CTC subsystem. CTC-I-related CSFs were also selected as demonstrated previously in this chapter's eight tables and the result of the processing of the DMS4CTC, as illustrated in Table 9, shows clearly that the CTC-I is not an independent component and in fact, it is strongly bonded to the Project's overall sRisk management approach. RDP4CTC's constraint is that CSAs having an average result below 8.5 will be ignored. As shown in Table 9 (which the average is 8.20), this fact keeps the CSAs (marked in green) that help make this work's conclusion; and one in red. It means that such a CTC-I integration will not succeed and that the CTC-I Project is very complex.

CSA Category of CSFs/KPIs	Influences transformation management	Average Result
RDP4CTC's Integration	Feasible	
ICS' Integration	Feasible	
ADM4CTC's Integration	Complex	
KMS4CTC/DMC4CTC Integration	Complex	
sRisks Management	Complex	
Basic Security Integration	Complex	
Complex Security Integration	Complex	
APD's Transformation and Integration	VeryComplex-Impossible	

Evaluate First Phase

Table 9. The CTC-HIS research's outcome is 8.20.

11 CONCLUSIONS

As mentioned, the Project is very complex and the recommendations are:

- The Project must be separated into multiple PCP transformation steps.
- The CTC-HIS is very complex to implement.
- The legacy ICS and its unbundling is a crucial step for the CTC-HIS-based PCP.
- The ADM4CTC supports PCP's construction.
- An Entity can build its own PCP, there is no need for a commercial product.
- A PCP must integrate various security aspects and it delivers major business advantages.
- The PCP enables the automation of saBBs to support implementation activities.

- CP security technics focus on the Entity's isolated security tools and services.
- The CTC-HIS has a holistic approach.
- GPM financial motives are the main reasons for security breaches and financial crimes.
- The RDP4CTC uses the HDT, where CSFs are tuned to support Project architects to diminish failure rates when building a CTC-HIS-based PCP. The CTC-HIS interfaces PCP security components, requirements, CSs, and Entity's resources. The CTC-HIS is an important factor in the Project's evolution and robustness. The PoC was based on the CSFs' binding to a specific RDP4CTC resource and the HDT that represents the relationships between the CTC-HIS requirements, saBBs, and CSFs. The result proves that a CTC-HIS for the PCP is very complex. TRADf's future research efforts will focus on the various strategy for CTC for AI.

References:

[1] Jonkers, H., Band, I., & Quartel, D. ArchiSurance Case Study. The Open Group. 2012.

[2] The Open Group. Architecture Development Method. The Open Group. USA. http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html. 2011.

[3] The Open Group. TOGAF 9.1. The Open Group. USA. http ://www.opengroup.org/subjectareas/enterprise/togaf . The Open Group. The Open Group. USA. 2011.

[4] Agievich, V. (2014). Mathematical model and multi-criteria analysis of designing large-scale enterprise roadmap. PhD thesis on the specialty 05.13.18 – Mathematical modelling, numerical methods and complexes of programs.

[5] OMG. DECISION MODEL AND NOTATION (DMN). OMG. https://www.omg.org/dmn/. 2022.

[6] Daellenbach, H., McNickle, D. & Dye, Sh. Management Science. Decision-making through systems thinking. 2nd edition. Plagrave Macmillian. USA. 2012.

[7] Easterbrook, S., Singer, J., Storey, M. & Damian, D. Guide to Advanced Empirical Software Engineering-Selecting Empirical Methods for Software Engineering Research. F. Shull et al. (eds.). Springer. 2008.

[8] Sullivan, D. Official Google Professional Cloud Architect-Study Guide. John Wiley & Sons, Inc. USA. 2020.

[9] Trad, A. Enterprise transformation projects in the financial industry and ethics (TPFI&E). Journal: The Business and Management Review. Pages 112. 2021.

[10] Transparency. CORRUPTION PERCEPTIONS INDEX. Transparency International. https://www.transparency.org/en/cpi/2020/index/nzl. 2020.

[11] Swissinfo. Switzerland diplomatically rejects Biden's 'fiscal paradise' label. 2021 Swissinfo. https://www.swissinfo.ch/eng/business/diplomacy_switzerland-diplomatically-rejects-biden-s—fiscal-paradise—label-/46578996. 2021.

