Advanced Research on Information Systems Security

ARIS^2
an
international journal

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Government Transformation Projects-The Role of E-Health Polymathic Secured Implementation (GTP-REHPSI)

Antoine Trad [a]*

[ac]Dr., 5 rue Carle Hebert, Courbevoie, 92400, France.
[a]Email: antoine.trad@ibistm.org

Abstract

This article illustrates the role and how to design and implement a Government Transformation Projects (GTP) in-house E-Health Polymathic Secured Implementation (GTP-REHPSI, or simply *e-health*) that can use the authors' previous works, like the Enterprise's Holistic Security *e-health* (ETP-HSC) [1,2,3]. In this article the focus is on *e-health* in the context of the comparison of major Governmental Health Systems (GHS) to be adapted for the Kingdom of Saudi Arabia's (KSA) health system. *e-health* includes interfaces to practically all major domains, like Traditional health domains, electronic/web-based health, AI based health modules.... *e-health* uses the author's Polymathic transformation framework and included methodology that supports the GTP-REHPSI [7]. Knowing that GTPs (and other types of transformations initiatives) are complex and have very high level of failure rates (at about 95 percent). GTP's main problem is in the acceptance and integration of a GTP-REHPSI and *e-health* [7]. *The e-health* shows how an GTP integrates GTP-REHPSI and AI based health modules to support GHS' major security breaches. The GTP-REHPSI is supported by the author's (today usable) Applied Holistic Mathematical Model (AHMM) for *e-health* (*M-Model*). This article is a Polymathics research and uses an adapted mixed-research method based on the Heuristic Decision Tree (HDT) [8,9]. The *M-Model* based *e-health* supports: 1) A mixed-method empirical Decision-Making System (DMS) and Knowledge Management System (KMS) (simply *Intelligence*); 2) An Action Research (AR) (ideal for GTP-REHPSIs) method for *e-health*; 3) Portable generic services' approach; and 3) An in-house framework for a successful finalization of secured GTPs. *The e-health* is a new block in the author's Research and Development Project (RDP) and is a natural evolution and the aim is to offer an example of an In-House Implemented (IHI) Transformation Framework (IHITF). *The e-health* for the KSA includes many of the author's research works on the applications of GTPs (simply a Project), global security concepts, Health systems, AI, and Mathematical Models (MM).

Keywords: e-health, Security Processes; Artificial Intelligence; Polymathic; Enterprise Security

Citation: A. Trad, "Transformations Government Transformation Projects-The Role of E-Health Polymathic Secured Implementation (GTP-REHPSI)", ARIS2-Journal, vol. 4, no. 2, pp. 75–110, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.39

----

* Corresponding author. Email address: antoine.trad@ibistm.org

1. Introduction

e-health uses, the GTP-REHPSI, specialized global security cases, Council of Cooperative Health Insurance (CCHI), Saudi Health Insurance Bus (SHIB) Project (SHIBP), Enterprise Architecture (EA), and other specialized domains. The AR based HDT solves problems and the solutions (and defines their paths to actions) are persisted in GTP-REHPSIs; and can be hammered in Project's security strategy. *e-health's* can be used by executive (or Project) managers, security architects/analysts, and infrastructure specialists to enable solutions to transform the legacy system. This RDP is Polymathic and includes existing IHITF modules like ETP-HSC, IHITF, (Re)Organization concepts for Projects, Information and Communication Systems (ICS)/secured ICS (sICS), EA, Health systems' analysis, and other…

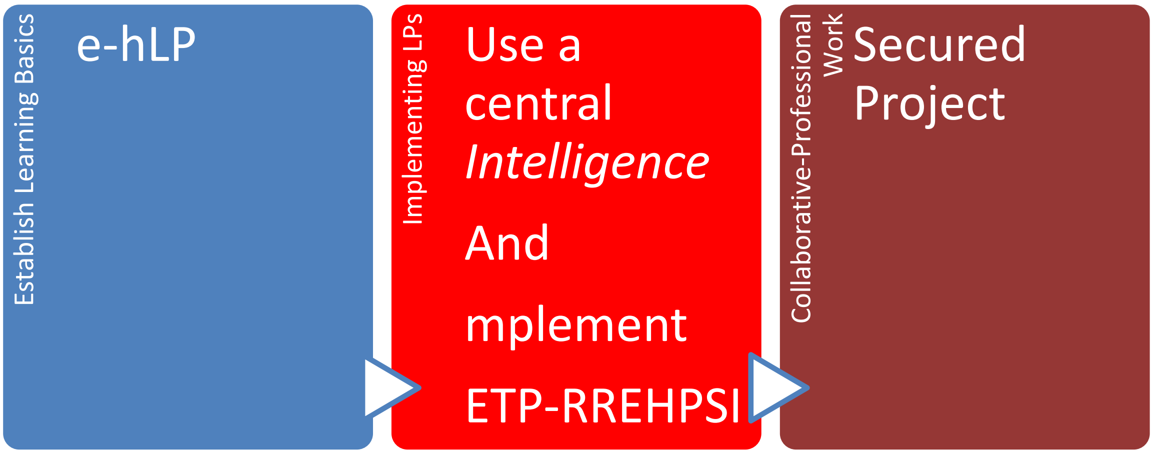

Establish Learning Basics
e-hLP
Implementing LPs
Use a central *Intelligence* And mplement ETP-RREHPSI
Collaborative-Professional Work
Secured Project

Figure 1: The integration of *e-health* in a Project.

This article is linked to all the author's works and previous RDP's findings, which implies that previous blocks are reused/included in this article. *e-health* uses the ETP-HSC that includes already analysed security mechanisms like: Managing Passwords, Firewalls, Secure Development and Operations, Antivirus, Wireless Fidelity, Malware, Security Monitoring and Log**s…** [10,11]. And *e-health's* Learning Process (e-hLP) [3] is used to implement, modify, and integrate GTP-REHPSIs related experiences as shown in Figure 1.

1.1. e-health's and GTP's Viewpoints

A Project can have many Viewpoints, that can include:

- "A" for EA and ICS based transformations.
- "F" for Asset, and financial transformations.
- "G" for Generic transformations.
- "I" for Infrastructural transformations.
- "O" for Organizational, Enterprise and Business transformations.
- "S" for Security based transformations.
- "C" for complete transformations that combines all previously mentioned Viewpoints and where some selected Viewpoints have a priority like "S" in this article (or GTP-REHPSI in this article).

1.2. e-health's Characteristics

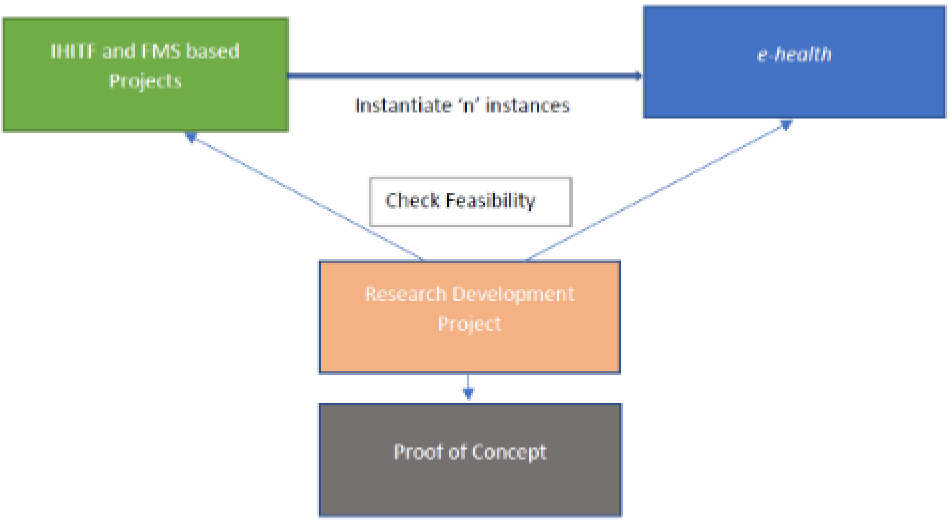

IHITF and FMS based Projects
Instantiate 'n' instances
e-health
Check Feasibility
Research Development Project
Proof of Concept

Figure 2: The interaction between the Project, RDP, and GTP-REHPSI/*e-health*.

This article uses the Factors' Management System (FMS) and IHITF or the author's Transformation Research Architecture Development framework (*TRADf*) that includes: 1) sICS for *e-health*, and corresponding GTP-REHPSI patterns; 2) *Intelligence*; 3) *e-health* generators; and 5) An RDP evolutive strategy, which is the 1st CSA and its heading is in fact the initial set of FMS' CSFs.

1.3. The FMS

The FMS includes and manages the following Project's artifacts:

- Critical Success Areas (CSA), Critical Success Factors (CSF), Key Performance Indicators (KPI), Concrete sICS VARiables (VAR).

- Project's CSAs, CSFs, KPIs, and VARs are known as Factors.
- GTP-REHPSI and *e-health* use the FMS based HDT to support *Intelligence* and hence solve security and common problem.
- Uses the Polymathic Rating and Weighting Concept (PRWC) to evaluate Factors.
- A FMS contains sets of CSAs and a CSA contains a set if CSFs.
- A CSF is a set of KPIs.
- A KPI maps (or corresponds) to a unique Project or GTP-REHPSI requirement or feature [15].
- For a given requirement (or a problem), TRADf selects initial sets of Factors, to be used by the HDT based *Intelligence*.
- A CSF maps to a requirement(s), GTP-REHPSI… [16,17].
- Factors are RDP's main Building Block (BB).

2. The RDP for e-health

2.1. M-Model's Generic Basic Elements

This article (like all author's works) uses generic MM elements that were already defined in the [2,3]. MM's basic elements help in building the Polymathic GHS's Meta-Model (PEMM) and M-Model's elements assess Project common and security risks; some of these basic elements are:

• ***a***	for atomic
• ***m***	mapping operator
• ***….***	
• *REQ*	*is a GTP or e-health* ***requirement***
• ….	
• *GAP*	*is a* GTP ***gap*** that results from *e-health*.
• ….	

2.2. M-Model's Nomenclature

The e-health uses *M-Model's* basic elements to construct its nomenclature that has two major parts: 1) ICS basics; and 2) The applied security requirements, as shown in Figure 3:

<u>Requirements Viewpoint (R):</u>

mcREQ = ***m*** KPI (R1)

mcMapping mcArtefact/mcREQ= mcArtefact + ***m*** mcREQ (R2)

FTR = mcREQ (R3)

PRB = ***m*** PRB (R4)

REQ = ***m*** CSF = $\underline{\bigcup}$ mcREQ (R5)

REQ = $\underline{\bigcup}$ FTR + $\underline{\bigcup}$ RUL + $\underline{\bigcup}$ CNT + $\underline{\bigcup}$ DIA + $\underline{\bigcup}$ REL (R6)

Figure 3: *M-Model*'s nomenclature.

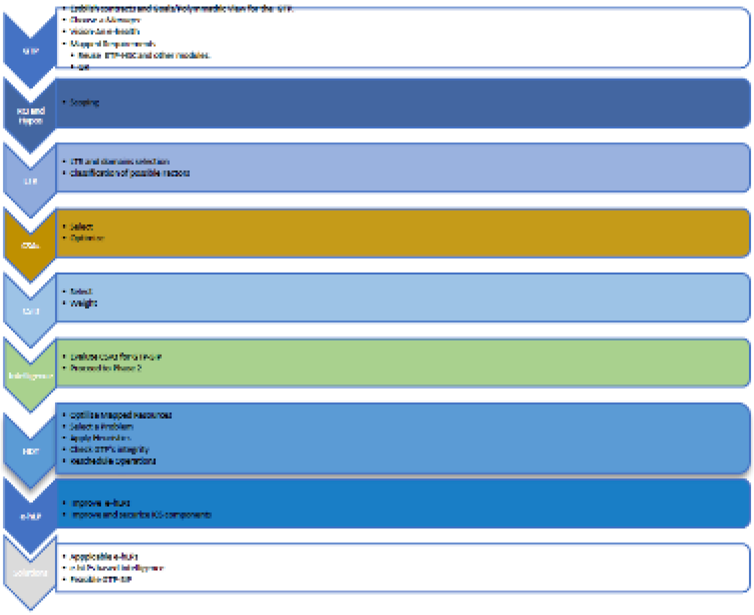
Where a GTP-REHPSI is the choreography of a set of actions that were used to solve a security problem or requirement.

2.3. A Polymathic Projects' and e-health's Approaches

The GTP-REHPSI and hence the *e-health* use the secured Unbundling Process (sUP) to disassemble and defragment the legacy organizational units (simply Unit), which in general have heterogenous methodologies/structures, (s)ICSs, Model View Control (MVC) pattern (that includes sets of atomic MVCs-aMVC) and security concepts. As shown in Figure 4, the *e-health* (and the underlying GTP-REHPSI) focuses on transforming and securing Unit's resources and applying Viewpoint "C", Viewpoint "C"'s has the following structure [2,3]:

- sMA = ∑ aBB + ∑ sBB + ∑ aMVC (C1)
- sBB = ∑ UP+ ∑ sMA + ∑ sOPM (C2)
- sCBB = ∑ sBB + ∑ sABB + ∑ SBB (C3)
- sIBB = ∑ sCBB (C4)
- Unit = ∑ sIBB (C5)
- GTP-REHPSI = ∑ Unit-modifications' actions (C6)
- …
- sUnit = ∑ sSUPL (C10) … secured Unit (sUnit)
- REHPSI(i) = ∑ sUnit-modifications' actions (C11)
- *GHS*(C) = ∑ REHPSI(i) (C12)

The e-health supports the refinement and securing secured Unit (sUnit) platform components.



.

Figure 4: *e-health*'s Polymathic approach.

The RDP presents *TRADf* which relates the selected Applied Case Studies (ACS) and the PoC, which are based on a concrete transformation initiative inspired by a concrete GTP-REHPSI, SHIB. Figure 4 shows the Polymathic-holistic approach used by the *e-health*. And the first step established the Research Question (RQ) and initiated an in-depth Polymathic Literature Review Process (PLRP).

2.4. The RQ and PLRP

The RDP's RQ is: "Can the *e-health* support a nation's health system; and thus, apply GTP-REHPSIs for a secured GHS?". Where this article's auxiliary RQ is: "How can GTP-REHPSIs accumulate Project's experiences in e-hLPs?". The RDP uses: AI related GTP-REHPSIs, EA/ADM inspired Transformation Development Method (TDM), *M-Model*, FMS, HDT, and *Intelligence*. PLRP's processing and analysis showed that there are no similar concepts, frameworks, and approaches; and that *TRADf*, has a clear lead in Polymathic Organizational Transformation Research. TRADf is used to show how can an GHS implement an IHITF for *e-health* or any other domain. Unfortunately, today are some non-Polymathic (or siloed) industry and scholar resources on the mentioned topics, like the case of The Open Group Architecture Framework (TOGAF) that can be used as a minor reference, which mentions superficially transformations initiatives. *e-health*, the M-Model, and other author's works), are un-conventional/pioneering, innovative and tries to cover a significative Projects' gap(s) and their eXtremly High Failure Rates (XHFR). XHFR are about 95% and that confirmed by the PLRP [12,13,14]. XHFR are due to siloed approaches and uncapable academic levels that is essentially focuses on immediate tangible or financial goals. The lack of a Polymathic approach to Projects and can endanger *e-health*. The PLRP used the following resources and references: 1) Articles and resources related to AR/GTP-REHPSIs, Education, ETP-HSC, sICS, GTP-REHPSI, generic reengineering, EA/TDM, and various types of Projects; 2) The existing author's RDP/PLRP works, and TRADf; 3) GTP's and *e-health*'s feasibilities, using a concrete ACS or SHIB; 4) Initial sets of Factors and the FMS; 5) The application of the HDT and PRWC; and 6) The RDP uses of the Empirical Engineering Research Model (EERM); and as shown in Figure 5, the next Project's step is to select and classify the sets of Factors in the FMS [15].

