The transformation framework
The role security in the global education system

Dr. Antoine Trad
IBISTM. France

Key words

Global Education, Security, Artificial Intelligence, heuristics, Transformation Manager's Profile, Transformation Project, Enterprise Architecture and Critical Success Factor

Abstract

This article analyses the role of Global Education System (GES) and proposes the Applied Holistic Mathematical Model for GES (AHMM4GES). The AHMM4GES is based on many years of research on business & educational transformations, Artificial Intelligence (AI), applied mathematics, software modelling, business & organizational engineering, skills & educational systems, financial analysis, security and enterprise architecture. The used research methodology is based on the author's authentic mixed research method that is supported by a mainly qualitative reasoning module. AHMM4GES's formalism mimics the human brain, by using empirical processes that are based on heuristics. The AHMM4GES is used to implement a decision-making system (or an expert system) to support a GES and uses a behaviour-driven development environment that can be easily adopted by any organization. The development environment can be used by any team member without any prior computer sciences qualifications.

The AHMM4GES is used to estimate the Role of AI based Security in GES's (RAISGES) context and tries to estimate the roles of the giants in this domain, like the USA, China, and India; and what would be the real role of the European Union and France.

The uniqueness and originality of this research is that the AHMM4GES promotes a holistic unbundling process, the alignment of transformation strategies to support GES' evolution. For a successful integration of AHMM4GES in projects, the manager's profile, education, skills and role are crucial, where his decisions are supported by the selection, implementation and processing of critical success factors. The main implication is a systemic approach that is the optimal to integrate an RAI4GES.

Corresponding author: Antoine Trad
Email address for the corresponding author: antoine.trad@ibistm.org
The first submission received: 10th June 2021
Revised submission received: 20th August 2021
Accepted: 25th August 2021

Introduction

Actual archaic Educational (or Business) Transformation Projects (simply a *Project*) are managed as silos where their components create a messy hairball that is called a secured Information and Communication System (ICS).

Figure 1. Technology Trends (Cearley, Walker & Burke, 2016)

To avoid such failed scenarios, this article recommends the usage of a AHMM4GES based Decision Making System for GES (DMS4GES), to solve education, business, and organizational problems, by offering a set of possible solutions. Solutions have the form of recommendations for any type of a GES problem. Problem solving uses a central qualitative method that is based on the Heuristic Decision Tree (HDT) process, which uses quantitative methods at its nodes. DMS4GES's actions produce solutions which can be applied by GES specialists to support the implementation of a *Project*. A DMS4GES is a multi-objective and multi-Critical Success Factors (CSF) based system, which is oriented for problems' solving and its main goal is to maximize the *Project's* success rate. As shown in Figure 1, the major strategic technology trend is AI based Security (AIbS) which is RAI4GES's main construct (Cearley, Walker & Burke, 2016). The RAI4GES supports a generic and cross-functional reasoning engine that is mainly based on: 1) CSFs' classification and management mechanism; 2) An adapted qualitative HDT based research method; and 3) A set of quantitative modules that can be triggered from its HDT's nodes. AHMM4GES's holistic concept is mainly business driven and is agnostic to a specific enterprise, country, business environments, governments, or organization (simply an *Entity*) (Trad & Kalpić, 2020a). *Entities* are increasingly using classical and Cybertechnologies to become Cyberentities. The transformed Cyberentity, must face new challenges, dangers, and security Risks (sRisk), when implementing its infrastructure and ICS. One of the most important sRisks is the stability of an *Entity* in an unsafe and unstable ecosystem that is mainly based on the ICS. Therefore, the security of an *Entity* should have a holistic concept like the RAI4GES for a *Project*.

The RAI4GES includes a methodology and a concept to manage AIbS for *Entities*, which includes classical and Cybersecurity. Cybersecurity is employed in the *Entity*'s architecture and operations processes. *Entity*'s transformation has many tangible advantages and unfortunately has also many sRisks and pitfalls. *Entity*'s main sRisks are data, modules, assets, and resources platform security, but there is a whole set of other types of ICS and domain specific sRisks. *Entities* are more or less sensitive on classical attacks and cyberattacks, depending on the size of the *Entity*, volume of transactions, data management and the applied agility. In order to identify classified *Entity*'s security breaches like data leaking, the proposed RAI4GES proposes a systematic and holistic approach to ICS' resources protection that includes Cybersecurity mechanisms. Cybersecurity is essential for ensuring *Entity*'s sensitive information, assets, and resources protection from a probable use of personal information that can be leaked and used by

hackers. *Entities* are facing excessive requests to optimize their assets and minimize sRisks, to guarantee sustainability, optimize costs, support transformation initiatives, to integrate security and governance frameworks (Trad, 2021a, 2021b).

Background

The *Project*'s technical implementation phase is the major cause of high failure rates; therefore, the transformation manager's (or simply the *Manager*) needs skills which should encompass: 1) Enterprise Architectures (EA), business process management and services technologies; 2) Unbundling environments; 3) Agile project management; 4) AI, algorithmics and mathematical models; 5) Organizational engineering; 6) Global educational systems; 7) Financial management; 8) Implementation phase's skills; and 9) ICS integration strategies. Therefore, the author recommends a *manager's* profile with an extended technocrat's profile (Farhoomand, 2004) that needs to be complemented with various cross-functional skills. More specifically, this research focuses on the influence of the *Manager*s' AI, high-tech and EA experience, background, and education. *Projects* integrate avant-garde knowledge and services technology components. To be successful, a GES must incorporate AI based tech and security to outperform their adversaries. Actually, there are many methodologies that can be used to implement *Project*s (Gartner, 2016), but all of them lack a holistic and anti-lockedin approach. The *Manager* can integrate an DMS4GES in EA's roadmap, in order to support the *Project's* complex and risky implementation (Zaiane & Ben Moussa, 2018).

The AHMM4GES delivers a generic skeleton for the DMS4GES that is capable to deliver just-in-time solutions. This article's research methodology is based on 1) A multi-domain literature review; 2) A mainly qualitative methodology; 3) A secondary quantitative methodology; and 4) An engineering-controlled experiment; which is the optimal methodology that can be applied in engineering projects (Easterbrook, Singer, Storey & Damian, 2008). Besides classical security and Cybersecurity, the Organized Financial Predator's Strategy (OFPS) must be aware of other types of organized asymmetric attacks like 1) Cyberwarfare; 2) Cyberterrorism; 3) Cyberhooliganism; 4) Cyberfinance attacks; and others. Just analysing data is a partial, limited and is a static solution, there is a need for a dynamic proactive HDT. There is also a need to control the activities and behaviour of persons (and groups), which are an important part of the *Entity*'s internals and to detect any probable violations. Violations can be modelled to deliver controlled access to *Entity*'s internals by political backup, spying services, assigned roles, responsibilities & credentials and defined standards. The RAI4GES uses CSFs that are stored in Critical Success Areas (CSA) and are managed by the author's framework.

The Author's Framework and Research Concept

The research concept is a part of the Transformation, Research, Architecture, Development framework (*TRADf*), which is composed of various modules. In this article, parts of previous works are reused for the better understanding of this complex concept. If everything was referenced, it would have been very difficult to follow and understand this article (Trad & Kalpić, 2011, 2016). This research concept can be considered as a non-conventional and pioneering one, in the field of *Projects* related to GES systems. The used mixed method can be considered as a natural complement to conventional Quantitative Analysis for GES (QNA4GES) and Qualitative Analysis for GES (QLA4GES) methods. Both methods are compatible, and the difference is in the scope and depth of the research process. Empirical research validity checks if the research concept is acceptable as a contribution to existing scientific (and engineering) knowledge. In this article, the author tries to prove that the resultant recommendations and Proof of Concept (PoC) or experiment, are valid and applicable. Using Google's scholar online search portal, in which the author combined the previously mentioned keywords and other major key topics; the

results show very clearly the uniqueness, originality and the absolute lead of the author's works/framework in the fields of transformation methodologies, complex research projects and enterprise architecture. It can be considered as an important jumpstart for the future scientific and industrial use. The author's framework and this study's main limitation is domain's complexity.