[12] Trad, A. Business Architecture and Transformation Projects: Enterprise Holistic Security Risk Management (ESRM). Book: Technological Development and Impact on Economic and Environmental Sustainability. Pages 269-310. IGI Global. USA.- 2022a.

[13] Trad, A. Entity Transformation Projects: The Military Technology Strategy (MTS). Journal: Proceedings of 12th SCF International Conference on "Contemporary Issues in Social Sciences". Pages. 308. 2021.

[14] Trad, A. Entity Transformation Projects: Security Management Concept (SMC). Journal: Proceedings of 12th SCF International Conference on "Contemporary Issues in Social Sciences". Pages 326. 2021.

[15] Vulić, I., Prodanović, R. Tot, An Example of a Methodology for Developing the Security of a Distributed Business System. Advances in Economics, Business and Management Research, volume 108. 5th IPMA SENET Project Management Conference (SENET 2019). Atlantis Press. 2019.

[16] Wikipedia. Cloud computing. The Wikipedia. https://en.wikipedia.org/wiki/Cloud_computing ; 2022.

[17] Bala, R., Gill, B., Smith, D., Wright, D., & Ji, K. Magic Quadrant for Cloud Infrastructure and Platform Services. Gartner Inc. https://www.gartner.com/doc/reprints?id=1-271SYZF2&ct=210802&st=sb. 2021.

[18] Airmic (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. Alarm-The Institute of Risk Management.

[19] Alderman, L. (2019). French Court Fines UBS $4.2 Billion for Helping Clients Evade Taxes. The New York Times. USA. Retrieved from https://www.nytimes.com/2019/02/20/business/ubs -france-tax-evasion.html

[20] Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage Risks through the Enterprise Architecture. 45th Hawaii International Conference on System Sciences. USA.
[21] Charles (2017). Hosting and Cloud Software Delivery modelled in Archimate. Agile Enterprise Architecture. https://agileea.com/2017/04/hosting-and-cloud-software-delivery-modelled-in-archimate/
[22] Checkpoint (2022a). What is Cloud Security? https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/#
[23] Cheyney, S. (2021). Strategy and Tactics, Military. Scholastic Inc. USA.
[24] Clark, D. (2002). Enterprise Security: The Manager's Defense Guide. USA: Addison-Wesley Professional.
[25] Digital Innovation Junction (2020). Cloud Innovative Model. https://www.digitalinnovationjunction.com/cloud-innovative-model/
[26] DODAF (2010). Deputy Chief Information Officer, The DoDAF Architecture Framework Version 2.02, U.S. Department of Defense. USA. URL: http://dodcio.defense.gov/dodaf20.aspx.
[27] Fu, Zh., & Mittnight, E. (2015). Critical Success Factors for Continually Monitoring, Evaluating and Assessing Management of Enterprise IT. ISACA. http://www.isaca.org/COBIT/focus/Pages/critical-success-factors-for-continually-monitoring-evaluating-and-assessing-management-of-enterprise-it.aspx
[28] IBM (2022a). An overview of cloud security. IBM. https://www.ibm.com/topics/cloud-security
[29] Green, J. (2020). Google Cloud GCPAIE: Hyper-Accessible AI & Machine Learning. Towards Data Science.
[30] Google (2022a). Cloud for financial services. Google. https://cloud.google.com/solutions/financial-services
[31] IIA (2004). Enterprise Risk Management — Integrated Framework. The Institute of Auditors.
[32] Kaspersky (2022a). Cloud security risks. Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security
[33] Kasarkod, J. (2011). Integration of SABSA Security Architecture Approaches with TOGAF ADM. InfoQ. https://www.infoq.com/news/2011/11/togaf-sabsa-integration/
[34] Kiseleva, I., Karmanov, M., Korotkov, A., Kuznetsov, V., & Gasparian, M., (2018). Risk management in business: concept, types, evaluation criteria. Revista ESPACIOS. ISSN 0798 1015.
[35] Kroese, R. (2014). Enterprise Risk Management Approach. Bizzdesign. https://bizzdesign.com/blog/enterprise-risk-management-approach/
[36] Le Monde (2019). Le Prix Nobel d'économie Angus Deaton : Quand l'Etat produit une élite prédatrice [Nobel Lauréate in Economics Angus Deaton : « When the state produces a predatory elite]. Le Monde. Retrieved from https://www.lemonde.fr/idees/article/2019/12/27/angus-deaton_-quand-l-etat-produit-une-elite-predatrice_6024205_3232.html
[37] Lucidchart (2022). Creating a holistic cloud security strategy. Lucidchart. https://www.lucidchart.com/blog/create-a-holistic-cloud-security-strategy
[38] Mačák, K. (2016). Is the International Law of Cyber Security in Crisis? Law School-University of Exeter. Exeter, United Kingdom. Cyber Power. 8th International Conference on Cyber Conflict. Tallinn: Estonia: NATO CCD COE Publications.
[39] Mees, W. (2017). Security by Design in an Enterprise Architecture Framework. Royal Military Academy, Department CISS. Renaissancelaan 30, 1000 Brussel. Belgium: NATO.
[40] Oxford Dictionaries (2017a). Security. London: Oxford Dictionaries. Retrieved on September 3, 2017, from: https://en.oxforddictionaries.com/definition/security
[41] Peterson, S. (2011). Why it Worked: Critical Success Factors of a Financial Reform Project in Africa. Faculty Research Working Paper Series. Harvard Kennedy School.
[42] Pratap, K., & Predovich, B. (2020). Magic Quadrant for IT Risk Management. Gartner Inc. USA.
[43] Ramada, P. (2013). How much did allegedly rigged interest rate (Libor) cost?. POSTED ON JUNE 4, 2013 BY R.G. RICHARDSONPOSTED IN UNCATEGORIZED ECOMTECHNOLOGY.
[44] Scharre, P. & Riikonen, A. (2020). Defense Technology Strategy. Center for a New American Security. USA.