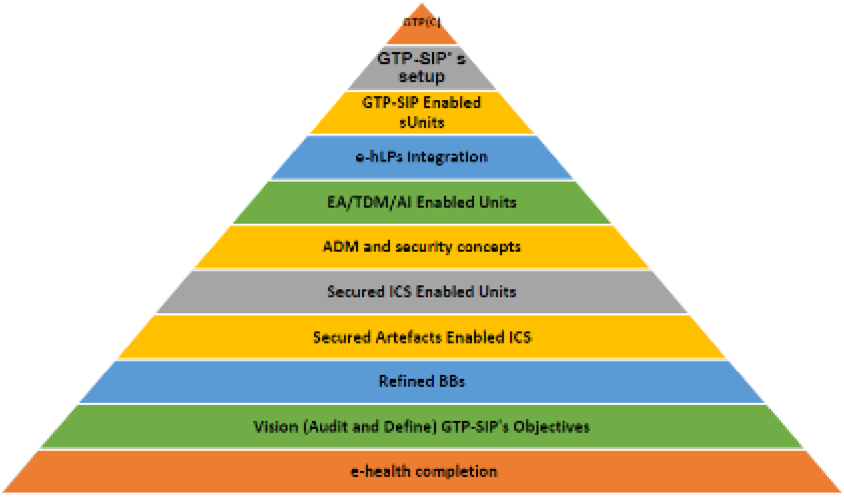

GTP(C)
GTP-SIP' s setup
GTP-SIP Enabled sUnits
e-hLPs integration
EA/TDM/AI Enabled Units
ADM and security concepts
Secured ICS Enabled Units
Secured Artefacts Enabled ICS
Refined BBs
Vision (Audit and Define) GTP-SIP's Objectives
e-health completion

Figure 5: *e-health*'s evolution.

The PRWC evaluates Factors and interfaces *Intelligence;* where *Intelligence's* requests are served by the IHITF as shown in Figure 6. KPIs are linked to concreted VARs [16,17,18,19]. RDPs' phases are: 1) Phase 1 (represented in CSA Decision Tables, CSA_DT), forms the empirical part of the RDP, CSA_ DTs check CSAs; and 2) Phase 2, tries to solve a concrete problem by using the HDT and PRWC.

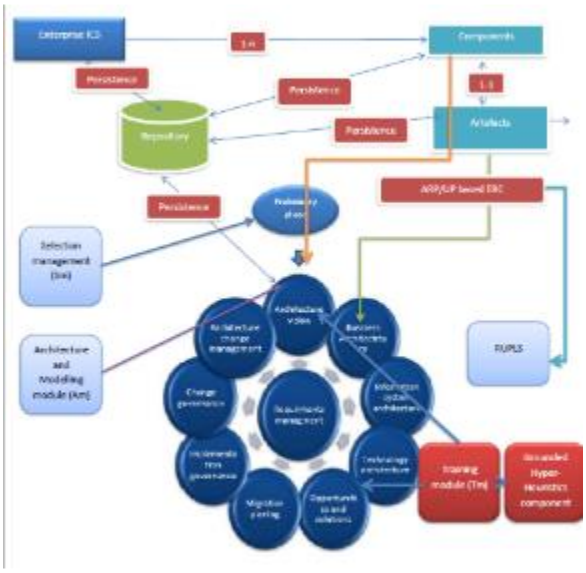


Figure 6: *The e-health* and FMS' integration with the RDP [20,21].

2.5. The PRWC an IHI Solution

This section explains the internal PRWC and Weightings (WGT) [22] that are a part of TRADf (or any IHITF), knowing that a Project can use also external products or concepts. or it can use an external commercial product. There are various ways on how a Project can use a generic PRWC. An GHS can use a standard PRWC or like in the case of TRADf, it can build its own one. TRADf's PRWC proposes the following rules:

- Sets up and initializes the CSA_DTs.
- The weighting for each CSA is CSA_WGT ϵ { 0.00% … 100.00% } which is a floating-point value/percentage values, which are derived from CSA_DT as one CSA_DT and a set of CSFs).
- The selected corresponding weightings to CSF ϵ { 1 … 10 } are fixed integer values.
- The selected corresponding ratings to CSF ϵ { 0.00% … 100.00% } are floating point percentage values.
- A weighting is defined for each PRWC CSF, and a rating for each KPI.
- The selected corresponding ratings for a KPI is KPI_RAT ϵ { 0.00% … 100.00% } and is derived from: 1) An ICS application/module VARs; 2) Estimated by the IHITF or a domain specialist; or 3) An external concept.
- CSA_WGT = ∑CSF*CSF_WGT.
- CSF_WGT = ∑KPI*KPI_RAT.
- KPI_RAT = ∑VAR*VAR_RAT.

2.6. PRWC Interfacing the System

It interfaces the system by:

- The *M-Model* applies the HDT, which uses the PRWC.
- PRWC (Project-iteration i) = ∑CSA*CSA_WGT.

- The *M-Model* applied a research mixed model, which uses a PRWC.
- *The e-health* uses the HDT which is mainly qualitative method and has specific calls to quantitative methods.
- Can use external solutions.

2.7. PRWC External Solutions

The PRWC can use standard solutions like:

- The Object Management Group's (OMG) [23]: 1) The DMN to support CSA_DTs' evaluations; 2) For implementing business decisions and business rules; and is optimal for Project's status checking; and 3) For HDT's operations.
- The weighted criteria matrix that supports: 1) *Intelligence* to evaluate Projects; and is based on the evaluation criteria (that has weighted by ratings). By evaluating alternatives based on KPIs with respect to defined criteria; and 2) A decision-making module that evaluates projects based on defined evaluation criteria weighted by ratings. By evaluating alternatives based on KPIs with respect to individual criteria [24].

And such complex PRWC needs the EERM as central research methodology.

2.8. EERM's Integration

The EERM is optimal for Projects' oriented RDPs and the HDT (which is a mixed-research) [16,17,18,19], and it includes: 1) A heuristics-reasoning approach; 2) Quantitative Analysis for PRWC (QNT4PWRC); 3) Qualitative Analysis for PRWC (QLT4PRWC) that is mainly based on the HDT; and 4) The RDP and GTP-REHPSI based *e-health's* feasibility [16,17]. The EERM checks if outcomes are acceptable and in such engineering initiatives (a PoC is a software prototype) tests the RQ by using its Factors (or independent variables) are processed to evaluate returned effects on these dependent variables. *e-health*'s author's related works are:

- A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-The role of transformation managers in organizational engineering [1].
- Enterprise Transformation Projects-The Role of Enterprise Architecture in Implementing a Holistic Security Refinement *e-health* (ETP-HSC) [2].
- Enterprise Transformation Projects-The Role of The Polymathic Security Learn Processes (ETP-RPSLP) [3].
- The CCHI/ SHIB Project [4].
- The Holistic Brick based Architecture for SHIB [5].
- An Intelligent Microartefact Patterns' based Architecture for SHIB [6].
- Business Transformation Projects-The Role of a Transcendent Software Engineering *e-health* (RoTSEC) [26].
- Business Transformation Projects-The Role of Requirements Engineering (RoRE) [27].
- Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basic Construction [28].
- Integrating Holistic Enterprise Architecture Pattern-A Proof of *e-health* [29].
- A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Project-Intelligent atomic building block architecture [30].
- Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-An Information System's Atomic Architecture Vision [31].
- Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process [32].
- Organizational and Digital Transformation Projects-A Mathematical Model for Enterprise Organizational Models [33].
- Organizational Transformation Projects-The Role of Global Cyber Security and Crimes (RoGCSC) [25].
- Using Applied Mathematical Models for Business Transformation [20,21].
- Applied Holistic Mathematical Models for Dynamic Systems (AHMM4DS) [12,13,14].
- Various Polymathic articles that support GTP-REHPSIs [3,10,11].

A GTP and *e-health* are complex and that causes resistances and hence XHFRs failures, to avoid such XHFR the Project needs to implement Transformation Readiness Checks (TRC).

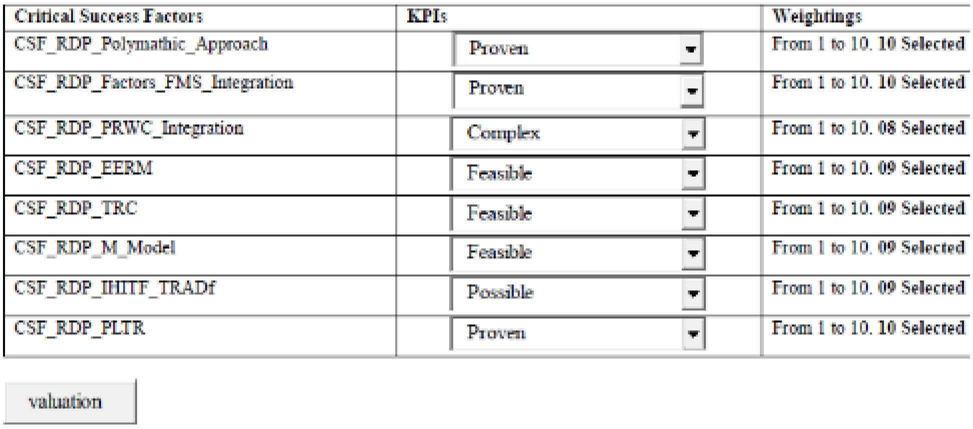
2.9. The TRC

Project's lack of Polymathic concept and related complexities' management are XHFRs' origins, and many sources confirm such facts, like *The Chaos Report*, edited by the Standish Group assert that: … *only about 29% of transformations come in on time and budget*… [34,35]. IHITF's TRC enables [36]:

- *Business Transformation Readiness Assessment* capacities.
- TDM's management and executions.
- *e-health* capacities and feasibility.
- GTP-REHPSI accumulates experiences and persisting in e-hLPs.
- Use an IHI Methodology, Domain, and Technology Common Artefacts Standard (MDTCAS).
- Gap Analysis (GAPA) to avoid Project's deviation.

2.10. PRWC RDP's CSFs

Table 1: This CSA has the average of 9.25.



Critical Success Factors	KPIs	Weightings
CSF_RDP_Polymathic_Approach	Proven	From 1 to 10. 10 Selected
CSF_RDP_Factors_FMS_Integration	Proven	From 1 to 10. 10 Selected
CSF_RDP_PRWC_Integration	Complex	From 1 to 10. 08 Selected
CSF_RDP_EERM	Feasible	From 1 to 10. 09 Selected
CSF_RDP_TRC	Feasible	From 1 to 10. 09 Selected
CSF_RDP_M_Model	Feasible	From 1 to 10. 09 Selected
CSF_RDP_IHITF_TRADf	Possible	From 1 to 10. 09 Selected
CSF_RDP_PLTR	Proven	From 1 to 10. 10 Selected

Based on the *M-Model*, PLRP, GAPA, and *Intelligence*, this CSA's CSFs/KPI were evaluated with the PRWC and the results are shown in Table 1 (or the 1st CSA_DT). This CSA's result of 9.25, which is high and that is due to the fact that the RDP's and TRADf's maturity [32]. As the RDP's CSA_DT presented positive results, the next CSA to be analyzed is the Project's Overview that is this article's ACS that is based on Automated *e-health* System (AeS).

3. The Project Overview

3.1. The AeS

The French GHS is based on a fully AeS, whose national holistic regulatory framework is definitely the best worldwide and that forces similar players to improve their e-services. This fact is based on the comparison of leading global AeS; and France's GHS has an absolute lead in all verified domains. A French citizen has the right on an e-card Vitale as shown in Figure 7, that gives basic rights in the *e-health* system. France's GHS and related social system that is based on humanistic values leaves nobody in desperate situations [37]. Because of France's

GHS and *e-health* system, the KSA decided to test its adaption and initiated SHIB project that is this article's CSA.

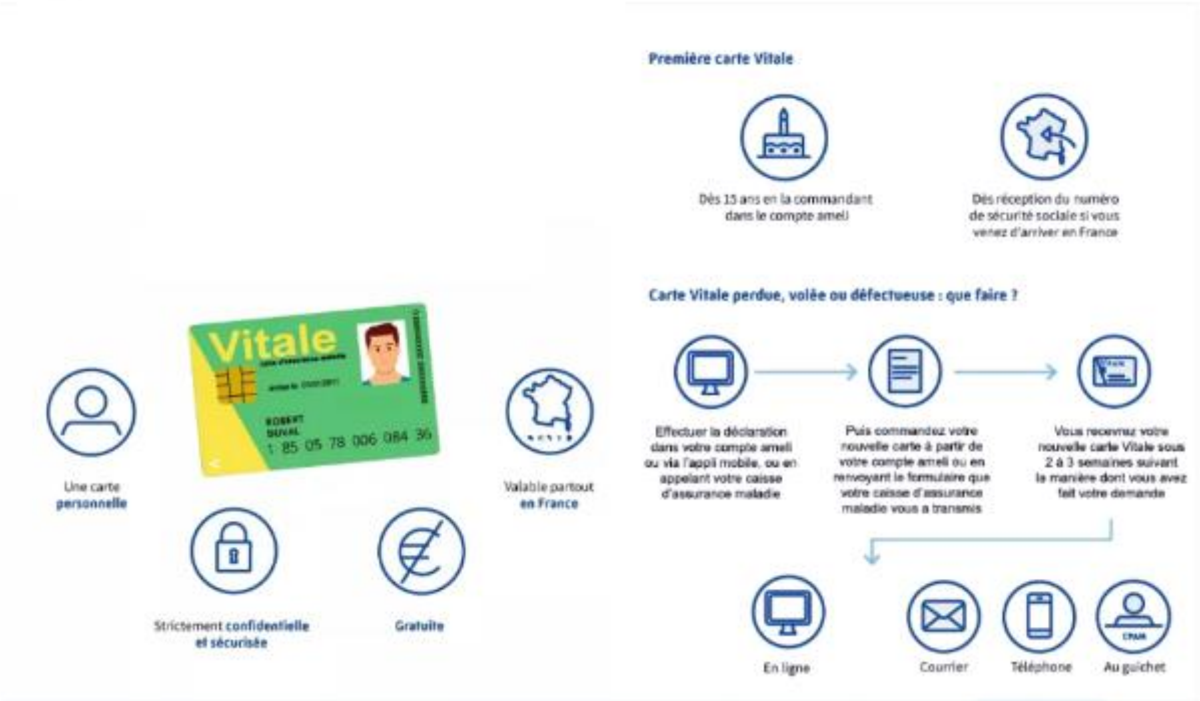

Vitale
ROBERT
DUVAL
1 85 05 78 006 084 36
Une carte personnelle
Valable partout en France
Strictement confidentielle et sécurisée
Gratuite
Première carte Vitale
Dès 15 ans en la commandant dans le compte ameli
Dès réception du numéro de sécurité sociale si vous venez d'arriver en France
Carte Vitale perdue, volée ou défectueuse : que faire ?
Effectuer la déclaration dans votre compte ameli ou via l'appli mobile, ou en appelant votre caisse d'assurance maladie
Puis commandez votre nouvelle carte à partir de votre compte ameli ou en renvoyant le formulaire que votre caisse d'assurance maladie vous a transmis
Vous recevrez votre nouvelle carte Vitale sous 2 à 3 semaines suivant la manière dont vous avez fait votre demande
En ligne
Courrier
Téléphone
CPAM
Au guichet

Figure 7: The fully automated French AeS.

The French GHS has demonstrated its humanistic principles during the latest massive pandemics (COVID-19) which has inflicted immense damages worldwide and especially in Western countries but also shown some Western countries real values. In the West, France's humanistic and solidary approach was more than evident and had imposed strict confinements, massive spendings, and the mobilizations of its efficient public sector/population, which makes France the best and real Humanistic Democracy (HD). But there were very astonishing and unhuman Materialistic Democracies (MD) or money-first attitudes, sere the so-called Nordic/Swedish, and Swiss approaches, in which very little was done, and has left people to their own fate and especially homeless, poor, migrants/foreigners… Knowing that North-Europe/Sweden and Switzerland praise themselves for a high standard of their GHSs, standards, and equality, but when it comes to finance (or money), then MD's GHSs seem to forget the humanistic part of medicine. In this major crisis Western corporations (except France) have made trillions of USDs in massive profits; and many companies and individuals have multiplied their richness, mainly because they have absorbed the largest part of the public spending. The COVID-19 crisis is a major test for multilateralism and there is a need for a humanistic approach to support the poor. And of avoid that countries (like North Europe/Sweden and Switzerland) and companies (mainly consulting) get richer who gained trillions and avoided to pay taxes. This all comes at the same time with massive immigrations waves, and climate change [37,38,39]. These make the French GHS and its *e-health* approach very credible and even a reference for health transformations, like SHIB.