The Research Question and Knowledge Gap

In previous phases of research, the author concluded that a *manager* is an Architect of an Adaptive Business Information System (AofABIS), who has in-depth knowledge of educational, business environments and can manage their essential CSFs. This defines the first step for the implementation of a successful *Project*, but the *Manager* must also have in-depth knowledge of: 1) Agile environments and EA; 2) AIbS and integrated development environments; 3) Businesspeoples' integration; 4) Project management; and 5) Coordination of implementation engineers (Trad, & Kalpić, 2014a, 2014b). This article's Research Question (RQ) is: *"What is the role of AI based security in the Global Education System?"*. The targeted domain is the role of France and the European Union in this global competition.

Artificial Intelligence

The European Commission defines AI, as a system that shows intelligent behavior, by analyzing the targeted environment and that can perform various tasks with autonomy, in order to achieve defined goals (European Commission, 2019). AI has the following fields (McCarthy, 1989; Bohnhoff, 2019): 1) Mathematical models and algorithms; 2) Deicison trees; 3) Learning fields, like Action Research (AR); 4) Automated scheduling and planning; 5) Technology, resilience, and processing environments; 6) Robotism, automation, and recognition; 7) Data based decision approach; and other advanced topics. The author's mixed method is based on AR, which is an interactive inquiry process that balances problem-solving actions. AR actions are implemented in a collaborative context using a data-driven collaborative analysis. AR tries to understand underlying causes which enables future predictions about organizational changes, as an iterative learning process, where AI is a strategy (or concept) and not a product.

Critical Success Areas, Factors

CSA is a selected set of CSFs, where a CSF is a set of Key Performance Indicators (KPI). Each KPI corresponds to a *Project* requirement and a problem type. For a given requirement (or problem), an initial set of CSAs and their CSFs is defined and then managed by the DMS4GES. CSFs are important for the mapping between GES problem types, knowledge constructs and organisational items. CSFs reflect possible problem types that must meet strategic *Project* goals and predefined constraints. Once the initial set of CSFs has been identified, then the *Project* can use the DMS4GES to propose a set of solution types. The RAI4GES delivers a set of solutions and recommendations (Trad & Kalpić, 2020a).

Market Standards and Frameworks

TRADf interfaces various market risk frameworks like the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is shown in Figure 2. The RAI4GES is a process, effected by an entity's board of directors, management & other personnel, applied in strategy setting & across the enterprise, designed to identify potential events that may affect the entity, manage sRisks and to provide reasonable assurance regarding the achievement of *Entity's* objectives…

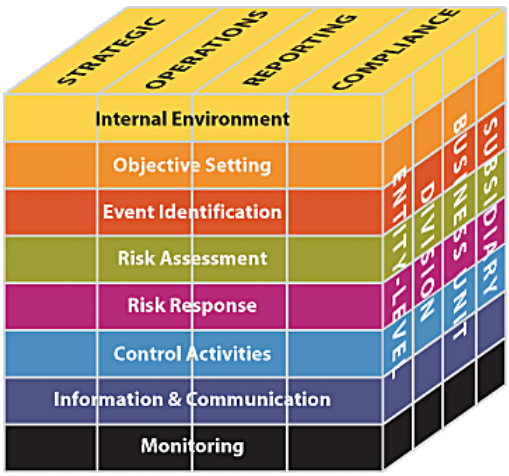

Figure 2. The COSO framework (IIA, 2004, Curtis, & Carey, 2012).

This COSO framework defines basic important components, proposes a common language and offers a roadmap for enterprise risk management. *Entity* objectives can have the following CSAs: 1) Strategic; 2) Operations; 3) Reporting; and 4) Compliance. And the following key CSFs are: 1) Organizational design of an *Entity*; 2) Establishing an RAI4GES; 3) Performing sRisk assessment; 4) Determining overall sRisk possibilities; 5) Identifying sRisk responses; 6) Communication of sRisk results; and 7) Monitoring and tracing (IIA, 2004, Curtis, & Carey, 2012).

The AHMM4GES

Basic MM's Nomenclature

Iteration	= An integer variable that denotes a *Project/ADM iteratio*	
microRequirement	= KPI	(1)
CSF	= Σ KPI	(2)
CSA	= Σ CSF	(3)
Requirement	= ⋃ microRequirement	(4)
microKnowledgeArtefact	= ⋃ knowledgeItem(s)	(4)
neuron	= action ° data + microKnowledgeArtefact	(5)
microArtefact	= ⋃ (e)neurons	(6)
microEntity or Enterprise	= ⋃ microArtefact	(7)
Entity or Enterprise	= ⋃ microEntity	(8)
microArtefactScenario	= ⋃ microArtefactDecisionMaking	(9)
Decision Making/Intelligence	= ⋃ microArtefactScenario	(10)
EnityIntelligence	= ⋃ Decision Making/InteligenceComponent	(11)
MM(*Iteration*) as an instance	= EnityIntelligence(*Iteration*)	(12)

Figure 3. AHMM4GES's nomenclature (Trad & Kalpić, 2020a)

The AHMM4GES includes a dynamic nomenclature that is used to facilitate the integration in any *Organization*. AHMM4GES's structure and is a set of coordinated modules, delivers solutions that correspond to various just in time processing schemes. AHMM4GES's nomenclature is the base of the DMS4GES, which is presented in Figure 3. AHMM4GES's instances support the DMS4GES, by using CSFs weightings and ratings (in phase 1) and is based on multicriteria evaluation.

Organization/Enterprise Architecture as an Applied Mathematical Model

A generic *Organizational* EA model and its Architecture Development Method (ADM) for GES (ADM4GES) are the kernel elements of this research. Where ADM4GES links DMS4GES's (and its internal

QLA4GES) microartefacts to the *Organization's* structure. The AHMM4GES and its underlining set of created instances is mainly a QLA4GES based on the HDT (Della Croce, & T'kindt, 2002). In each HDT's node a precise call to DMS4GES functions (or other) can be executed. GES's transformation model uses an objective function, for the maximization or minimization.

The Role of Enterprise Architecture

The Architecture Basics

Project's EA, known also as the *target architecture*, in which *Project* teams align the traditional *Organization's* EA's vision. The traditional *Organization's* EA layers, represents a silo model where it is very hard to melt down into an agile EA. In fact, it represents a hairball of silo sub-components of domain and technology entities. Moving to a standardized EA is the first step to a *just-enough* architecture.

Integration of the ADM4GES

ADM4GES's integration in *Project*s, enables the automation and auto-generation of AI and other microartefacts, throughout all ADM4GES's phases. The ADM4GES encloses cyclic iterations, where information about all EA phases' activities is logged. ADM4GES's is not dedicated to any specific *Organization*, domain, or technology platform.

Global Architecture Capability

Understanding the *Organization* and adapting it to an optimal EA model, assumes that the *Manager* is capable of optimizing all the *Organization's* heterogeneous and dislocated processes, into a holistic integrated GES. A GES is agile can be adapted to any *Organization's* EA strategy. *Managers* know that the effective management and integration of data-information through ICS' related technologies, is a key CSF to *Project's* success and an indispensable means to achieving GES's *sustainable competitive advantage*.