[45] Stupples, B., Sazonov, A., & Woolley, S. (2019, July 26). UBS Whistle-Blower Hunts Trillions Hidden in Treasure Isles. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2019-07-26/ubs-whistle-blower-hunts-trillions-hidden-in-treasure-islands

[46] The Open Group (2021). Cloud Computing for Business. The Open Group. http://www.opengroup.org/cloud/cloud_for_business/index.htm

[47] The Open Group (2011). Security Architecture and the ADM. The Open Group. https://pubs.opengroup.org/architecture/togaf91-doc/arch/chap21.html

[48] The Open Group (2021). The Open Group Cloud Ecosystem Reference Model – Using the Cloud Ecosystem Reference Model with the TOGAF Standard (Informative). The Open Group. http://www.opengroup.org/cloud/cloud_ecosystem_rm/p5.htm

[49] The Uniform Law Commissioners (2015). Electronic Transactions Act Summary. New York: The Uniform Law Commissioners.

[50] Togaf-Modeling (2020). Application communication diagrams. Togaf-Modeling.org. https://www.togaf-modeling.org/models/application-architecture/application-communication-diagrams.html

[51] Trad, A. (2022). Business Transformation Projects: The Integration of Cloud Business Platforms (ICBP). SCF International Conference on "Contemporary Issues

[52] Trad, A. (2021). The Security Management Concept (SMC). STF Conference. Turkey.

[53] Trad, A. (2017). The Business Transformation and Enterprise Architecture Framework-Applied to analyse the historically recent Rise and the 1975 Fall of the Lebanese Business Ecosystem. Hershey, PA: IGI-Global.

[54] Trad, A., & Kalpić, D. (2019). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation-The Role of Cyber and Information Technology Security in Automated Business Environments. IGI-Global. USA.

[55] Unwin, D. (2013). Security Architecture-Enterprise Architecture. Business Aspect.

[56] Ylimäki T. (2006). Potential critical success factors for EA. Journal of Enterprise Architecture, Vol. 2, No. 4, pp. 29-40.

[57] Trad, A., & Kalpić, D. Using Applied Mathematical Models for Business Transformation. IGI Complete Author Book. IGI Global. USA. 2020a.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Antoine Trad, has written the article and developed the proof of concept.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)