3.2. The ACS-The SHIB project

The KSA wanted to develop its GHS with CCHI's management and GHS' vision included the design a model of *e-health* which:

- Conforms to the highest international standards for quality and security.
- Strengthened the health care services, which will be patient-centered, and secured.
- Offers interoperability of its e-services, in order that a person's health data is available to GHS' professionals and healthcare establishments.
- Enables the transfer of patients between GHS Units.
- Manages spendings and better financial controls.
- Global e-services inter-action.
- Manages massive health information and flows.
- Offers a secure technical and software infrastructure.
- Supports the evolutions in health e-service.
- Supports the design, integration, and operations of SHIB.
- Implements a Main Data Center & Disaster Recovery site.
- Monitors GHS' insurance industry with high efficiency from the medical and financial perspectives.
- Establishes healthcare statistical reports.
- Professionally manages Project's phases.

3.3. Project's Phases

The Project's and *e-health* phases are:

- Development: includes the design and development of sICS solutions.
- Business Process (BP) Outsourcing: Concerns customer, processing on its behalf its BPs.
- Network: The creation, organization and management of diverse partners (service providers, health professional, publishers, etc.).
- Software as a Service (SaaS): The legacy ICS is unbundled in e-services, which are recomposed in e-health BPs.
- Management of information and associated e-services: To design added value e-services.
- Security infrastructure and digital confidence: To offer rusted security infrastructure to support high volumes of sensitive information in real time.

3.4. GTP-REHPSI Main Objectives

GTP-REHPSI's main objectives are:

- Physical security, where the main aim was to offer high level of security that includes GHS' physical security and to ensure compliance with established references that lay down general security requirements (like the ISO 2700X series of standards…).
- The sICS is managed by an RSSI (Information Systems Security Manager).
- Security and physical safety are managed by the Physical Security Manager (Security Officer).
- Video surveillance and access control by contactless badge or Biometric access control.
- The protection of personal that includes: 1) Respecting Freedoms; 2) Conformity and risk management; 3) Build sICS skills; 4) Enforce legal controls.
- Supporting the Insurance Management Services (IMS) that supports: 1) Send messages over the network; 2) Validate Health Practitioner Status; 3) Claim supporting document services management; 4) Raise Complaint services management; 5) Tracking Complaint Services; 6) Reporting Fraud services; and 7) Detecting Fraud / Misuse service; and 8) Generating Reports Service.

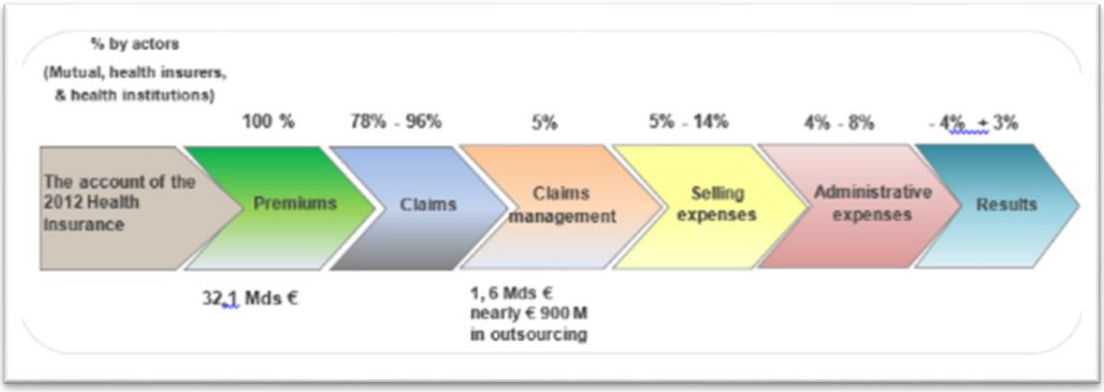


Figure 8: The Evolution of *e-health*.

The evolution of the French GHS care reimbursements in 2012 was € 16 billion, € 900 million as shown in Figure 8. That needs special sICS solutions.

3.5. sICS Solutions' Overview

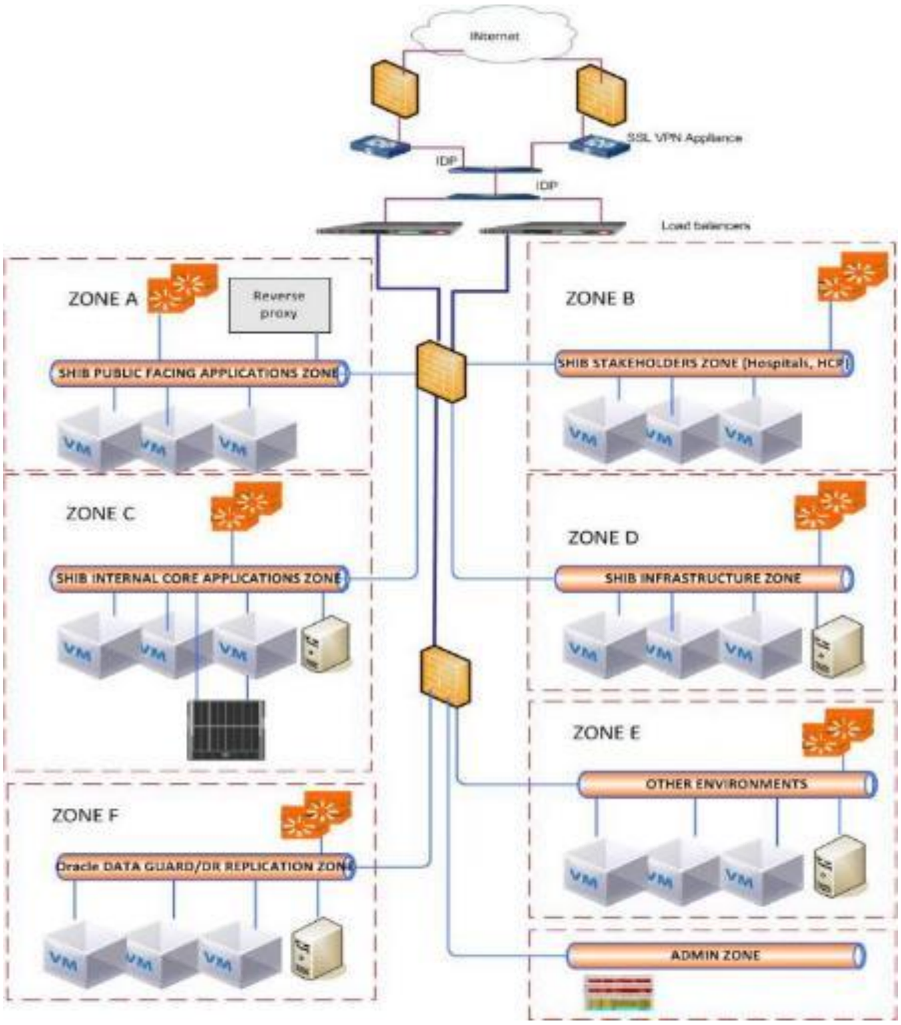


Figure 9: *e-health* sICS security zones.

In *e-health* sICS data and processes grow exponentially both in volume and in quality, and therefore the importance of effective sICS processing, which needs well-designed and managed, mostly in the AeS sector, where the sensitivity of information is a fundamental parameter and the capacity to synchronize information and actions between various players. *e-health's* e-services support: Third-party payments, GHS' Data management, detecting fraud, Data-flows management, High-level of security, Optimizing costs, Invoices' management, Value-added services. These e-services are integrated in BPs to ensure uninterrupted chain of trust (information, flow, delimiters…). The GTP-REHPSI allows the relevant integration of, in response to the *e-health's* domain developments, to support sICS':

- Connectivity: 1) To federate actors of the global healthcare sector with an enhanced technical flexibility and reliability; 2) Manages a network of partners (healthcare professionals, insurers, health institutions); 3) Interconnects pharmacists, hospitals, insurers, practitioners, health care institutions, specialists, governmental organizations; 4) Manages the identification and authentication of these actors, the access rights to the services and the flow of information including the reimbursement of healthcare costs; 5) Establishes a robust link between health-care professionals and a central sICS; 6) The health-care professional performs medical processes which are precisely defined in the fee structure with a control of the insurance schemes.
- Interoperability: 1) The solution is interoperable and applies data standards; 2) Data processing with remote sICS; 3) Supports HL7 standard based solutions; 4) Offers BBs to interface publishers to support health professionals' business needs; and 5) An operations team to support customers in real time.
- Capability, scalability, and Auditing: Implementing control rules requires specific workflows to detect suspicious activities. A suspicion activity is identified by monitoring and will be implemented by Business Process Management (BPM) and supports: Detecting by a user or an operator; Validating the fraud by authorities; Configuring the fraud detection rules; Executing detection rules; and Reporting detections in real-time by the monitoring systems.
- Defines adapted security zones as shown in Figure 9.

3.6. The Security and Operations Concept

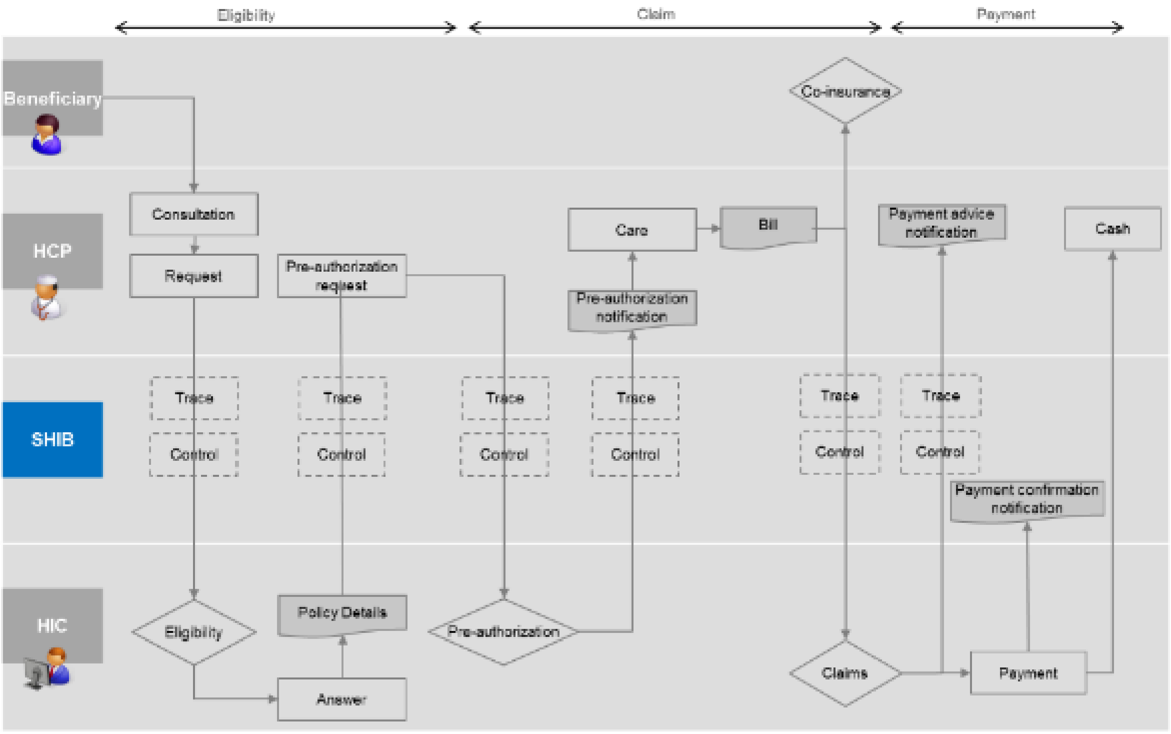


Figure 10: *e-health* main e-services.

e-health security and operation concept include, as shown in Figure 10:

- A security infrastructure capable of managing huge volumes of sensitive data/information, in real-time, which can be duplicated.
- Has a pool of e-services capable of managing data/information supplier's identity, their traceability and access permissions.
- Guarantees data integrity, confidentiality, retention, and trusted third party.
- Through our expertise in the management of sensitive information, we have developed a remote medicine platform aimed at strengthening the monitoring of patients with chronic diseases…
- An expert system that supports monitoring and the coordination of patients…
- Patients are equiped with sensors connected to the GHS.
- Scalable technical that supports TDM/Business architectures and to respond to massive requests…
- Secured integration of external partners, evolution of users and patients' profiles.
- Evolution of spaces like workplace, webhosting.
- Supports messages exchanging between: GHS and Health Care providers and Health Care financers….
- Messages are HL7 based and can be collected, traced, and processed.
- Control exchanges include: Eligibility, Claim, Payment, messages (associated with same medical treatment/service).
- Infringements (regulatory or fraudulent) are Persisted in specialized stores.
- Security includes the following components: 1) The PKI that handles the lifecycle of the X 509 certificates; 2) The IAM that is used to configure access to all e-health's components; 3) The LDAP responsible for storing of information on individuals, groups or entities; 4) The Security Information and Event Management (SIEM) is for aggregating and correlating security events, used for generalized supervision of security for the project.

Identity and Authorization Management (IAM) manages the lifecycle of users/patients and access control throughout the GHS for any e-service. To support the isolation of roles, *e-health* is based on the principle of the least privilege. Users' management uses authentication that is managed by a central authentication server. Identity is looked up in the repository to retrieve the user roles and data/information. A user can access *e-health* using a personal login/password. In order to give an increased confidence to authentication process, the service can provide for future needs a wide range of authentication method within strong authentication. Business to Business (B2B) partners have certificates and a private key to ensure the confidentiality and the authentication of any exchange with the Project. Non-repudiation is also covered with the digital signature and archiving of every transaction with the Project. We chose to implement a fine-grained model of authorization which is built around a Role Based Access Control (RBAC) rather than a Discretionary Access Control which would not fit the required need of traceability and policy enforcement. The chosen IAM service, supported by Oracle Identity and Access Management, is a user centric component which enforces compliance by mandatory logging and auditing of requested authentication and access. The authorization mechanism used allows giving fine grain access to data or functionalities.

3.7. Claim Management Service and Payment Management Service

e-health enable the Heal Care Providers (HCP) to send a claim by using e-services; and the system returns payment notifications service. The payment notification, the claim payment, the pre-authorization as well as the eligibility request will all be grouped into a same insurance claim record to keep e- transactions' coherence. As shown in Figure 11 the BP is designed using a Business Process Management (BPM) environment. The scheme is illustrative to show how the process would be designed in the solution, using BPMN 2.0 standards. The Integration of BPMs is supported by the Services Oriented Architecture (SOA) which allows the mapping of native BPs and e-services. BPMs use Enterprise Service Bus (ESB) for intra GHS communications.

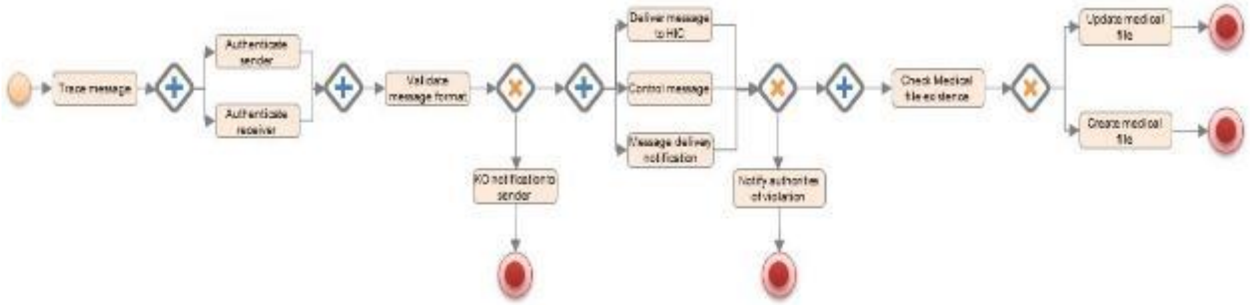


Figure 11: e-service supports BPs.