Project Risk Readiness Assessment

Project Risk Readiness Assessment has the following characteristics (The Open Group, 2011a):

The *Manager* must have in-depth knowledge of EA's *Business Transformation Readiness Assessment (BTRA)* procedures, which means that he has the *Capacity to Execute* and the ability to perform all ICS' tasks, which are required by the *Project*, including the skills, tools, processes and management of capabilities for the *Project's* implementation phase.

The *Manager* must also design the *Enterprise Capacity to Execute*; which is the ability of the *Organization* to execute the tasks required by the endeavour, in areas outside of ICS, including the ability to make decisions, using the built-in HDT's reasoning model, within the defined time constraints; that is very typical for complex *Projects*.

Project Risk Activities

Project Risk Activities include the following requirements and characteristics (The Open Group, 2011a):

- The *Manager* must identify the *Business Transformation Risks and Mitigation Activities*.
- The proposed recommendations curriculum enforces the *Manager*s' profile. Where, the *Manager* uses the ADM4GES to manage the implementation phase.
- Transformation Readiness skills.

EA can perform all *Project's* tasks, including selecting and defining tools and processes. The *Organization* has a demonstrated ability to deal with GES and skills enforcements curriculum management and requirements. The curriculum for Transformation Readiness has the following characteristics (The Open Group, 2011a):

- The *Manager* who has a profile of an Architect of Adaptive GES (AofAGES), which is an extension of the previous AofABIS profile, must have in-depth knowledge of framework's and *BTRA*. Which means that he has the capacity to execute all GES related tasks and activities required by the *Project*, including the holistic management skills, modeling background, AI modules, GES processes, and hands-on management capabilities for the implementation of the transformation.
- In the last years, there has been successful execution of similar complex projects, and there are appropriate standardized processes, methods, modeling skills, and a heuristics-based model for deciding what skills and activities are needed.
- The *Manager* must also design the *Organization's* capacity to function, which is the ability of the *Organization* to implement GES's modules, in areas related to ICS and AI technologies, including the DMS4GES, by using HDT's reasoning model, within the limited time constraints.
- The *Manager* has to demonstrate the ability to manage and integrate a DMS4GES, related issues and GES requirements.

Business Integration and Inter-operability

GES's Integration has the following requirements and characteristics (TOGAF, Catalog, 2011): 1) Integration supports the *Organization's* link with GES's eco-system and various modules, which in turn insures its sustainability; 2) Inter-resources operability is supported by an interchangeable format, that makes the *Organization's* interfaces generic, standardized and independent; 3) EA tools support the serialization of GES processes that use serialized and standardized files format; and 4) This interchange format supports GES's integration process, that facilitates the use of the interaction matrix, which shows the mapping between the services and functional domains.

Entity's Infrastructure and Business Development Environments

Managing GES's infrastructure, by the *Manager,* implies that he must be capable of modeling the transformed agile platform that is based on: 1) Resources sharing; 2) High availability; 3) Load-balancing; and 4) Voluminous data storages. *Organization's* security is also important, where the *Manager* has to have the skills needed to define GES standards on how to design and implement security concepts for processes, in a way to protect GES's logic from being copied, so the *Organization* can avoid erosion. There are many modeling strategies to achieve that goal.

Tools for Architecture and Modeling

*Manager*s who focus on delivering business outcomes must understand that *Project*'s EA tools, which comprise an important investment that can be wasted if not prepared correctly and used. Selecting and adapting any tool requires also understanding the vendor placement in the market. A tools roadmap is centralized and inter-operable across the entire GES.

Assess Readiness for Business Transformation

A BTRA can be used to assess GES's readiness to undergo a *Project*, where this assessment process is based on the analysis (and rating) of a defined set of readiness CSFs. The results of the readiness assessment are combined with a capability assessment process. These results are then used to shape the scope of the EA, in order to identify the activities required within the GES and to also identify the eventual risk areas (The Open Group, 2011a).

Identify the Transformation Risks and Mitigation Activities

Used to identify the risks associated with the *Architecture Vision* concept and to assess the initial levels of risk (like, catastrophic, critical, marginal, or negligible) and the potential frequency associated with them. A mitigation strategy for each risk must be also assigned (The Open Group, 2011a).

Confirm Readiness and Risk for a Project

Used to review the findings of the *BTRA* that was previously conducted in *Phase A* and to determine their impact on the *Architecture Roadmap* and the *Implementation and Migration Strategy*. In this phase, it is important to identify, classify and mitigate risks associated with the *Project*. All risks are documented in the *Consolidated Gaps, Solutions and Dependencies* matrix. *Project's* implementation requires knowledge and awareness of GES's transformation CSFs that impact the visionary state, in which evolution ICSs CSFs are crucial. GES's *Implementation and Migration Plan* must take both into consideration and neglecting them and focusing on the ICS will result in a fragile GES (The Open Group, 2011a).

Lean and Automated Systems for an Agile GES

Project's success is also measured by intangible CSFs and benefits because they insure its long-term *Organization's* survival. These agile mechanist *Organizations* needs a generic approach based on Service Oriented Architecture (SOA), that has created a deep paradigmatic shift in GES. It is replacing colossal monolithic traditional systems with its traditional applications, which split across GES.

AI based Security for the DMS4GES

AI systems management refers to expert systems and global systems modelling, which is supported by the EA's mapping concept. AI systems management is an approach for building and deploying intelligent systems and it replaces conventional GESs with DMS4GES (Daellenbach & McNickle, 2005).

GES Services

Cross-functional GES's concept permits the linking of *Organization's* components using the ICS, automated domain processes and services. The unbundling of the monolithic GES, is modelled by the *Manager* who must have extensive skills, he breaks down the actual monolithic GES into a repository of services. This is basically an alignment of GES's resources that is based on the 1:1 concept. A GES must support a variety of different actors including browsers, browsers, and native applications. GES handles service requests by executing processes (Richardson, 2014).

Architecture and Modeling

Architecture and modeling strategy for the selection, modeling strategy, education, and training framework, is to establish a modeling pattern that plugs-in a standardized EA and the unified modeling language methodology.

Data Modeling Pattern

The complex description of data models and related modelling patterns, does not do depend on the types of databases that are used; but the diversity of data-sources generates major problems in *Project*s, especially in its implementation phase.

Knowledge Management Pattern

The processes has to persist GES knowledge and today there are the following artefacts: The process-oriented knowledge management framework will be applied for the *Project*'s knowledge management component that will help in the selection, modeling strategy establishment and training activities which will use just-in-time knowledge assistance. It will also help the *Manager*s in updating and delivering the acquired knowledge on…

Integrating a Continuum

EA supports the *Manager* to coordinate *Projects*, by linking GES and its ICS. CSFs and recommendations are the base of a tuneable RAI4GES. *GES* recommendations are needed for finding the optimal *Managers*' profiles needed to manage the design and implementation of *Projects*. There has been a lot developed and written on enabling success in *Projects*, but the author proposes to inspect why *Managers* fail in the implementation phase of *Projects*. That is mainly due to the *Managers*' lack of knowledge in managing integration and implementation of a continuum.

Management of Resources, Artefacts and CSFs, Using AHMM4GES

TRADf's mapping strategy is used to relate and assemble the *Project*'s microartefacts, requirements and resources. This mapping concept is used to automate the building and deployment of *Project* microartefacts' instances in all *Project's* phases; and is based on DMS4GES that maps the *Project's* microartefacts to CSFs (The Open Group, 2011a). The *Project*'s must define the initial set of CSFs.