3.8. The Role of EA

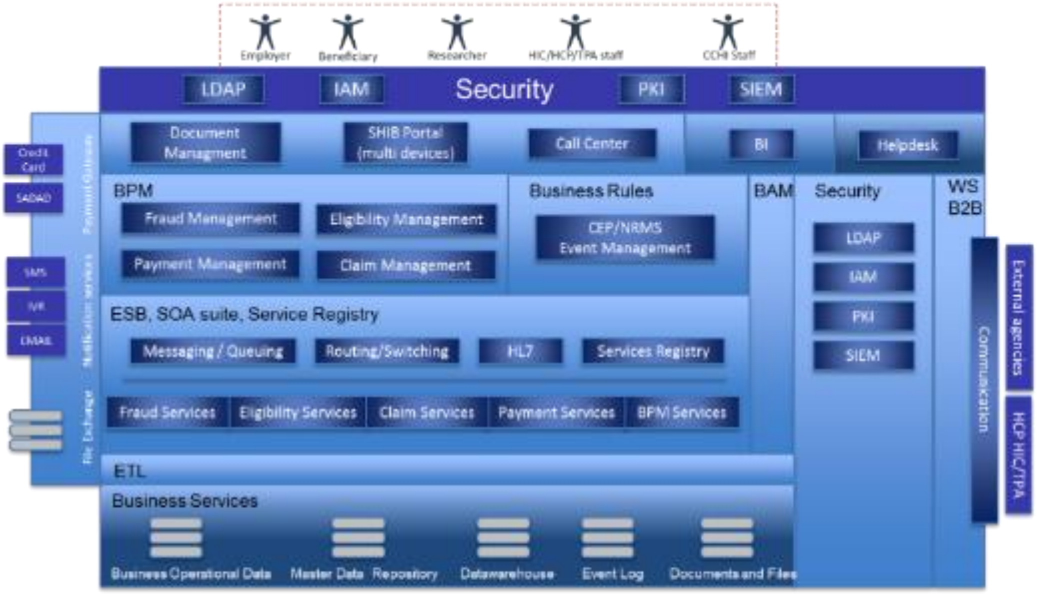


Figure 12: EA’s logical view.

e-health’s EA and especially Business Architecture (BA) satisfies Project’s requirements using BBs needed for the following BA/functional domains as shown in Figure 12, which is considered a logical view and that includes:

- Operations: Supports the exchange of HL7 messages to manage eligibility, claims, payment monitoring and e-services.
- Configuration: Provides sICS administrators capacities to manage BPMs, BP rules/events, and file-exchange.
- Distribution: Is ensured by a front-end/portal, B2B exchanges supported by web-services, Contact-center, Management of BBs, and Management of authentication/authorization
- Management and auditing offers: Real-time monitoring using Business Activity Monitoring (BAM); Statistical reports and retrospective analyses using Business Intelligence (BI).
- Support: For logging, monitoring and solving requests/complaints.
- BPMs (BPMN2) are heavily used and are related to BAM and BI environments. BPMs are main EA’s components; and their topology is based on: 1) GHS’ e-services with DataBase (DB) accesses; 2) BA-services which incorporate BPs and data; 3) BP services which stored in the BPM system (BPMS).
- The BAM includes: 1) Monitoring and regulating technical activities on the service-bus; 2) Detecting

thresholds (like fraud); and 3) Loss of connectivity.

- e-services registry is a catalogue containing information (like versions and other) on the internal/external services to be used by *e-health*.
- The EA Repository: That is supported by TOGAF, ArchiMate, BPMN… EA's artifacts persisted in a repository with a secured interface that enables: Business analysis; Solution/Application modelling;

ESB exchange include: 1) File-exchange platform to exchange information via a secure channels; 2) e- services for B2B which provides inter-applications communication; 3) Notifications' management of emails or SMS; 4) Payment solution provides the integration with local payment systems; 5) ETL is used for file exchange e-services; 6) Databases are used like: Operational to processes operational data, such as health system data, reimbursements…; Repository contains data on the medical centers, insurance companies, health practitioners…; Journals that contain all the events met throughout the system; Data-warehouse is all the data aggregated from the other databases…; Documentation contains all the e-health's documents.

3.9. The Role of Standards-HL7

e-health's HL7 was selected for messages' management and that stems from the HL7's domain Financial Claims & Reimbursement (FICR) that supports the following scenarios: 1) A storyboard like request; and 2) Offers a development methodology that adapts to targeted *e-health* requirements. In both cases, the GTP-REHPSI uses a message framework that supports all types of interactions and a referential model, as shown in Figure 13.

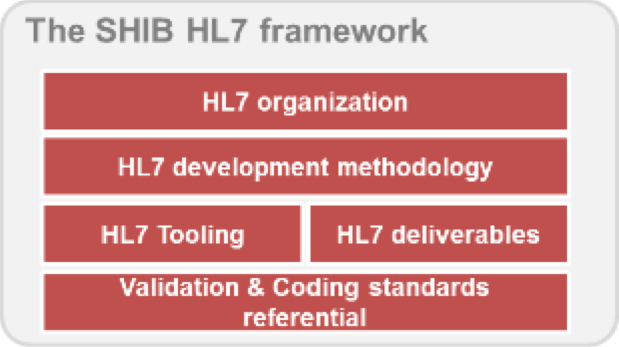

The SHIB HL7 framework
HL7 organization
HL7 development methodology
HL7 Tooling
HL7 deliverables
Validation & Coding standards referential

Figure 13: HL7 referential model.

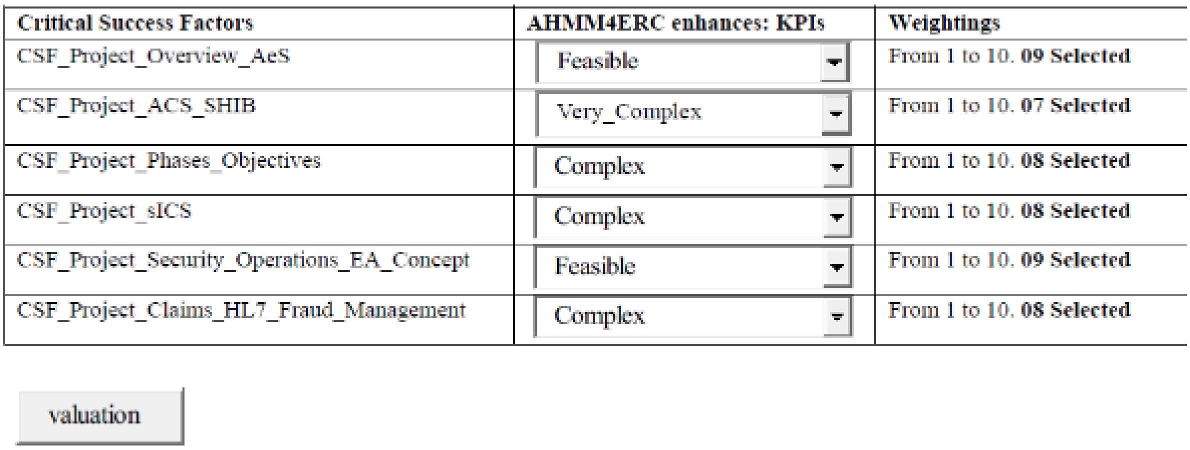
HL7's structure is based on 1) The portability of its organization (localization) to must comply with the framework established by the HL7 Technical Committees); and 2) KSA's HL7 Affiliate Organization must adopt it with its existing standards. Knowing that HL7 environments use message development methodology that is based on eXtensible Mark-up Language (XML) schemas.

3.10. Detecting Abusive and Fraudulent Accesses

e-health enables the detection of Suspicious accesses usages are treated in a validation flow. Review of validation processes, includes Checking components, Authority checking, Validation given by a manager, Configuration of control, Stakeholders are notified b of their actions, Fraud is notified in real-time; Use BI to detect fraud.

3.11. Project's Overview CSFs

Table 2: This CSA has the average found 8.15.



Critical Success Factors	AHMM4ERC enhances: KPIs	Weightings
CSF_Project_Overview_AeS	Feasible	From 1 to 10. **09 Selected**
CSF_Project_ACS_SHIB	Very_Complex	From 1 to 10. **07 Selected**
CSF_Project_Phases_Objectives	Complex	From 1 to 10. **08 Selected**
CSF_Project_sICS	Complex	From 1 to 10. **08 Selected**
CSF_Project_Security_Operations_EA_Concept	Feasible	From 1 to 10. **09 Selected**
CSF_Project_Claims_HL7_Fraud_Management	Complex	From 1 to 10. **08 Selected**

Based on the *M-Model*, PLRP, GAPA, and *Intelligence*, this CSA's CSFs/KPI were evaluated with the PRWC and the results are shown in Table 2 (or the 1st CSA_DT). This CSA's result of 8.15, which is a limit value, that is due to Project's complexities. As the RDP's CSA_DT presented results, the next CSA to be analyzed is the Project's Security Overview.

4. Project's Security Overview

4.1. The Role of Security Basics

e-health's interfaces existing market standard frameworks like: 1) EA (like TOGAF) which can support GTP-REHPSIs [41]; 2) An IHITF and associated MMs like the proposed *M-Model* [8,9]; 3) Unbundling *GHS's* resources, security mechanisms, and e-services pool [41,42]; 4) AI domains for *e-health* [43,44]; 5) A scalable sICS and an agile group work support [45]; 6); Problem solving concept that is supported by *Intelligence*; 7) Sherwood Applied Business Security Architecture (SABSA) like environments [46]; 8) The Committee of Sponsoring Organizations of the Treadway Commission (COSO); and many others. The User Management Service (UMS) integrates IAM, which supports: Authentication, Authorization, Access control, Access rights, Entitlements, Access delegation and User Lifecycle Management (ULM) operations. The relation with the SIEM and RBAC services that ensures that illegal actions are detected and traced. Based on Enterprise Manager, the global architecture integrates a Role Based Access Control within every component used. Security-monitoring is based on SIEM that aggregates sICS' logs alerting security-relevant warnings.

4.2. Public Key Infrastructure (PKI) Servers (PKIS) and External Frameworks

e-health's PKI solution is based on leading PKI products as shown in Figure 14.

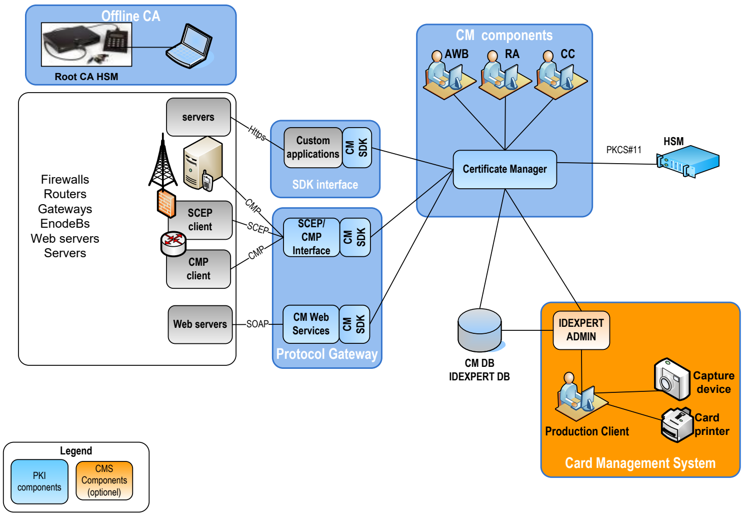


Figure 14: PKI solution for *e-health*.

The PKI solution is flexible and modular with each component performing a single task within the system. Key features and benefits of the proposed PKI solution include: Zero footprint, Flexible and modular, Extensible, Standards-based, High capacity, and High availability. That can be supported by the IBM Security Framework (IBMSF) that is shown in Figure 14.

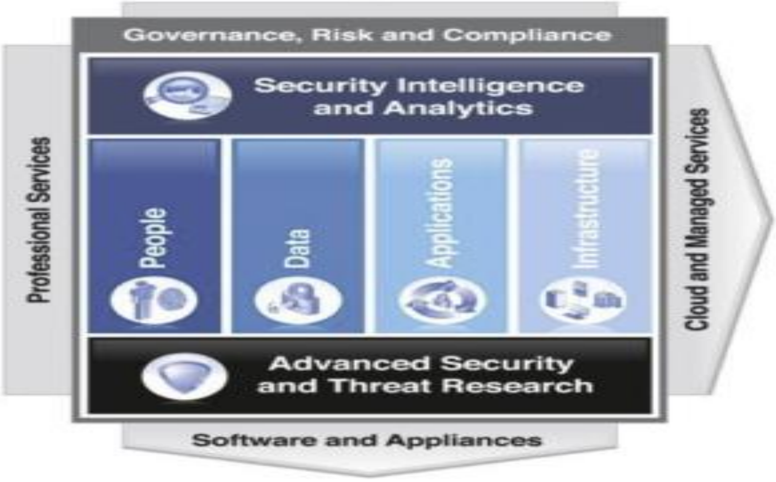

Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Software and Appliances
Professional Services
Cloud and Managed Services

Figure 15: IBMSF's Structure.

As shown in Figure 15, IBMSF defines *e-health* security strategies, architectures, and is used for developing solutions that can be secure from the initial phase. Governance is GTP-REHPSI's strategic phase and uses IBMSF that offers guidance to all Project's phases. The IBMSF manages GTP-REHPSI/security Critical Risks (GCR) end-to-end across the GHS. ISF supports the GCRs to: 1) Trace and prioritize risks; 2) use holistic flexible infrastructure; 3) Solves security problems; 4) Detects vulnerabilities, attacks, viruses and other malware, spam, phishing, web- threats, and Cybercriminal activities; 5) Governance and compliance; 6) Security based

Intelligence and analysis; 6) Human factors; 7) Applications and data/information; and 8) Supporting infrastructure. The GTP-REHPSI supports the following views: Business**,** Technical, and Solution Architecture. And principles: Defense in depth, Auditability, least privilege, and Security is model driven.

4.3. Encryption's Basics

e-health's encryption is used in the following activities: Traffic, Field, Message, Database, and System-wide. GTP-REHPSI sensitive information stored in encrypted DB using Transparent Data Encryption (TDE) it offers the masking the use of encryption for *e-health's* applications. *e-health's* encryption must respect performance criterias and information privacy. The TDE manages sensitive data and are also encrypted. This procedure has the advantage of masking the use of encryption for the applications and guaranteeing fine grained encryption. The reason why encryption is not solely implemented at a system wide level is to offer the best performance while making no compromise on information privacy. Particular attention has been paid to avoiding a conflict of interests between security administrators in charge of the keys and system administrators which have access to the data. Here also the tools provided by Advanced Security Options can be used to only authorize database administrators to carry out maintenance and tuning without giving read rights on all or part of a database table. The PKI solution is flexible and modular with each component performing a single task within the system. Key features and benefits of the proposed PKI solution includes: High availability; Physical security service; Host and endpoint security service; and Secured endpoint protection.

4.4. *The Role* of Security Monitoring

e-health's proactive monitoring supports proactive monitoring service with the goal is to detect the fault before the customer does and then to notify the customer proactively informing of the fault. As shown in Figure 16, proactive surveillance and monitoring inputs: 1) Proactive monitoring; and 2) Standard e-services.

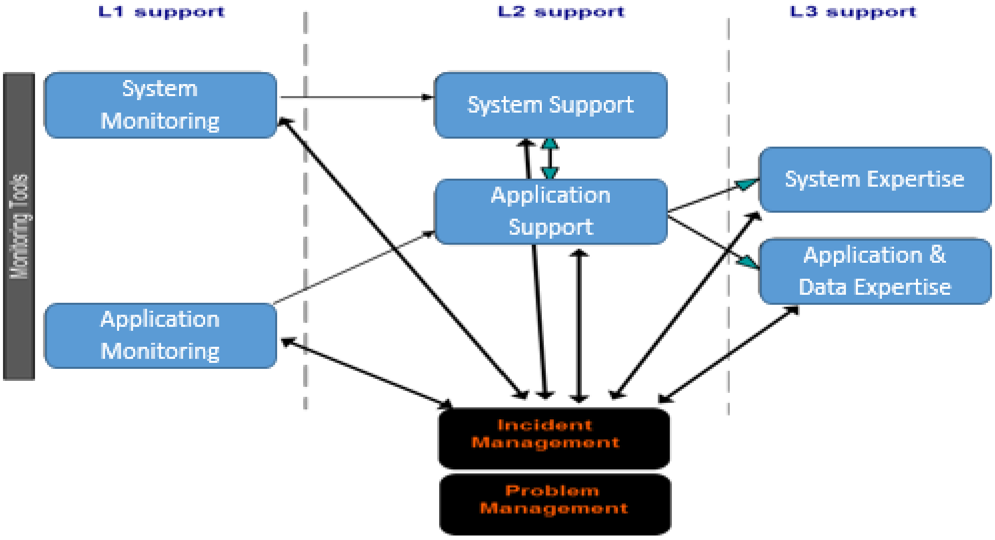


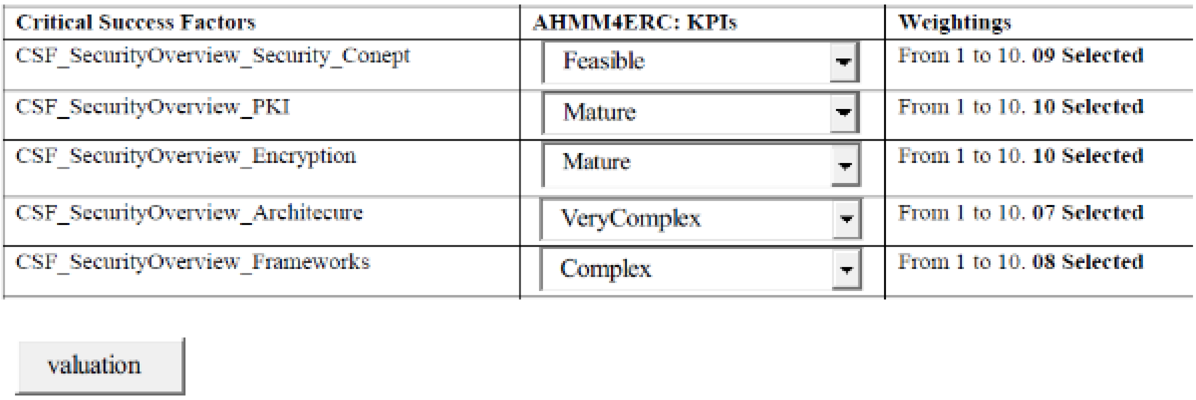
Figure 16: Monitoring and support.

The goal is to 'detect' the incident before SHIB customers does and then to notify SHIB customers proactively informing of the security incidents. Security Incidents: 1) External security breach like: Denial of Service attacks

(DOS); and 2) Internal security breach, like a virus that is generating large volumes of traffic. Impact analysis includes: 1) Capture the impact of the change; 2) The dependency and the relationship of the configuration items; and 3) Impact on affected resources.

4.5. Security's Overview CSFs

Table 3: This CSA has the average of 8.80.



Critical Success Factors	AHMM4ERC: KPIs	Weightings
CSF_SecurityOverview_Security_Conept	Feasible	From 1 to 10. **09 Selected**
CSF_SecurityOverview_PKI	Mature	From 1 to 10. **10 Selected**
CSF_SecurityOverview_Encryption	Mature	From 1 to 10. **10 Selected**
CSF_SecurityOverview_Architecure	VeryComplex	From 1 to 10. **07 Selected**
CSF_SecurityOverview_Frameworks	Complex	From 1 to 10. **08 Selected**

Factors were evaluated with the PRWC and the results are shown in Table 3. This CSA's result of 8.80 which is satisfying, that is due to mature external security products. As this CSA_DT presented satisfying results, the next CSA to be analyzed is the Project's architecture that is this article's ACS.

5. Project Architecture and Setup

5.1. EA and the Role of e-services

e-health's s and Projects in general need an organizational engineering phase that is based on standards, mapping concepts, modelling technics, and interoperability. EA standards and methodologies support Projects, to become part of the global *e-health* system. XHFRs makes it difficult to follow frequent changes and this fact might cost GHS a lot. A well-planned *Project* is based on a platform of flexible e-services using e-technologies in order to attain the needed level of agility by using an GHS Engineering Pattern (GEP) without incurring high production, maintenance and implementation costs [7,15]. The GTP requires the knowledge of a large set of technologies and methodologies. Adapting just the underlined technologies is not enough and the main problem arises due to lack of business systems' agility. Such an agility approach, as shown in Figure 1, can be built on basic elements called microartefacts [1,8]. GTP changes depends on refactored e-services that includes [30,31]: 1) The interfaces to different services' standards; 2) The e-services based architecture; and 3) The holistic e-services concept, as shown in Figure 17. The evolution of sICS have made Projects more robust and simplified the management of changes by using the holistic e-services concept. And today standards are well established; and they are all operational, in fact there are too many standards, and we can even talk of a standard proliferation [15,48]. The GEP uses BPMs': 1) Engineering; 2) Optimization; 3) e-services' interfacing; and 4) Monitoring. An GEP establishes a common approach to breakdown of the legacy ICS [12,13,14]. The IHITF uses EA methodologies like TOGAF, and an adapted e-services based TDM (e-TDM) which can be used for Digital Transformations (DT) [16,17].

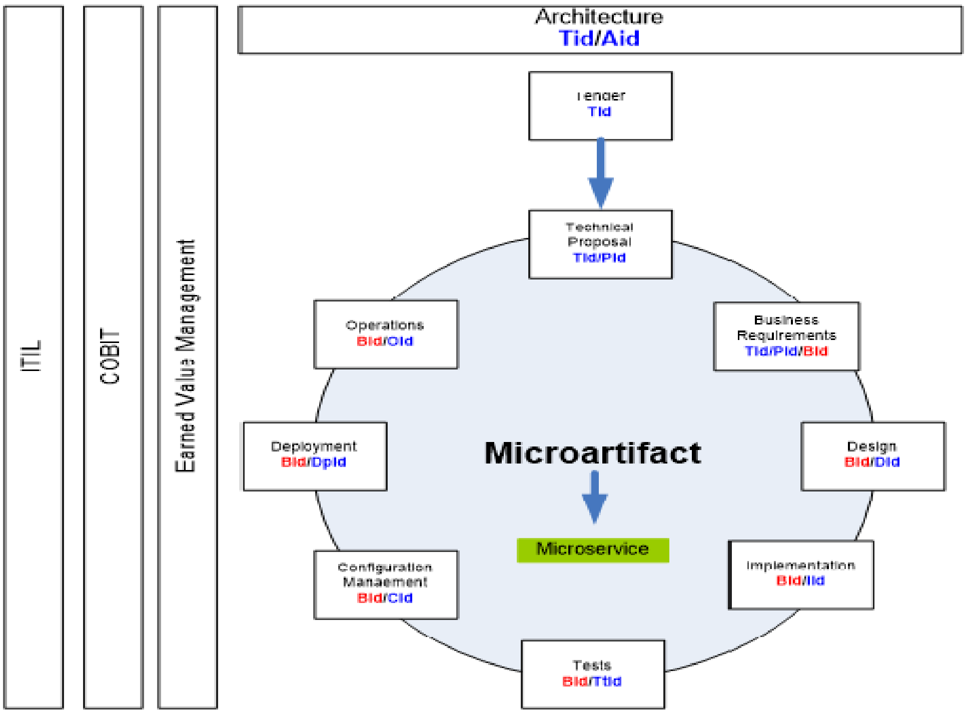


Figure 17: The holistic e-services concept

5.2. The Role of DT Strategy

Today there are many ICS and security frameworks, and they apply siloed-legacy ICS. The GTP-REHPSI and its e-health: 1) Supports the automation of a holistic security architecture, design, and integration operations; 2) Its controls uses networked secured Building Blocks (sBB) that originate from various domains like finance, governance and other; 3) It tries to detect sICS problems, financial crimes, business disruptions and corruption; and 4) Implements Cybersecurity mechanisms. Cybersecurity is responsible to avoid security related dangers and threats; and to support an sICS. To deliver an sICS, the e-health's first step is to successfully implement a DT that offers a common platform for secured e-services and resources. DTs are strategic for Projects, because they support high-adoption rate of sICS/digital technologies. DTs use TDM and secured MDTCAS (sMDTCAS) to integrate digitized Application Domain (APD) models [32,33]. An GHS must offer an all-inclusive DT based on e-health, sMDTCAS, and e-TDM.

5.3. The Role of e-TDM

e-health's e-TDM promotes the usage of existing services architectures like microservices, throughout e-TDM phases. These architecture services can be: 1) Service Oriented Architecture (SOA) and its repository [18]; 2) Building e-services based BBs; and 3) Defining Solution BBs (SBB). In e-TDM's business architecture phase includes the: 1) Mapping of GHS' structure; 2) The definition of strategic goals and objectives; 3) Refinement of *e-health* functions; 4) *e-health* data BBs; 5) BPMs and EA modelling languages; 6) Definition of *e-health* actor's roles; 7) Correlation of *e-health* and GTP functions; and 8) *e-health* data model development [12,13,14,19,20,21,26]. The GEP uses the "1:1" concept which supports: 1) Different BB types; 2) Monitoring and logging activities; 3) sICS alignment; 4) The refactoring of legacy ICS resources; 5) Aligning security requirements; 6) Integration Intelligence; 7) Implementing optimal e-TDM patterns; 8) Defining the role of secured BPMs; 9) The management of frequent changes; 10) The mapping of the e-services to other Project resources; 11) Defining the role of agile project management and FMS; and 12) e-services granularity and integration.

5.4. e-services' Granularity and Integration

e-health's e-services control concept supports the unbundling of the legacy ICS by breaking it down into a set of classified and secured e-services, and have the needed level of granularity [27,30,31]. From e-TDM's perspective a e-service can have any size and it depends on the Project's vision and how they are classified. These e-service are classified into specialized repositories, granularity depends on e-service' classification depth that in turn depends on the type of BPMs. e-services' architecture governance focuses on the life cycle of a services' architecture from its inception through modelling, assembly, deployment, management and eventually exclusion. Universal Description, Discovery and Integration (UDDI) service catalogues and BPs' metadata-repositories are integrated with the operation's Configuration Management Data Base that enables a GTP-REHPSI's platform e-services' management. The complexity lies in managing e-services and their life cycle and how to operationally monitor them. e-services' life cycle is based e-TDM's governance that defines e-services': 1) Strategy and portfolio; 2) Design processes; 3) Transition that management of change, configuration, releases, plans and tests processes; and 4) Operations management. The GEP is built on e-services' choreography that are stored in the e-TDM's continuum that includes [30,31]: 1) A unique e-services' identifier; 2) Related Project requirements to other resources; 3) Requirements capture both *e-health* and technical requests; 4) Contains an autonomous sICS solution based on e-services; 5) A e-TDM manages the development of the choreography of e-services; 6) Unifies the implementation of GEP; 6) An e-service can be an aggregation of other e-services; 7) An e-service is reusable and can be easily replaceable; 8) An e-service can have many instances; and 9) An e-service enables interoperability, integration, and mapping. Such activities have a deep paradigmatic shift in sICS, and legacy ICS are split across different nides. Stateless domain objects in the form of XML containers are an important change; this is a new transformational shift. Stateless domain objects in XML form unbundles sICS' nodes into independent BBs which interact across network. *E-health* integrates the Object Mapping System (OMS) template to support dynamic claims system [47], that all needs PEMM.

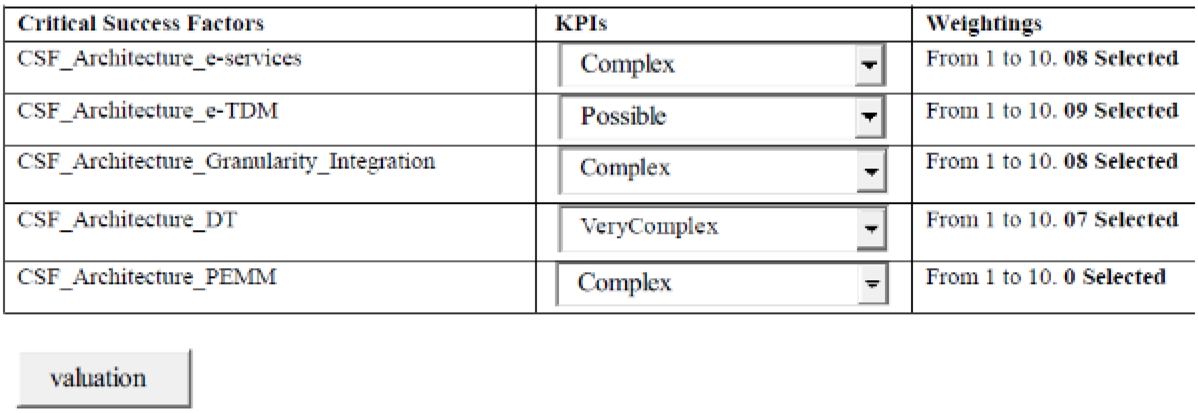
5.5. The Role of PEMM

e-health's needs a PEMM, where it is crucial for Projects and GTP-REHPSI; which might take many years to finalize. To avoid GHS locked-in commercial sICS/Security and AI products, a recommended way is to apply a Relational DataBase (RDB) based *PEMM*. An RDB-based PEMM can be implemented by using GHS' sICS/data-storage and RDB Security concepts and mechanisms; without the need for continuous massive investments in siloed-commercial products. A PEMM supports a Project, because the RDB is normally used in all sICS' and Security subsystems. RDB's primary advantage is that they contain all the essential security requirements, information, structures, integrity-checking controls, and applied MM constraints/constructs. Another possibility is to use an Asset Management (AM) based PEMM, in which a Project can use the Holistic Project Asset Management *e-health* (HPAMC) to support a PMM. The HPAMC manages and secures GHS assets that includes all its resources/assets: 1) Business cases, requirements, and processes; 2) Financial and real-estates assets; 3)

Software, RDBs, sICS components; and other types of assets. The PEMM delivers a transcendent and generic approach which is usable by the secured MDTCAS (sMDTCAS) [49].

5.6. e-TDM's CSFs

Table 4: This CSA has the average of 9.25.



Critical Success Factors	KPIs	Weightings
CSF_Architecture_e-services	Complex	From 1 to 10. **08 Selected**
CSF_Architecture_e-TDM	Possible	From 1 to 10. **09 Selected**
CSF_Architecture_Granularity_Integration	Complex	From 1 to 10. **08 Selected**
CSF_Architecture_DT	VeryComplex	From 1 to 10. **07 Selected**
CSF_Architecture_PEMM	Complex	From 1 to 10. **0 Selected**

The Factors were evaluated with the PRWC, and the results are shown in Table 4. This CSA's result of 8.0, which is low, that is due to the complex unbundling process. As this CSA_DT presented unsatisfactory results, the next CSA to be analyzed is the Project's system implementation.

6. Project's System Implementation

6.1. The SLC

The SLC is related to managing e-services related to *e-health* and the manner how to operationally trace-monitor interrelated e-services' compositions and their interaction with the GHS partners and actors. e-services can use SOA governance model that offers e-services' [60]:

- Strategy that manages the portfolio and ownership.
- Design that delivers solutions for e-TDM, sICS, and other artefacts implementation issues.
- Operations is governed with focus on keeping e-services running.
- Governance can use Information Technology Infrastructure Library (ITIL) which has the focus on sICS e-services.
- Interfacing standard security and common frameworks.

6.2. Using Standard Security Frameworks

e-health can use standard frameworks like COSO defines basic components, a common language and a roadmap for Project's GCR management. GCR's mitigation and management objectives are: 1) Strategic; 2) Operations; 3) Reporting; and 4) Compliance. And related Factors are [55]: 1) Organizational; 2) *e-health's* interfacing; 3) GCR's assessment; 4) Determining GCR's possibilities; 5) Identifying GCR responses and actions; 6) Communication of GCR results and storing them in GTP-REHPSIs; 7) Monitoring; and 8) Integrating the Digital Forensics and Incident Response (DFIR) *e-health* (DFIRC).

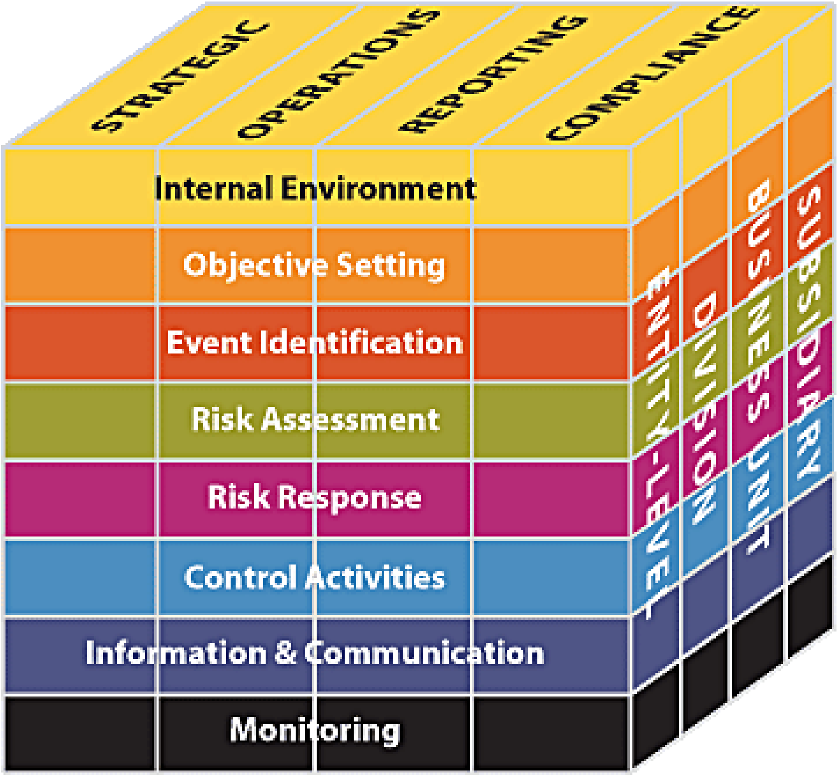


Figure 18: Interfacing the COSO framework [55].