The Role of Finance

AI based Financial and Technology Strategies

AI has transformed Financial and Technology (FinTech) offering and improved capabilities that depends on the used platform. Banks have spent $5.6 billion USD on AI and Machine Learning (ML) platforms in 2019, which is a fraction of profits that are estimated to $250 billion USD. Where the main CSFs are, automation of tasks, to focus on strategic objectives, to support customers and to detecting fraud and financial crimes. FinTech's main activities areas are (Buttice, 2020):

- *Fraud Detection and Compliance:* according to Alan Turing's Institute, with $70 billion USD spent by banks on compliance tasks in the U.S. The amount of money spent on fraud is staggering. AI is important in detecting financial fraud. ML can process massive data points in seconds and to identify erroneous transactions.
- *Improving Customer Support:* a critical application of AI in FinTech is customer service. Chatbots are a dominate capacity in all other verticals and are also gaining ground in the banking industry.
- *Preventing Account Takeovers:* an important part of our private identity has become public, and cybercriminals steal private data to access people's accounts and assets.
- *Next-gen Due Diligence Process:* mergers and acquisitions due diligence is an intensive process, requiring an important workload, a large set of paper documents and physical space to manage and store the data. Today the scope of due diligence is more ambitious, encompassing ICS, intellectual property, tax information, regulatory norms, and many other topics. AI and ML are transforming this field and adapt rapidly.
- *Fighting Against Money Laundering:* detecting money laundering and terrorist activities financing schemes are the most important challenges. AI, Artificial Neural Networks (ANN) and ML algorithms are more efficient than traditional statistic method in detecting financial crimes and organized predators.
- *Data-Driven Client Acquisition:* like any sector with different players offering services to a customer base and where competition exists. Efficient marketing is vital to acquire clients and AI/ML assists by applying behavioral and risk mitigation intelligence. AI based research and global information supports the understanding the drivers of churn and customer acquisition.
- *Computer Vision and Bank Surveillance:* in the U.S., Federal Reserve and banks are targeted by 3,000 robberies every year. Vision-based and recognition applications are used to support security systems.

- *Easing the Account Reconciliation Process:* account reconciliation is a sensitive point in the financial closing process. *Organizations* face account reconciliation challenges which is a tedious and a complex process that is managed by AI/ML processes.
- *Automated Bookkeeping Systems: Organizations* are often challenged by complex back-office's activities. AI based automated bookkeeping can assist *Organizations* in complex back-office tasks, from accounting to managing payrolls. Applying ML with custom rules, processes, and calculations, supports the system to combine various data sources and to identify transaction patterns.
- *Algorithmic Trading:* the first Automated Trading Systems (ATS) was implemented in the 70's, algorithmic trading reached new heights dur to AI systems. It is not only about implementing rules to trade on the global markets, modern ATS can learn from data structures by using ML (and deep learning).
- *Predictive Analytics and the Future of Forecasting:* accurate cash forecasting is particularly important for treasury professionals to fund distribution accounts, make optimal decisions for borrowing (or investing), maintain target balances, and satisfy all regulatory requirements. Business professionals are unable to forecast by using many variables (or CSFs) required for the correlation and regression analysis processes. Predictive analytics uses ML, data mining and modeling to historical and real-time QLA4GES to predict events and enhance cash forecast.
- *Detecting Signs of Discrimination and Harassment:* various types of dynamics exist in financial services, especially since it is an industry dominated by predators. Awareness has increased and many *Organizations* filed discrimination complaints and they were retaliated against, which means that the majority of victims are demoralized.

The Role of Accounting

Predator Tactics

Concerning predator financial tactics, where the most damaging fact, is that the *Project* fails, what can negatively affect the *Organization's* sustainability and it can leave it to become prone to rigorous accounting austerity procedures. In this article, the author proposes a set of recommendations on how to avoid such blocking and damaging situations. Today many advanced RAISGES related finance and accounting automation concepts exist. This article can support *Projects* through the automation of all its financial operations and their related accounting processes. That also enables the underlying RAISGES to control accounting systems which interacts with global eco-systems. The RAISGES can detect predator's resulting financial problems, crimes, and irregularities.

Automated Accounting

RAISGES promotes financial engineering that uses references to various types of asset management and related financial activities, like in the case of *Project's* accounting activities. These activities are conducted by different types of avant-garde governance, ICS, and business service technologies. The current form of integration is based on block-chains' automation. The RAISGES can be applied to many types of *Project* accounting engineering subfields. *Organizations* are encountering pressure to manage their assets proactively and holistically, to ensure their ethical integrity and to avoid predators' scenarios. A *Project* needs a just in time decision making, planning and optimization activities; and to achieve that goal, the designed *Project's* process manages the inventory of the *Organization's* assets.

Organized Financial Predator's Strategy

OFPS Basics

The OFPS is based on the following facts and assumptions:

- Financial crime is in general considered as the financial aspects used in the support of religious terrorist acts. States applying state crime exists (Agger & Jensen, 1996), so various types of means are used to support state crime (like Switzerland), like religion, ideology…
- The use of psychology to stop all possible legal initiatives and even make predator related banks make substantial gains.
- The Nobel prize winner, the British economist, Angus Deatoon, warns about the destructive FPS (Le Monde, 2019). Such profiles can be classified as predator profiles.
- Destroying, various banking and financial institutions worldwide, which might be a menace for the predator-oriented banks. Like in the case of Lebanon… (Trad, 2019).
- Although FinTech can be used to tackle financial Cybercriminal, it seems that the countries that support massive financial crimes are making the largest investment in these innovative technologies (Ravanetti, 2016).

FPS Model

This section analyzes FPS' model that has the following main characteristics:

- The Swiss Union des Banques Suisse (UBS), is not just a bank, it is the skeleton of the Swiss financial system and closely related to the Swiss government apparatus…
- The Swiss UBS, in which 32 trillion US dollars are *hidden* in only one remote island, so the question is, how much money this so-called bank illegally detains? … (Stupples, Sazonov & Woolley, 2019).
- The Swiss locked-in Swiss model combines: 1) the power and blockage of the Swiss law; 2) Too Big to Fail banks are untouchable; 3) Banking secrecy; 4) Ultraliberal economy; 5) Rejection of local and global standards; and 6) A specific political environment.
- The peak of such a predator's behavior is the Fraud scandal related to the UBS that was hit with a historic fine and this incredible Fraud crime, was openly supported and protected by the Swiss Federal Court that makes FPS a state model (Alderman, 2019; Tagliabuejune, 1986).
- Accountancy crimes, committed by FPS accountants are daily business (Cornevin, 2020).
- There are many predators Fraud cases that damage practically all countries, like the USA, France, Germany, Greece, many African countries, Lebanon and many other… The hidden capital is reused as a credit to some of poor countries.
- Some credible sources like the Global Forum on Transparency and Exchange of Information for Tax Purposes peer review in 2011, has identified important deficiencies in the legal foundations for transparency and corruption, especially in relation with effective exchange of information (OECD 2011, 2014).
- In the USA, a federal judge accused the UBS of causing *catastrophic* investor losses in residential mortgage-backed securities sold before the 2008 financial crisis that caused more than $41 billion of damage of subprime and other risky loans in 40 offerings (Stempel, 2019).
- The financial crisis of 2007 (that lasted to the year 2009) was marked by widespread fraud in the mortgage securitization industry (Fligstein & Roehrkasse, 2019).
- 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.
- The Role of Education and Ethics; the Nobel prize winner, the British economist, Angus Deatoon, warns about the destructive predator professionals, graduating from business schools and he recommends stopping this type of brutalities. The leading school with such a

perception is the Chicago school and the Swiss HEC (Le Monde, 2019). Such profiles can be classified as predator profiles which should be filtered from a GES system.