The e-health can interface frameworks like COSO which include common components, a common language and offers a roadmap for risk-management, which modifies and enhances GTP-REHPSIs. The GHS structure depends on e-services and sICS which are used to (re)organize sUnits. *The e-health* uses sMDTCAS and e-TDM to integrate standard methodologies, like TOGAF and SABSA [46,56].

6.3. Using Common Environments Frameworks

e-health can establish a global Cybersecurity and crimes detection strategy. *The e-health* includes Cybersecurity and governance of GCRs and related Factors, which can be mitigated, to ensure GHS' global evolution and to predict (and eventually) block Cyber (or traditional) crimes/misdeeds. GHS and its partners Cyberspace's resilience, control, and security concepts are siloed, insufficient, chaotic, and concentrate only on sICS/technical-platforms' infrastructural characteristics, which can be fed in GTP-REHPSIs. GHSs are aggressed by Cybercrimes that are based on Cybersecurity weaknesses and violations that are difficult to detect. Secured Projects and hence *Entities* are very complex to secure, because of various sICS and APD problems, and they depend on the *GHS's* structure and GTP-REHPSIs management. The sICS related *Projects* use TDM's cyclic phases, which includes sUPs. Figure 18 shows sBPMs' Security roadmap, which can be integrated in GTP-REHPSIs. Using sBPMs in GTP-REHPSIs enables: 1) The reduction of GTP-REHPSIs complexities; 2) Parallel development of sBPMs using secured DevOps (DevSecOps); 3) Valuation and allocation of Security controls to sICS elements, e-services; 4) Optimizing interdependencies between sBPMs and Security controls; 5) GHS wide Security monitoring, optimization and improvement of GTP-REHPSIs using DevSecOps. [57,72]; and 6) Offering Managed Security Services (MSS).

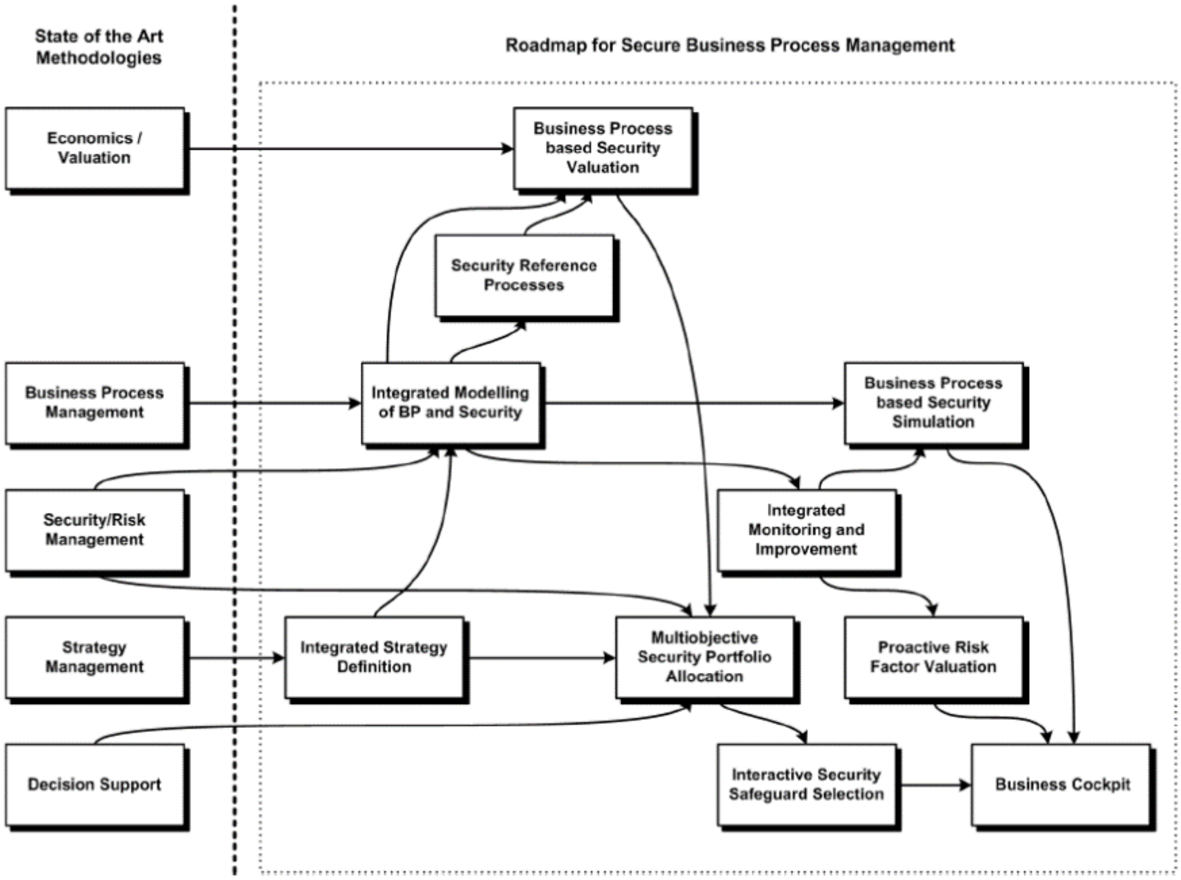

State of the Art Methodologies
Roadmap for Secure Business Process Management
Economics / Valuation
Business Process based Security Valuation
Security Reference Processes
Business Process Management
Integrated Modelling of BP and Security
Business Process based Security Simulation
Security/Risk Management
Integrated Monitoring and Improvement
Strategy Management
Integrated Strategy Definition
Multiobjective Security Portfolio Allocation
Proactive Risk Factor Valuation
Decision Support
Interactive Security Safeguard Selection
Business Cockpit

Figure 19: Roadmap for secured sBPMs for GTP-REHPSIs [57].

6.4. The MSS and SEIM

e-health's MSS and SIEM support:

- Managed firewall and IPS service(s), that offers Monitoring and managing firewalls and IPS' capability to prevent security threats.
- A single point of contact, because it provides real-time monitoring, management and customized protection capabilities.
- Interfaces frameworks like IBMSF, which analysis emerging security issues.
- Manages security information and event management to effectively identify and respond to security threats, manage compliance and other.
- 24/24 security monitoring and reporting to reduce GCRs.
- Managed information and events can: 1) Reduce complexity; 2) Manages resources; 3) Improve security and compliance management.
- Improves operational efficiency.

6.5. Professional Services and Governance

As shown in Figure 20, *e-health's professional services and governance support*

- Defines sICS policies and related standards.
- Includes audit, compliance, and reporting.
- Defines a layered model of governance, GCR management, and compliance that are aligned with sICS policies.

- sICS policies are a set of security controls which are assisted with GHS' legal and regulatory norms.
- Accumulates e-hLPs for developing different governance, GCR management, and compliance controls
- Defines security principles which are the fundamental of a robust GTP-SIP.

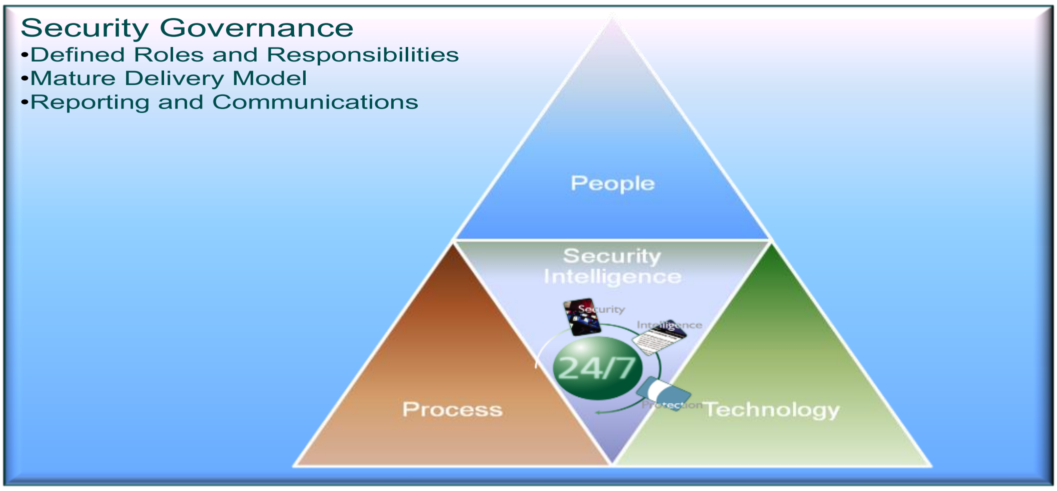
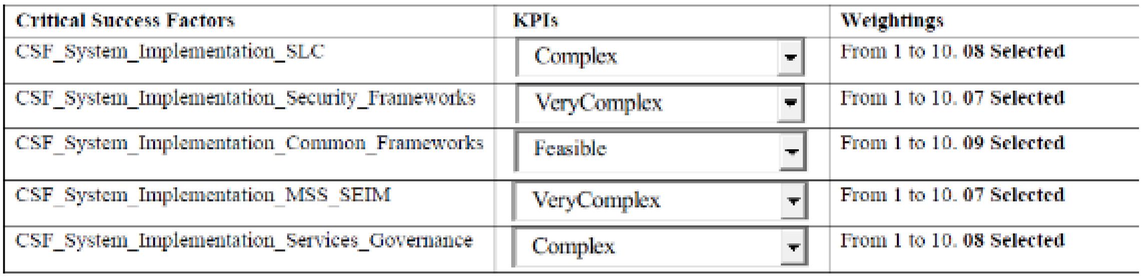


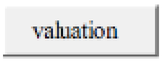
Figure 20: Security Governance diagram

6.6. Project's System Implementation CSFs

Table 5: This CSA has the average of 7.75.



Critical Success Factors	KPIs	Weightings
CSF_System_Implementation_SLC	Complex	From 1 to 10. 08 Selected
CSF_System_Implementation_Security_Frameworks	VeryComplex	From 1 to 10. 07 Selected
CSF_System_Implementation_Common_Frameworks	Feasible	From 1 to 10. 09 Selected
CSF_System_Implementation_MSS_SEIM	VeryComplex	From 1 to 10. 07 Selected
CSF_System_Implementation_Services_Governance	Complex	From 1 to 10. 08 Selected



Factors evaluated with the PRWC and the results are shown in Table 5. This CSA's result of 7.75, which is very low, is due to siloed architectures. As this CSA_DT presented negative results, the next CSA to be analyzed is the Project's high-level implementation that is this article's ACS.

7. High-Level Implementation

7.1. The Role of PEMM

e-health is a security driven-concept that offers templates to support GHS' Intelligence and also is coupled with the PEMM and sMDTCAS. The PEMM and sMDTCAS support the mapping concept for the common, APD, and Project's requirements. The PEMM and sMDTCAS need a successful sUP... The sUP generates e-services which contain *Intelligence* and application services and for that there is the need to apply the "1:1" mapping concept. *The e-health* use PEMM and sMDTCAS interfaces to interact with various Natural Language Programming (NLP) scripts which's main aim is: 1) To find HDT based solutions; 2) Locate fallouts; 3) Interface different sICS-languages and IDEs; 4) Security components; and 5) Accesses PEMM's dictionaries and registries. GTP-REHPSIs and related NLP scripts use traditional UDDI or Application Programming Interface (API) to manage accesses to e-services and secured BPMs (sBPM) catalogues. Registries link Intelligence, sBPMs and their interaction with e-services, which are registered by active GTP-REHPSIs. The PEMM uses the registry and dictionary to interface the sICS and security components. The PEMM can be used to access high-level management tools like in the case of the Strengths, Weaknesses, Opportunities, Threats (SWOT). SWOT to evaluate the effectiveness of *e-health's* integration in a GHS. A PEMM applies SWOT and relates Factors by using *e-health's* for GHS Factors (*e-health*4GHSF) class-structure. Each CSA contains related *e-health's* CSFs and in turn KPIs where each KPI links to an sICS variable (VAR, which is a e-service's attribute(s) and is represented as e-service.VAR) [49, 50], the various structures are shown in Figure 16.

```
SWOT2CSA
{…};

CSA2CSF
{…};

CSF2KPI
{…};
```

Interfacing to secured BBs (sBB) (and secured Composite BBs-sCBB), with KPI elements relate VARs by using the KPI2VAR structure:

```
KPI2VAR
{…};
```

Figure 21: *e-health*4GHSF's structures.

7.2. The Role of Implementation

e-health's PEMM and *e-health*4GHSF's, interface the sICS environment's components to persisted GTP-REHPSIs, by:

- Security concepts and architecture guidelines.
- Behaviour Driven Development (BDD) that is accessed by NLP scripts.
- Modelling languages like UML, OOM, and ArchiMate which include behavioural and structural elements (and a wide range of relationships) [51].
- Application cartography refinement tools and extracted diagrams, like TOGAF's Application Communication Diagram (ACD) that depicts all used ICS and Security models; with their mappings related to communication between secured applications and accesses sCBBs.
- API's Management (APIM) tools [52].
- Test Driven Development (TDD) is a programming approach and a concept where software developers design the test first concept.
- Acceptance Test-Driven Development (ATDD) that is applied to test the collaboration of business clients, *Project* engineers, *Project* testers and software engineers to finalize a subsystem [53].
- A secured GTP-REHPSI Test (sSIPT) that combines TDDs, ATDDs and is based on developing tests where tests represent the results of the requirement's behaviour of a set of NLP scripts.
- Requirements' implementation uses NLP scripts and methodologies like UML.

- *PEMM*'s and sMDTCAS' capabilities to interface GTP-REHPSI based *Intelligence*.
- GTP-REHPSI accumulated Implementation Development Environments (IDE) and Development and Operations (DevOps) experiences.
- *The e-health* consults Security specialists, executive directors, Project-members, and is designed to identify EA and Security risks [54].
- Integrating standards ^{2}frameworks, like risk frameworks; like the popular COSO which is presented in Figure 17.

7.3. The Role of DevSecOps

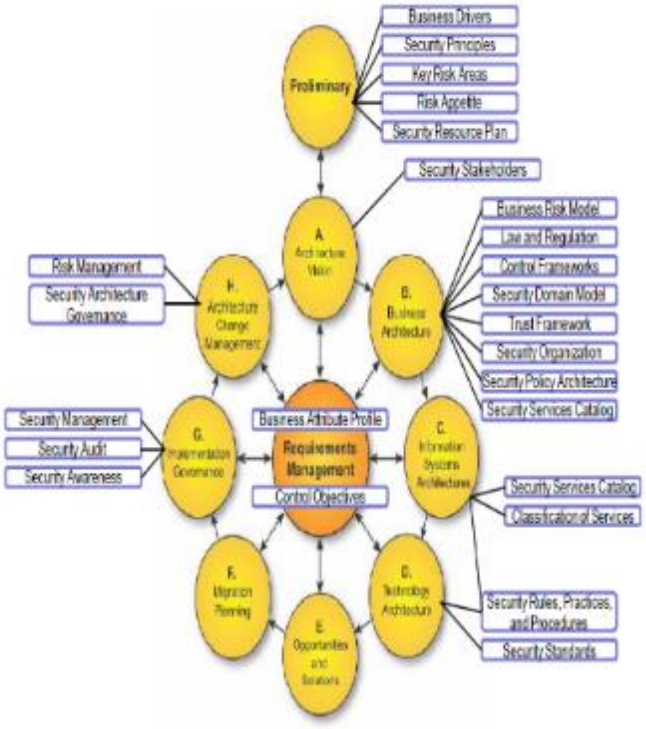


Figure 22: Integration of SABSA with the *e-health* [56].

e-health's DevSecOps manages: 1) *Project's* IDEs, developers, operations and security specialists; 2) Is controlled by a GHS Secured Control and Logging Infrastructure (ESCLI), which feeds GTP-REHPSIs; and 3) GTP-REHPSIs editing. Cyberbusiness platforms are not Project and APD agnostic but can offer: 1) Better performance; 2) Reliability; and 3) Cybersecurity/Tracing in GTP-REHPSIs. sUnits are controlled/monitored in real-time by the ESCLI which is optimal for monitoring and support GTP-REHPSIs' presentation, sorting, and tuning. An ESCLI can used to analyse, collect and store in GTP-REHPSIs. A GHS can also build an IHI secured Cloud (sCloud) to avoid locked-in situations and important security breaches. *e-health's* uses EA/TDM to support interfacing market risk frameworks like COSO, which is shown in Figure 19 [25]. *GHS(S/C)* needs the *e-health* to combine many security fields where Cybersecurity is the central issue. Therefore, the *e-health* needs the e-TDM, which interfaces frameworks like ADM/e-TDM, SAFe, COBIT, CISA… Unfortunately, today, we are just tackling isolated fields like Software security, Network Security. As shown in Figure 23.