Locked-in Situations and Building a Vision

RAISGES must define basic rules and objectives, to avoid financial locked-in situations. Locked-in situations can be defined as follows, "*a situation where an investor is unwilling or unable to exit a position because of the regulations, taxes or penalties associated with doing so. This may be an investment vehicle, such as a retirement plan, which cannot be accessed until a specified retirement date*". Financial or technological (or even a combination) locked-in, is when building the financial and technological structure of a GES system. The *Project* team and *Manager* must be cautious of eventual various devastating locked-in scenario(s). Even though some countries like Switzerland offer attractive financial and tax package(s), this country applies a coordinated legal and financial locked-in trap; it is a sealed system and represents an unwritten concept that can at any moment sweep out the financial resources from any business environment and even powerful countries like, the USA and France. Swiss banks and other Swiss financial institutions are under no supervision, whatsoever and they are free to operate using hit and run tactics. That indirectly makes this country, the financial industry's super protector that sets up fortifications against any possible legal intrusion; even when these institutions are executing massive irregular, criminal and illegal activities (International Monetary Fund, 2009). FinTech based locked-in, implies that technologies in the actual financial domain, influences its productivity, growth, and monetary policy. It supports also sophisticated predator crime schemes. It is a technology-driven domain and because of its hyper evolution depends on technology, the financial institution can be driven easily in a locked-in situation (Balling, Lierman & Mullineux, 2003). RAISGES should avoid adopting a unique tool, the so-called all-in-one FinTech tools.

Slavery and Financial Aggressiveness

Looking at the cultural background, the legendary Germanic (mainly Germans, Swiss and Austrians) hatred of Semites and their support of the great Ottoman genocides, added to the fact, that major Nazi officers became consultants of pan-Arab genocidal dictators and executive bankers of major Swiss banks. There is also the case of slavery, discrimination, and racism in Germanic central Europe and more specifically in the regions of the peace-loving Helvetic Confederation, where Swiss historians, who are supported by dozens of major public figures, launched a committee that inspects the case for *organized and structured worldwide slavery*. This massive case of slavery was directed and managed by Swiss bankers and political leaders. This committee's main aim is to estimate reparations in the context of Switzerland's related organize slavery crimes against humanities. In these crimes' major Swiss high-level politicians, trading companies, world class banks, cantons (like the Canton of Vaud, who still carries a slavery apartheidic mentality), predatory family enterprises, mercenary contractors, soldiers, and private individuals. All mentioned Swiss organizations profited from organized slave trade. Switzerland organized financial links to the slave trade and can considered global predators of manhood and nationhood. These facts show this nation's culture of financial greediness that comes out always, exactly like in the period of the second world war and the case of plundering of victims of the Holocaust (Swissinfo, 2019).

Legal and Regulatory Constraints to be Integrated

To design and implement an adequate regulatory component, there is a need to implement an AHMM4GES based legal intelligence module (Gray, 1997). The International Organization of Securities Commissions (IOSCO) identified 8 areas that constitute what is called FinTech. Such areas are payments, insurance, planning, trading, and investments, blockchain, lending/crowdfunding, data and analytics and security. The growth of the FinTech market implies several relevant issues and risks from a legal and

governance perspectives. In this respect, financial regulation is increasingly complex with major financial entities required to comply with strict regulations in various jurisdictions. Like in various sectors, the complexity for regulators is to find the right balance between FinTech, national cultures and the need to regulate them correctly. Based on the European Banking Authority's report on prudential risks and opportunities, there are legal issues that must be considered when dealing with FinTech.

The Role and Fundaments of AI based Security

Managing Passwords

To The RAI4GES ensures *Entity's* passwords' management that have a complex pattern, and which cannot be hacked easily. An ICS actor should have different usernames, security dongles and passwords for different systems; that can be enforced by voice, biometric; visual recognition …

Firewalls

A firewall is an important EA, RAI4GES and Cybersecurity element, which is used to protect an *Entity's* distributed network(s) from Cyberattacks in the form of malware and other types of dangers. There are many types of firewalls, and they have different security capabilities; therefore, the RAI4GES defines a firewall metamodel.

Secure Development and Operations

To block Cyberattacks, Secure DevOps (SecDevOps) can be integrated with the ADM4GES. SecDevOps integrates security in the development and operations processes, by using sets of best practices designed to support *Entities'* implementation processes. Applications development and operations are coordinated by a secure DevOps process managed by agile methodologies. SecDevOps manages developers, operations, and security team members. The RAI4GES uses agile SecDevOps procedures to identify patterns for managing transformation and development (Mees, 2017).

Antivirus, Viruses and Worms

Antivirus software applications are used to detect and remove threats known as viruses. The main recommendation is to keep *Entity's* applications and modules updated for the *Entity's* optimal defense strategy and concept. A Virus is a piece of software that is installed on the *Entity's* ICS without an official approval and operates without official control. The RAI4GES proposes various security controls to protect the ICS against Cyberattacks, like viruses, worms or trojan horses. Cyberattackers and Cybercriminals use ICS' vulnerabilities to install pirate code like worms, in the *Entity's* database(s), by using badly intentioned SQL instructions. Such misdeeds give Cybercriminals, access to profitable login credentials information.

Emails

Electronic mails (Email) can be dangerous, because they may contain attachments, when opened can launch applications or scripts that can modify the ICS. The main recommendation is not to open email attachments from unknown, spam or anonymous expeditors. Email attachments could be infected with malware or any kind of spyware software. It also recommended not to use embedded hyperlinks in emails that are issued by anonymous senders or unknown web links. These are the common patterns in which malware is dispatched on ICS' endpoints.

Wireless Fidelity

ICS' mobile endpoints should block: 1) The connections to open Wireless Fidelity (WIFI) connections in public serviced sections; and 2) It should also block unauthorized smart devices like cellphones from connecting to the ICS. Connections to unprotected network endpoints makes ICS nodes vulnerable and

Cyberattackers may use *Man-in-the-Middle* tactics and this the most popular types of WIFI Cyberattacks; where on open WIFI network endpoints, Cyberattackers can *sniff* network packets. In RAI4GES and Cybersecurity, a Man-In-The-Middle, Monster-In-The-Middle, Machine-In-The-Middle, MitM or Person-In-The-Middle (PITM), in which Cyberattackers secretly listen and can alter the communications between endpoints.

Malware

The term Malware derives from *MALicious software*, which is an application that infects and damages the ICS without authorized permissions; the RAI4GES should use the following mechanisms to block: 1) Viruses by integrating Antivirus modules that also block Malicious intrusions; 2) *Activate Network Threat Protection* strategies; 3) Firewall installations; and 4) Trojan horses' detection. Trojan horses are email Malwares which make multiple installations on the ICS to leak information and make substantial damages. These types of viruses are the most damaging ones.

Capacity building – Skill & Competence development

The ADM4GES supports the RAI4GES to create best practices and *Entity*-specific security capabilities. The RAI4GES supports EA and security experts to avoid missing critical security pitfalls, and this chapter offers recommendations on the needed skills to carry out AIbS activities. The AIbS is treated as a separate architecture domain within the EA, which fully integrates it. AIbS is the enforcement of the *Entity's* security policies which includes the following AIbS skills and characteristics (The Open Group, 2011a): 1) Security methodology; 2) Management of discrete views and viewpoints; 3) To design non-normative flows through the ICS; 4) To design single-purpose components; and 5) To develop EA, AIbS and ICS models.