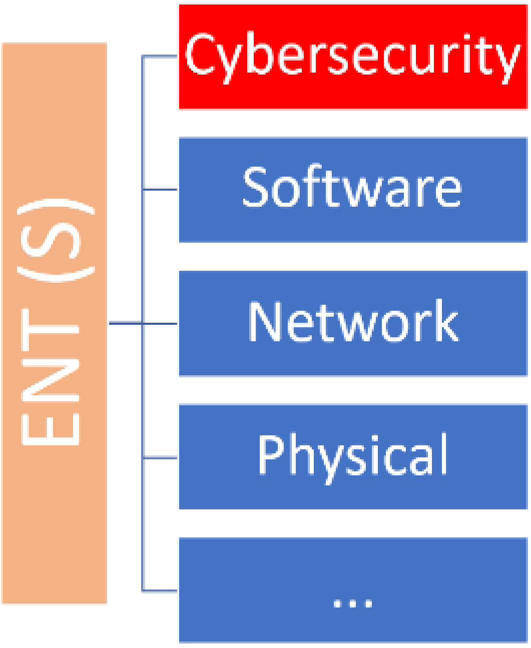


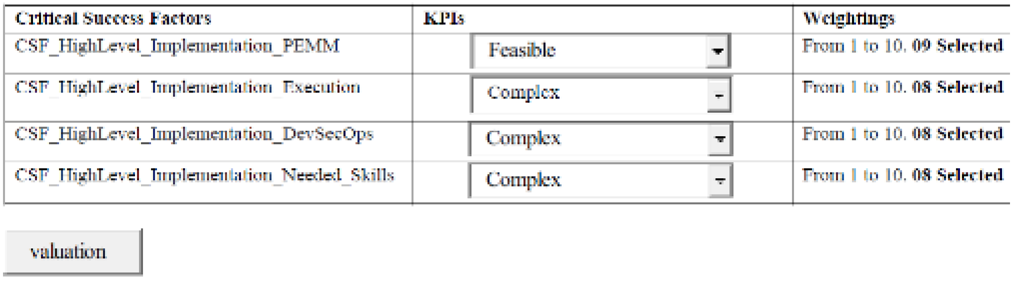
Figure 23: *e-health's* ETP-HSC Approach [1].

7.4. The Role of Needed Skills

e-health's needed set of skills are [58,59]: 1) Polymathic Security architecture; 2) Interfacing of EA and Security architectures; 3) Detailed AI and GTP-REHPSIs modeling and integration; 4) Interfacing AI components; 5) *e-health* related application's sBPMs and e-services; 6) Security and common requirement engineering; 7) Standardized sICS integration; 8) e-TDM/EA, sMDTCAS, and related Business, Data, Application, and Technology Architectures; 9) Generic skills like leadership and audit; 10) Business and organizational engineering; 11) PM technics; 12) ICS IDE technologies; 13) Business use cases design sBPMs integration; 12) Standard frameworks; 13) Building PEMMs*;* and other.

7.5. High-Level Implementation's CSFs

Table 6: This CSA has the average of 8.25.



Critical Success Factors	KPIs	Weightings
CSF_HighLevel_Implementation_PEMM	Feasible	From 1 to 10. 09 Selected
CSF_HighLevel_Implementation_Execution	Complex	From 1 to 10. 08 Selected
CSF_HighLevel_Implementation_DevSecOps	Complex	From 1 to 10. 08 Selected
CSF_HighLevel_Implementation_Needed_Skills	Complex	From 1 to 10. 08 Selected

Factors were evaluated with the PRWC, and the results are shown in Table 6. This CSA's result of 8.25, which is satisfactory, which is due to tools interfacing.

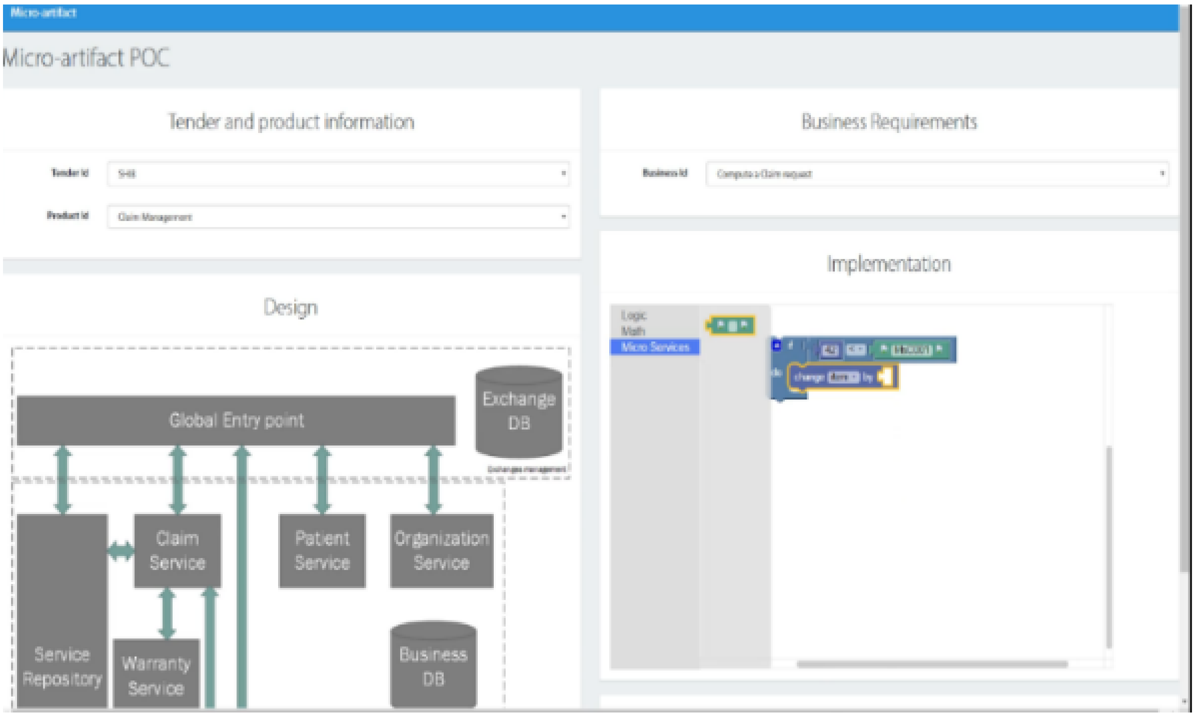
8. The PoC

8.1. PoC's Resources and Environments

The PoC was implemented by using the following resources and environments: 1) The *TRADf* to demonstrate an IHITF; 2) Various EA environments; 3) Java Extended Edition; 4) Microsoft Visual Studio; 5) Microsoft Windows operating system; and 6) Author's previous works and PoCs.

8.2. PoC's User Interface

The User Interface, as shown in Figure 24, links Project's Global Unique Identifiers (GUID) to the defined requirements and unbundled artefacts. Each requirement has a its unique design part-document, which defines an implementation scenario (or a sBPM) that is choreography of e-services.



Micro-artifact

Micro-artifact POC

Tender and product information

Tender id: S-88

Product id: Claim Management

Business Requirements

Business id: Compute a Claim request

Design

Implementation

Figure 24: The user interface which manages BBs and other artefacts.

8.3. PoC's Preparations

The next step is to reuse previous PoCs modules (like the ETP-HSC's [1]) and then to prepare the IHITF by setting-up the sMDTCAS, e-TDM, and the GTP-REHPSIs as shown in Figure 25 [61]. This PoC uses various *TRADf* modules, like the sUP and *e-health*, which focus on the extraction and securing of the unbundled e-services.

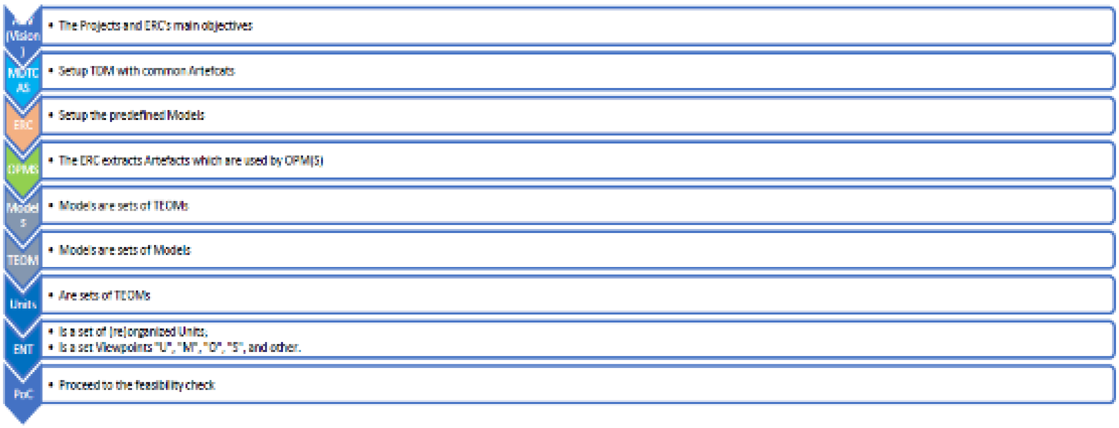

(Vision)
• The Projects and ERC's main objectives
MDTCAS
• Setup TDM with common Artefacts
ERC
• Setup the predefined Models
OPMS
• The ERC extracts Artefacts which are used by OPM(S)
Models
• Models are sets of TEOMs
TEOM
• Models are sets of Models
Units
• Are sets of TEOMs
ENT
• Is a set of (re)organized Units.
• Is a set Viewpoints "U", "M", "O", "S", and other.
PoC
• Proceed to the feasibility check

Figure 25: PoC's preparations sequences [1].

sCBBs are assembled to build e-services' based sBPMs/scenarios and GHS Transactions, which need the optimal level/approach of granularity that respects the "1:1" mapping mechanism. A logical view of a series of e-services based GHS Transactions is presented in Figure 26, and their consumption of e-services. where events are managed by the sICS node-servers, that requires a specific encryption which is managed by the e-TDM. The GHS Transaction uses a set of sCBBs.

sUP-APD Environnement	Provides APD e-services
Controller	Passes an e-service request
Find e-service	Execute
Data Source	Return information and update GTP-REHPSIs

Figure 26: GHS Transaction's elements.

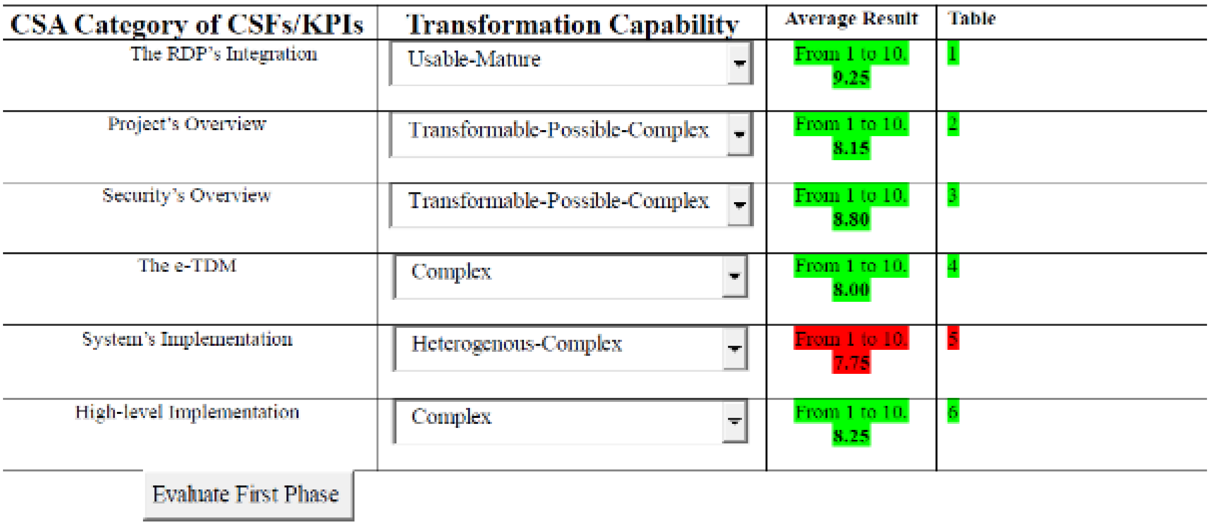
8.4. PoC's Design

PoC's main constraint is to implement an sICS and adapted security controls, by using the sMDTCAS and e-TDM. The sMDTCAS is used to design e-services, and corresponding diagram. e-services based diagrams are used to design and implement sBPMs (and hence HDT scenarios) in the transformed sUnits. To identify the initial sets of Factors (CSAs' CSFs) and test whether the RQ's of CSFs affect *e-health's* integration. The PoC uses the HDT based mixed qualitative-quantitative method. The PoC in the beginning uses Phase 1 that is mainly based on the HDT CSA_DTs, which uses the PRWC for evaluation purposes. Phase 1 is used to rate/weight the importance of CSAs and CSFs for the usage of *e-health* and that is done using a CSA_DTs [62].

8.5. PoC's Phase 1

PLRP's outcome proved the existence of an important research gap and it's (or Phase 1's) outcome supports RQ's credibility, by the use of the LRP and *TRADf*'s archive or knowledgebase, of an important set of references, previous author's IHITF, articles, works, documents, and links.

Table 7: PoC's phase 1 outcome is (rounded) 8.40.



CSA Category of CSFs/KPIs	Transformation Capability	Average Result	Table
The RDP's Integration	Usable-Mature ▾	From 1 to 10. 9.25	1
Project's Overview	Transformable-Possible-Complex ▾	From 1 to 10. 8.15	2
Security's Overview	Transformable-Possible-Complex ▾	From 1 to 10. 8.80	3
The e-TDM	Complex ▾	From 1 to 10. 8.00	4
System's Implementation	Heterogenous-Complex ▾	From 1 to 10. 7.75	5
High-level Implementation	Complex ▾	From 1 to 10. 8.25	6

Factors are associated to HDT's NLP (or sBPM) scenarios, where CSFs' are linked to RDP resources. The HDT represents the relationships between this RDP's RQ, GTP-REHPSI, and Project requirements, e-services, and selected sets of Factors. PoC's interfaces were implemented using TRADf, which supports *e-health's* calls to e-services. Factors were selected and evaluated (using PPRWC, WGTs, HDT, and *Intelligence*) and the results are presented in Table 7, which shows that the *e-health* is a very important Project's phase and cannot be an independent transformation initiative. HDT's main constraint is that CSAs having an average result below 7.5, will be ignored. This mentioned fact leaves this RDP's CSAs and CSA-DTs (marked in green) effective for RDP's and articles conclusion(s); and drops the CSAs marked in red. Phase 1, shows that the GTP-REHPSI and *e-health* are very complex but that the PoC can proceed with Phase 2.

8.6. PoC's Phase

Starts with sMDTCAS, e-TDM's, GTP-REHPSI's setups and Factors' selection. Phase's 2 setup includes: 1) Sub-phase A or the GTP-REHPSI and Architecture Vision phase's goals, establishes a *e-health* approach and goals; 2) Sub-phase B or the Business Architecture phase establishes *e-health's* target e-TDM/EA and related GTP-REHPSIs' activities; 3) Sub-phase C shows and uses the Application Communication Diagram to describe *e-healths*' activities; 4) Sub-phase D or the Target Technology Architecture shows the needed GTP-REHPSI and *e-health's* optimal infrastructure landscape; and 5) Sub-phases E and F, or the Implementation and Migration Planning, presents the transition GTP-REHPSI based architecture, which proposes intermediate situation(s) and evaluates GTP-REHPSI (and *e-health*'s) status(es). e-services and HDT based *Intelligence* has mappings to GHS's resources and the *e-health* defines relationships between e-services, *PEMM*/sMDTCAS, GTP-REHPSIs, and Problems (PRB).

8.7. PoC's PRBs Processing in an HDT Node

The *Intelligence* solves *e-health's* PRBs, where Factors link to specific *e-health* PRB type and has a set of actions that are processed in a concrete HDT node. For this goal, the action *CSF_e-health_or_GTP-REHPSI_Extraction_Procedure* was called and delivered SOL(s). Solving PRBs involves the selection of actions and possible Solutions (SOL) for multiple *Project* activities. The HDT is on mixed quantitative/qualitative and has a dual objective that uses the following steps:

- In Phase 1, *TRADf's* interface implements HDT scripts to process the selected CSAs. And then relates PoC's resources to *CSF_e-health_or_GTP-REHPSI_Extraction_Procedure*.
- The *Intelligence* is configured to weight and tuned to support the HDT.
- Link the selected node to HDT to deliver the root node.
- The HDT starts with the *CSF_e-health_or_GTP-REHPSI_Extraction_Procedure* and proposes SOL(s) in the form of *e-health* actions/improvements.

HDT scripts support *M-Model*'s instance that are processed in the background to deliver *e-health* or ETP-HSC risk procedures and value(s). The *M-Model* based *Intelligence* uses e-services to deliver *e-health* operations, which are a set of *e-healths* actions that are stored in GTP-REHPSIs.

8.8. PoC's High-Level Implementation

Using Factors to interface SWOT as by the following steps:

- Linking *e-health* e-services (and resources) to SWOT.
- Links Factors to structures, like CSA2CSF, CSF2KPI, and KPI2VAR…
- Factors tags are linked to various SWOT scenarios.
- From the IHITF's frontend mapping actions are activated by: 1) Selecting HDT nodes that contains *e-health's* Factors, and 2) Selecting the security problem to be solved. SWOT/ STORM uses Intelligence to generate needed actions to solve a request and store the results in GTP-REHPSIs. Intelligence and its HDT NLP scripts to deliver SWOT's output/solutions.
- Output/solutions persisted in GTP-REHPSIs.

9. Conclusions and Recommendations

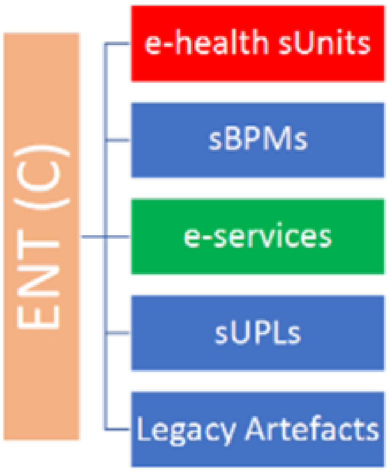


Figure 27: Viewpoint's "C" evolution roadmap.

To transform a GHS is a need for an IHITF and a Polymathic strategy that is based on standards, mapping concepts and e-services interoperability. This article and its PoC offered a set of recommendations knowing that Projects' have XHFRs. e-TDM provides the link between the defined requirements and its Project's implementation and using e- services to serve requests. Today many e-standards exist, and a Project must have an agile holistic view on its phases and resources. e-services are sUP's result and used in sBPMs. The GTP-REHPSI based PoC proved Project's complexities. *The e-health* supports sICS, e-services and sBPMs to support the transformation of GHS and its sUnits. The GTP-REHPSI is optimal for a GHS and its security management. The PLRP presented the research gap, that is due to the fact that are no similar IHITF, *MetaModel/*sMDTCAS approaches and that there is an extreme lack of a Polymathic-holistic approaches. There are siloed and limited manual security tools and methods, but the *e-health* presents the possibility to implement an IHITF and *e-health*. The RDP is a part of a series of publications on Projects, Security strategies, e-health, PEMM, TDM/EA, Polymathic models… The Project uses e-services, HDT and Factors to support *e-health* activities, where the *e-health* focuses on managing secured GHS operations. GTP-REHPSI and *e-health* synchronizes a structured relationship between: Health activities, Global Security, GCRs' management, sMDTCAS, e-TDM/EA, and HDT based *Intelligence*. The PoC's Table 7 result of (rounded) 8.40 that used Factors and CSFs' binding to a RDP resources, the *Intelligence*, RQ, *e-health,* and e-services, shows that the *e-health* is very complex due to siloed nature of GHSs and the lack of Polymathic skills and this article's set of recommendations are:

- This article presents the role of Projects and GTP-REHPSI; and the focus is on the GHS adapted for the KSA and SHID.
- Projects have XHFRs at about 95 percent; andare due to siloed approaches.
- All author's works are based on TRADf, AHMM, (e-)TDM, and an RDP concept; which are today mature and can be applied in various APDs and any type of transformation initiative.
- *e-health* must avoid locked-in security situations.
- This RDP uses a multi-dimensional *e-health*, because it has: 1) Interoperable e-services; 2) An adapted mixed-research approach; 2) Presents the IHITF; and 3) A methodological approach based on EA/e-TDM and *Intelligence*.
- The PRLR asserted the existence of a research gap.
- Use a MM, like the *M-Model*, to support GTP-REHPSIs and HDT.
- Cross-functional/Polymathic skills are needed for Projects and *e-health*.
- *The e-health* unbundles the legacy BPMs to support sUnits, which can face problems in the alignment of various e-services.
- DevSecOps' integration in *e-health,* enables the automation of all Project's security developments.
- *e-health* coordinates GHS' activities.
- The sMDTCAS, PEMM, and e-TDM support *e-health*.
- *e-health* constraints are controlled and monitored by the sICS.
- sUnit's transformation needs an IHITF and sMDTCAS that transforms and secures a GHS.
- Avoid consulting firms and commercial products to build an IHI *e-health* system.
- GTP-REHPSI and *e-health* are very complex.
- Viewpoint's "C" presents a structured evolution's roadmap for the *e-health*, as shown in Figure 27.
- The Project offers a flexible and scalable sICS.
- Use AR based HDT to solve GTP-REHPSI problems.
- Use the PRWC based CSA_DTs to filter and weight CSAs.

- *The e-health* interfaces high-level tools and environments like SWOT.

References

[1] Trad, A., & Kalpić, D. (2016). A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-The role of transformation managers in organisational engineering. Journal: Chinese American Scholars Association Conference E-Leader, Austria.

[2] A. Trad. Enterprise Transformation Projects-The Role of Enterprise Architecture in Implementing a Holistic Security Concept (ETP-HSC). ISSN: 2795-4609 | ISSN: 2795-4560. Advanced Research on Information Systems Security, an International Journal (ARIS2) (2023) Volume 3, No 1, pp 04-35. International Journal. 2023.

[3] A. Trad (2024a). Enterprise Transformation Projects-The Role of The Polymathic Security Learn Processes (ETP-RPSLP). Jorunal: Advanced Research on Information Systems Security, an International Journal (ARIS2). 2024.

[4] SHIB (2016a). COUNCIL OF COOPERATIVE HEALTH INSURANCE (CCHI). SAUDI HEALTH INSURANCE BUS (SHIB) PROJECT. NUMBER: 2/34/Z. MOBILY, BUSINESS SALES. RIYADH, KINGDOM OF SAUDI ARABIA.

[5] Trad, A. (2016). The Holistic Brick based Architecture. SHIB. France.

[6] Trad, A. (2016). An Intelligent Microartefact Patterns' based Architecture. SHIB. France.

[7] A. Trad. Enterprise Transformation Projects- The Polymathic Enterprise Architecture Based Generic Learning Processes (PEAbGLP). 2024. IGI. Submitted.

[8] A. Trad and D. Kalpića. Using Applied Mathematical Models for Business Transformation. IGI Complete Author Book. IGI Global. USA. 2019.

[9] A. Trad. The Business Transformation and Enterprise Architecture Framework-The Applied Holistic Mathematical Model's Persistence Concept (AHMMPC). WSEAS. 2019.

[10] A. Trad. Academic and Educational Transformation Projects-The Role Team-Based Learning in Polymathics (RTBLP). IGI Global. USA. 2023.

[11] A. Trad. Academic and Educational Transformation Projects-The Role Team-Based Learning in Polymathics For University Cycle (RTBLP4UC). IGI Global. USA. 2023.

[12] J. Koenig, K. Rustan and M. Leino. *Programming Language Features for Refinement*. Stanford University. USA. 2016.

[13] C. Block. 12 Reasons Your Digital Transformation Will Fail. Forbes Coaches Council. Forbes. https://www.forbes.com/sites/forbescoachescouncil/2022/03/16/12-reasons-your-digital-transformation-will-fail/?sh=4e5a5f751f1e. 2022.

[14] Z. Dello Ioio. 5 reasons why digital transformation projects fail (2023). Enate. https://www.enate.io/blog/why-digital-transformation-projects-fail#:~:text=Technology%20is%20always%20evolving%20and,considering%20making%20their%20own%20changes. 2023.

[15] A. Trad and D. Kalpić. An applied mathematical model for business transformation-The Holistic Critical Success Factors Management System (HCSFMS). Encyclopaedia of E-Commerce Development. Journal: Encyclopaedia of E-Commerce Development, Implementation, and Management. Hershey, PA: IGI-Global. 2018

[16] S. Peterson. Why it Worked: Critical Success Factors of a Financial Reform Project in Africa. *Faculty Research Working Paper Series*. Harvard Kennedy School. 2011

[17] The Open Group, Requirements. ADM Architecture Requirements Management. The Open Group. USA. http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap15.html. (2011).

[18] B. Dick. Action research: action and research. Australia: Southern Cross. University Press. [21-27]. 2001.

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

[20] Kabzeva, A., Niemann, M., Müller, P., Steinmetz, P. Applying TOGAF to Define and Govern a Service-oriented Architecture in a Large-scale «research & development (R&D). Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru. 2010.

[21] A. Trad. Applied Holistic Mathematical Models for Dynamic Systems (AHMM4DS). International Journal of Cyber-Physical Systems (IJCPS). IGI-Global. USA. DOI: 10.4018/IJCPS.2021010101. 2021.

[22] A. Trad. Business, Economic, and Common Transformation Projects-The Polymathic Ratings and Weightings Concept (PRWC). Submitted.

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

[24] Ouye, J. Facility Technics Facility Management Consulting, 505 17th Street, Suite 300, Oakland, CA 94612. USA.

[25] A. Trad. Organizational Transformation Projects-The Role of Global Cyber Security and Crimes (RoGCSC). IGI Global. USA. 2023.

[26] A. Trad. Business Transformation Projects-The Role of a Transcendent Software Engineering Concept (RoTSEC). IGI Book Chapter. IGI Global. USA. 2022.

[27] A. Trad. Business Transformation Projects-The Role of Requirements Engineering (RoRE). IGI Book Chapter. IGI Global. USA. 2022.

[28] A. Trad. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basic Construction. IGI Book Chapter. IGI Global. USA. 2023.

[29] A. Trad. Integrating Holistic Enterprise Architecture Pattern-A Proof of Concept. IGI Book Chapter. IGI Global. USA. 2023.

[30] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-Intelligent atomic building block architecture. Journal: Procedia Computer Science, Volume 64, Pages 214-223. Elsevier. 2015.

[31] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-An Information System's Atomic Architecture Vision. Journal: Procedia Computer Science. Volume 64, Pages 204-213. Elsevier. 2015.

[32] A. Trad. Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process. IGI Global. USA. 2023.

[33] A. Trad. Organizational and Digital Transformation Projects-A Mathematical Model for Enterprise Organizational Models. IGI. USA. 2022.

[34] B. O'Riordan. INNOVATION-Why Transformations Fail And How They Can Succeed With People Power. Forbes. 2021.

[35] Standish. The Chaos Reports. http://www.standish.com, Standish. USA. 2011.

[36] The Open Group. Introduction to the Architecture Development Method (ADM). The Open Group. USA. 2011.

[37] A. Trad. Societal Transformation Projects: The Role of an Adaptable Democracy (RAD)–A Humanistic Approach. Book: Considerations on Education for Economic, Social, and Environmental Sustainability. Pages: 381-422. IGI Global. USA. 2023.

[38] Consultor. Comment l'hosto britannique est devenu McKinsey addict. Consultor. https://www.consultor.fr/articles/comment-l-hosto-britannique-est-devenu-mckinsey-addict. 2022.

[39] OECD. COVID-19 spending helped to lift foreign aid to an all-time high in 2020 but more effort needed. Organisation for Economic Co-operation and Development (OECD). https://www.oecd.org/development/covid. 2021.

[40] H. Pushpakumara, P. Jayaweera and W. Manjulan. Using the Open Group Architecture Framework (TOGAF) for Quality Assurance in Higher Education Teaching and Learning. January 2021 SSRN Electronic Journal. DOI: 10.2139/ssrn.3808691. 2021.

[41] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-Intelligent aBB architecture. Centeris. Portugal. 2015.

[42] A. Trad. Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process. IGI-Global. USA. 2023.

[43] A. Trad and D. Kalpić. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basics. IGI. USA. 2022.

[44] A. Trad and D. Kalpić. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Implementation. IGI. USA. 2022.

[45] A. Trad. Business Transformation Project's-The Impact of Rise of Over-the-Top (OTT). IGI-Global. USA. 2023.

[46] SABSA. *Sherwood Applied Business Security Architecture*. SABSA. 2020. Available https://sabsa.org/

[47] A. Trad and D. Kalpić. Building a XML based object mapping system (OMS). Conference: Proceedings of the 23rd International Conference on Information Technology Interfaces, 2001. ITI 2001. Pages: 89-94. IEEE. 2001.

[48] Godinho de Matos, M., Tribolet1, J., Magalhãe, R. "Organisational Engineering: An Overview of Current Perspectives". Insituto Superior Técnico. Portugal.

[49] A. Trad. A Relational DataBase based Enterprise Transformation Projects. Journal: International Journal of Mathematics and Computers in Simulation. Volume 17, Pages. 1-11. NAUN. npublications.com. 2023. Javatpoint. Understanding SWOT Analysis. Javatpoint. https://www.javatpoint.com/swot. 2021.

[50] A. Trad and D. Kalpić. SWOT based Transformation's Organizational Risks' Management (STORM). E-leaders conference, Check Republic. www.g-casa.om. 2023

[51] Hosiaisluoma. Holistic Enterprise Development. 2022. Avalable https://www.hosiaisluoma.fi/blog/archimate-examples

[52] S. Patni. Pro RESTful APIs Design, Build and Integrate with REST, JSON, XML and JAX-RS. 2017.

[53] D. Janzen and H. Saiedian. Test-driven development concepts, taxonomy, and future direction. Published in: Computer (Volume: 38, Issue: 9, Sept. 2005). IEEE. 2005.

[54] A. Trad. The transformation framework The role security in the global education system. Journal: International Journal of Higher Education Management. Volume: 8, Issue 1. Centre for Business & Economic Research. UK. ijhem.com. 2021.

[55] Enterprise SecurityA. Trad. The business transformation enterprise architecture framework for innovation: The role of artificial intelligence in the global business education (RAIGBE). Journal: The Business & Management Review. Volume: 12, Issue 1, Pages: 82-97. Centre for Business & Economic Research. UK. cberuk.com. 2021.

[56] A. Trad and D. Kalpić. Business transformation project's architect's profile (BTPAP). The Business & Management Review. Volume 12, Issue 2, Pages 137-153. Centre for Business & Economic "Research. cberuk.com. 2021.

[57] J. Van Hoof. Using ITIL for SOA Governance. SOA and EDA. http://soa-eda.blogspot.fr/2007/12/using-itil-for-soa-governance.html . 2007.

[58] The Open Group. Risk Management. pubs.opengroup.org/architecture/togaf9-doc/arch/chap31.html. The Open Group. USA. 2011.

[59] T. Thune. Success Factors in Higher Education–Industry Collaboration: A case study of collaboration in the engineering field. Tertiary Education and Management volume 17, pages31–50. 2011.