Guidance on Security for the Architecture Domains

AIbS requirements are pervasive in all EA domains and to all ADM4GES phases. Security focuses mainly on the infrastructure that is not visible to the *Entity's* business function. RAI4GES focuses on the protection of the ICS and *Entity's* assets. AIbS manages single-purpose components and measures the quality of the ICS. Common AIbS artifacts can include: 1) Business rules for handling of data/information assets; 2) Defined security policies, 3) Codified data/information assets' ownership and custody; 4) sRisk analysis documentation; and 5) Data classification policy documentation. The *Entity security* view of the EA has its own unique building blocks, collaborations, and interfaces. These security-unique blocks must interface with the *Entity's* ICS in an optimal manner, to support its security policies and to avoid interfering with ICS operations. AIbS is effective to design and implement security-specific controls in the *Target Architecture* in the initial development cycle to support reengineering development and deployment. The RAI4GES manages the normal flow of application's 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 ADM4GES phases, recommendations are given on security-specific management. AIbS decisions are traceable to business and policy decisions and their sRisk management. The areas of concern for the AIbS are (The Open Group, 2011a):

- Authentication: The substantiation of the identity to the *Entity*.
- Authorization: The definition and enforcement of permitted capabilities for a person whose identity has been established.
- Audit: The ability to provide forensic data confirming that the ICS has been used in accordance with AIbS 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 services' 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.

Security Monitoring and Logs

The RAI4GES is not dedicated to any specific environment, and it offers to support: 1) Performance and availability; 2) Reliability and recovery; 3) Attack's tracing; and 4) Cybersecurity fundaments. The ICS is controlled and monitored in real-time, using the *Entity's* Unified Logging Subsystem (EULS) and is integrated to support the RAI4GES. EULS' exist and are powerful monitoring subsystems that support the presentation, sorting and tuning of stored logs. EULSs can be designed to analyses, collect and store security related data from various ICS sources to support the central logging system. An ICS continuously needs to manage massive central logging system that persists event logs, sorts of security logs for security purposes and system performances.

The Legal Constraints

The RAI4GES supports the *Entity's* legal integration and constraints and in order to achieve this legal support, CSFs are selected and asserted, to monitor the used artefacts. These CSFs manage the differences in Cyberbusiness' local and international laws. An *Entity* or Cyberbusiness environment must have the capacity to proactively recognize erroneous Cybertransactions and Cyberattacks, in a systemic manner (Daellenbach & McNickle, 2005).

Cybertransactions' Security Violations

The European commission defines a legislation to govern *Entity's* Cyberbusiness activities; and progress has been done in this direction. European commission's member states have implemented and enforced Cyberlaws related to national practices. Cybertransactions outcomes have to be continually legally asserted, verified, traced and their periodic summaries are reported to the *Entity's* executive management (Fu & Mittnight, 2015). Cyberbusinesses are orthogonal to global Cybersecurity requirements, where the *Entity's* role defines the responsibility of its resources. Management of the *Entity's* legal interests, resources, and accesses should be managed by EA, AIbS and security experts. Thus, the Cyberbusiness structure is an important consideration in the legal assertion and access management of Cybertransaction's security. The regulation for the Cybertransaction's security and law needs qualified timestamps for robust electronic certification like those used in the European Union (European Union, 2014).

Cybertransaction law

Cybertransaction is 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 *Entity's* Cyberbusiness and electronic government activities. Many *Entities* have adopted Cyberbusiness and electronic government regulations. The Uniform Electronic Transactions Act represents the first effort in providing some standardized rules to govern Cybertransactions and Cyberlaws. Facts show that international law on global security is inefficient and are in an agonizing state. Advanced states are hesitant to integrate international law that is 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 (Mačák, 2016).

Cyber business Legislation Monitoring

The integration of the RAI4GES is done with the use of TOGAF's standardized legal environment. This legal environment supports data protection laws, contract law, procurement law, fraud law and many other legislation domains to counter OFPS misdeeds, which are the most fatal types of crimes and Cybercrimes.

Financial Cybercrime Schemes

FinTech and ICS are crucial for an *Entity* and its financial controls critical system(s). Today such FinTech standards and fields are robust, resilient and can be applied as automated synchronized (block) chains; to enable the traditional financial environments to become a part of a networked financial world. FinTech platforms can be applied to support an RAI4GES and sRisks mitigation, to avoid locked-in situations. OFPS related locked-in, when building the financial structure of the future transformed *Entity*, the *Project* team and RAI4GES must be cautious of eventual financial locked-in situation(s), which is a major security problem. Even though some countries like Switzerland offer attractive financial and tax package(s), this country applies a coordinated legal and financial locked-in trap; it is sealed and represents an unwritten concept that can at any moment sweep out the financial resources from an *Entity* and even powerful countries like the USA, UK, and France. This locked-in Swiss OFPS model, combines: 1) Specific culture and mentality; 2) The power of Swiss law; 3) Too Big to Fail state banks; 4) Banking secrecy that protects financial crimes; 5) Ultraliberal economy; 6) rejection of local and global standards; and laws; 7) Isolationism and racism; and 8) A finance supportive political environment for collective plundering. Swiss banks and other Swiss financial institutions are under no supervision whatsoever; and are free to hit and run. That indirectly makes this *Entity* the financial and malware industry's super protector that sets up fortifications against any possible legal intrusion; even when these institutions are executing massive irregular, criminal and illegal activities.

The author refers to this phenomenon as an instance of the Black Swan phenomena or simply the directed Swiss Black Swan, which *Entity's* (and countries) should try to avoid and penalize. It is probably wiser to pay more taxes and social services then to face such phenomena and traps (International Monetary Fund, 2009. The major problem with combating such a system is that some countries have hermetically closed system characterized by the following attitudes: 1) Police and information services, blocking any attempt to pursue financial criminal acts; 2) The legal system, ignoring any attempt to investigate financial criminal acts; 3) Legal support too expensive, to discourage any action of law enforcing; 4) Psychological harassment, to discredit investigators; 5) Intolerance and discrimination, to block any foreign request; 6) A powerful global network, to embed and hide various dubious operations; 7) Financial guerrilla-like and hit and run tactics, to confiscate wealth; and 8) Occurrence of financial locked-in situations. Some financial haven states target to become leaders in FinTech, which is not very assuring; because FinTech should combat state criminality and enforce global security international law. It is recommended to avoid any form of financial and technological collaboration with OFPS oriented *Entities*.

The Role of Global Education and Profile Definition

RAI4GES supports GESs and the profile's selection, which will hopefully help to minimize *Project's* failure rates. Profiles depends on the type of activity. The RAI4GES can be used in various GES's subdomains, and it helps in the *selection* of the future *Managers*, who can design the change processes. Such Managers are also specialized in designing solutions endemic to *Projects* (Doyle, 1995).

The Anglo-Saxon Model

The college degree choices of Jeff Bezos and other CEOs like, Bill Gates and Mark Zuckerberg who dropped out of college, but they became wealthy entrepreneurs. In this model, a degree is not a step to success. Ultimately, if getting mega-rich from business is a goal, there is no prescribed path. Success has to do with meeting the right opportunities and specific way lessons are interpreted. Mark Zuckerberg, Bill Gates, and many others, did not even complete their degrees (Schwantes, 2020). These facts are pushing the notions of certifications that are considered more valuable than university degrees.

The European Model

Mainly the European continental part can be presented with the case of Serge Dassault, a French engineer, businessman and politician. He was the chairman and chief executive officer of Dassault Group. He graduated the prestigious École Polytechnique, SUPAERO and HEC Paris. This is the case of many European *Managers* and will this tendency continue is an uncertainty.

Instructional versus Academic Organizations

The main differences between these two disciplines are (Rob & Roy, 2013):

- Certifications attract hiring *Manager*s, who suggest the implementation of certifications in traditional university programs.
- Certifications have been integrated in university programs and there were difficulties because certifications are based on commercial tools. This is a very commercial approach.
- The frequent changing nature of certifications is every two years.
- Certification programs can improve traditional lecturing and converge with standards.
- Students are interested in certifications.
- This can on the long-term, lock in many countries and *Organizations*, as AI tools come from a single mainstream.
- Certifications are superficial and can just assist a specialist, but an academic diploma stays essential.
- Ethical Principles

This research and framework on the following main ethical principles (Murray, 1996):

- Content competence: a university professor or teacher maintains a high level of matter knowledge and ensures that his courses' contents are ethical, current, accurate, representative, and appropriate to the program of studies and global ethical standards.
- Pedagogical competence: a pedagogically competent professor communicates the main courses' objectives to the students. And he is aware of possible instructional methods or strategies and adapts methods of teaching to research realities (including personal or self-reflective research). These methods should be effective in helping students to accomplish the objectives.
- Dealing with sensitive topics: students would find sensitive or discomforting topics embarrassing and that is why such topics should be presented in an open honest and didactical manner.
- Student development process: the teacher's responsibility is to contribute to the intellectual development of the student (in the teacher's area of expertise), and he should try to avoid actions such as exploitation and discrimination that detract from student development.
- Dual relationships with students: to avoid conflict of interest, a teacher does not enter into dual-role relationships with students. Such relationships may detract from students' development or may drive to favoritism on the part of the teacher.

- Confidentiality: student behavior, grades, attendance records and private communications are dealt with as confidential resources and are released only with student consent, or for legitimate academic purposes, or if there are reasonable grounds for believing that released communications will be beneficial to the student and the educational environment.
- Respect for colleagues: a university teacher respects his colleagues and works cooperatively with colleagues in the interest of academic development.
- Valid assessment of students: the importance of assessment of student performances in higher education is the teachers' responsibility. Where he makes the right steps to ensure that assessments are valid, fair, and congruent with course objectives.
- Respect for institution: in the interests of student development, a university teacher is aware of and respects the academic objectives, rules, and standards.

The author would add the following:

- To avoid the production of future predators, whose only goal is to gain a lot of money educational *Organizations* must include objectives other than just making money (Le Monde, 2019).
- To privilege ethics and to present cases of fraud and financial criminality like the case of the UBS and Switzerland, which are anti-academic (Stupples, Sazonov & Woolley, 2019).
- To promote Nelson Mandela's moto, which is, *education is the most powerful weapon which you can use to change the world…*
- Jules Ferry, the legendary French minister of education, privileged the approach in making men equal in their rights, dignity, mutual respect to replace animosity. He used the moto, *with unequal education, I challenge you to never have equal rights, not theoretical equality, but real equality and equal rights is the very foundation of democracy...*

Manager as a Cross-Functional Architect

Enterprise Architecture

Understanding *Organizations* and the CSFs that can influence their survival and competitiveness, is only the first step towards a successful *Project*. The *Manager* must have in depth knowledge of: *Project* architecture and its development management, businesspeople integration, agile project management and management of computer engineers. The *Manager* acts as solution designer and implementation architect. Accordingly, this research unifies resources from distinct but related areas: business processes, ICS infrastructure and *Project* resources. EA develops concepts for the *Manager*'s selection and proposes a method to weight and inter-relate his various skills with CSFs. Estimating *Manager* skills requires a profound knowledge of the *Organization's* architecture, business processes, services, ICS, and *Project* management issues. That rounds up the profile of an AofAGES, which enhances the previous AofABIS profile, where he acts as a coordinator of GES teams, EA specialists and other activities (Trad, & Kalpić, 2013a, 2013b, 2013c).

Enterprise Architecture Skills

Another perspective of skills are the *Project*'s architecture modeling skills that typically comprises: 1) Detailed business modeling; 2) Business building component design; 3) Business applications and actor's role design; 4) Requirement engineering; and 4) Standardized business integration, etc.… EA is considered as a superset of Business, Data, Application, and Technology Architecture. A typical EA team undertaking the development of a *Project* architecture as described in TOGAF would comprise the following roles: 1) Architecture Board Members; 2) Architecture Sponsor; and 3) Architecture Manager.

Categories of Skills

An EA team skill set will need to include the following main categories of skills:

- Generic skills: comprises, leadership, teamworking, inter-personal skills, etc.
- Business skills and methods comprises, business cases, business process, strategic planning, etc.
- EA skills: comprises, modeling, building block design, applications and role design, systems integration, etc.
- Project management skills comprises, managing business change, project management methods and tools, etc.
- ICS general skills comprises, brokering applications, asset management, migration planning, SLAs, etc.
- Technical ICS skills: comprises, software engineering, security, data interchange, data management, etc.
- Legal skills: comprises, data protection laws, contract law, procurement law, fraud, etc.

Modeling Skills

Modeling strategy establishment skills comprise: 1) Business use cases design; 2) Business process modeling; 3) Business integration; 4) Strategic planning; and 5) services modeling, etc... The *Manager* must understand the business requirements, then he must probe for business information, influence *Project*'s team members, facilitate consensus in the implementation phase, synthesizes and translates strategic requirements into actionable tasks, manage CSF based risks, etc. The *Manager* participates in the discovery, modeling and design of the business scenarios that are the initial driving phase for the solution. The *Manager* manages the requirements and develops business models of components for the final agile business environment. Then he must tune these business models through iterations to fit all business scenarios.

The Profile, Curriculum and Pattern

GES's curriculum must comprise the knowledge of business modelling and EA, automated real-time process environments, agile project management, organizational behavior, AI, and ICS implementation know-how (Trad, & Kalpić, 2014a, 2014b). The profile and educational curriculum round up the AofAGES.

Managerial Educational Benefits and Recommendations

By Importance	
1	The Manager is an AofAGES
2	The Manager must have extensive experience in Projects
3	The Project must avoid a locked-in situation
4	Implement a light version of ADM4GES
5	An AI concept is a strategy and not a tool
6	Education and training, are academic and not a certification farm
7	The GES must define its own AI strategy
8	RAI4GES can be applied to any organization

Table 1: The list of recommendation

This research offers a set of GES recommendations and benefits. *TRADf*'s HDT uses the recommendations to give *Project* the possibility to tune the details of the AofAGES profile (Vella, Corne, Murphy, 2009).

The Proof of Concept

The PoC is implemented using *TRADf* which uses micro artefacts and the "1:1" mapping concept.

The Literature Review's Outcome

The quantitative part of the mixed method that is made up of the set of CSFs. The surveyed types of specialists and managers were: 1) Business and ICS school professors and directors, 2) Managers of information systems, 3) *Project* managers, 4) Human resources, 5) Educational professionals and transformation managers. The surveys confirmed the research RQ. The research shows that the *Manager* is an AofAGES. Therefore, a concrete *TRADf* was built and the PoC delivered the recommendations on how to select and train a *Manager* (Trad, & Kalpić, 2014a, 2014b; SAP, 2012a). The literature review process' (or Phase 1) uses the research's archive of references and links that are analysed using a specific interface. After selecting the CSA/CSFs and linking them to micro artefacts scenarios; this concludes Phase 1. The PoC (or Phase 2), that uses a grounded hyper-heuristic to process solutions to a given problem.

From Phase 1 to Phase 2

AHMM4GES's main constraints and the *Project's* components supports the PoC. A main constraint is that a CSA average must be higher than 7.5. In this PoC's CSA/CSFs evaluation, has an average result higher than 8, as shown in Table 2.

Critical Success Factors	KPIs	Weightings
CSF_RAISGES_TRADf_ResearchProject	Proven	From 1 to 10. **10 Selected**
CSF_RAISGES_EA_AIbS	Complex	From 1 to 10. **08 Selected**
CSF_RAISGES_DMS4GES	Feasible	From 1 to 10. **09 Selected**
CSF_RAISGES_Finance	Complex	From 1 to 10. **08 Selected**
CSF_RAISGES_Education_Ethics	Complex	From 1 to 10. **08 Selected**
CSF_RAISGES_Profile_Definition	VeryComplex	From 1 to 10. **07 Selected**

Evaluate

Table 2: The outcome of Phase 1 has an average of 8.30.

Phase 2, the Setup

The PoC uses *TRADf's* development environment to configure the DMS4GES and selects problems, actions, and applicable solutions to verify RAISGES's feasibility. The case study is a concrete insurance case.

Linking the Applied Case Study – Integration and Unification

The PoC and the ArchiSurance case with goals as shown in Figure 3, it analyses a merger, of an old system's landscape that has become siloed, that results in abundant data and code. The PoC, a financial auditing scenario.

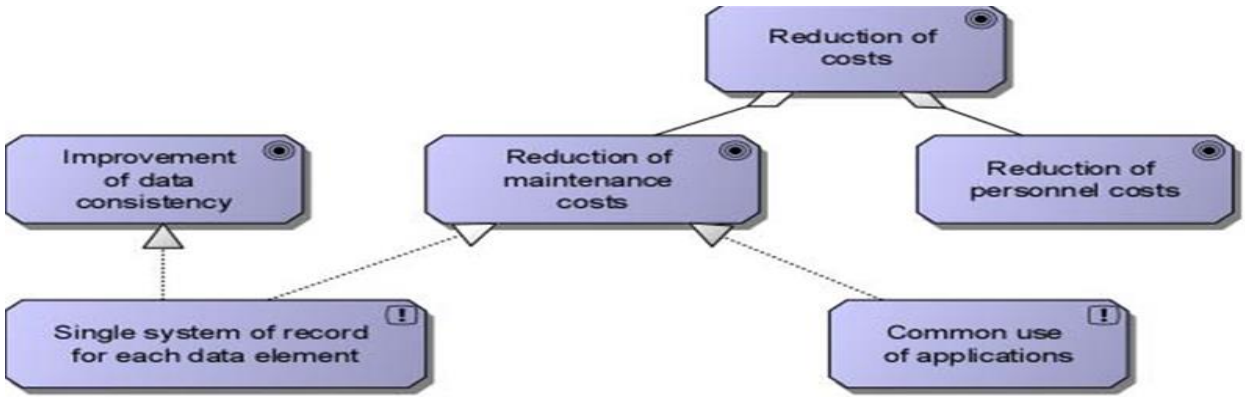

Figure 4. Transformation goals (Jonkers, Band & Quartel, 2012).

PoC's Processing on a Concrete Tree Node

In Phase 2, the hyper-heuristics approach is used, to find a combination of heuristics' action, used to solve a problem related to the RQ. A selected CSF is linked to a problem type and a related set of actions where the processing starts in the root node. Each problem, like this case the PRB_GES_Single Data Record System problem, has the following set of actions:

ACT_GES_Single Data Record System Define Possible Audit Processing

For this DMS4GES related PoC, the author has selected the CSF_GES_Single Data Record System_ Validation as the active CSF, taken from the CSFs pool. In this PoC the goal is to find solutions related to this selected CSF's related problems. The author has decided to apply the AHMM4GES based reasoning to try to solve the CSF_GES_Single Data Record System Validation issues and the related problem or the PRB_GES_Single Data Record System_ Validation, which is solved by using the following steps:

- Relating the case infrastructure and financial transactions' integration capabilities to CSF_GES_Single Data Record System_ Validation capabilities is done in Phase 1.
- Link the processing of this node to the pseudo-quantitative modules, then by using qualitative modules, filter and deliver the initial state that is the root node of the HDT.
- The internal heuristics engine is configured, weighted, and tuned using configuration information.
- The set of possible solutions results from HDT processing. Then the reasoning engine is launched to find the set of possible solutions in the form of possible improvements.
- From the *TRADf* client's interface, the development setup and editing interface can be launched to develop the finance related data services to be used in micro artefacts.
- Selected Node Solution in Phase 2

The development scripts make up the processing logic of the RAISGES's defined problems and is supported by a set of actions. Where these actions are processed in the *TRADf* background to support service micro artefacts that are called by the engine's actions, which delivers the solution.

Conclusion

The empirical phase of this research tries to prove the RQ and delivers an optimal GES profile definition of the *Manager* and a set of recommendations. GES's characteristics are needed to holistically manage the design and to implement an educational environment. More specifically, the author gives an overview of the research in grounded hyper-heuristics model internals, used by the DMS4GES. The research's most important findings are:

- *A concrete framework*: *TRADf* is a concrete framework used to implement an RAI4GES.
- *Knowledge gap*: The literature review found a gap between the traditional approaches and needed GES.
- *Evolutionary mixed method*: This research uses a AHMM4GES to create: 1) the role of AI for GES; 2) the *Manager* profile; and 3) GES prerequisites.
- *The PoC:* delivered the research's recommendations on how to implement an RAI4GES.
- *Manager Profile and educational prerequisites*: *Organizations* produce general profiles that can hardly cope with heterogeneous complexity and fast changes. These high frequency changes are mainly due to the hyper-evolution of AI and technology. The research confirms the role of *Manager* as a AofAGES.
- *Estimating of the Manager skills:* requires a profound knowledge of EA, SOA, AI, and agile project management; this rounds up the profile of an AofAGES.
- *Europe's and France's approaches:* are doing very well in the related academic fields, but concerning the industrial part, it is practically inexistant. It finds itself in a locked-in situation and it has to establish a strategy to join the major GES and AI and security players.
- This research delivers a concrete AofAGES profile.

References

Agger, I., & Jensen, S. (1996). Trauma and Healing Under State Terrorism. London: ZEB Books.

AMInfo. (2014). Middle Eastern clients in the HSBC Switzerland leaks. Swiss Leaks. Retrieved from http://ameinfo.com/luxury-lifestyle/list-middle-eastern-clients-in-the-hsbc-switzerland-leaks

Balling, M., Lierman, F., & Mullineux, A. (2003). Technology and Finance: Challenges for Financial Markets, Business Strategies and Policy Makers. NY: Routledge.

Buttice, C. (2020). Top 12 AI Use Cases: Artificial Intelligence in FinTech. AltaML-Techopedia. https://images.techopedia.com/top-12-ai-use-cases-artificial-intelligence-in-FinTech/2/34048

Cearley, D., Walker, M., Burke, B. (2016). Top 10 Strategic Technology Trends for 2017.

Cornevin, Ch. (2020). La police démantèle un vaste système de blanchiment de fraude fiscale... [Police dismantle massive tax fraud laundering scheme]. Le Figaro. France. Retrieved from https://www.lefigaro.fr/actualite-france/la-police-demantele-un-vaste-systeme-de-blanchiment-de-fraude-fiscale-20200110

Curtis, P., & Carey, M. (2012). Committee of Sponsoring Organizations of the Treadway Commission-Risk Assessment in Practice. Deloitte & Touche LLP.

Daellenbach, H., McNickle, D., & DYE, Sh. (2012). *Management Science. Decision-making through systems thinking*. 2nd edition. Plagrave Macmillian. USA.

D'Amato, G. (1995). Switzerland: A Multicultural Country without Multicultural Policies? In Vertovec, S. & Wessendorf, S. (Eds.) The Multiculturalism Backlash: European Discourses, Policies and Practices. NY: Routledge.

Della Croce, F., & T'kindt, V. (2002). A Recovering Beam Search algorithm for the one-machine dynamic total completion time scheduling problem, Journal of the Operational Research Society, 53:11, 1275-1280. Taylor & Francis.

Doyle, M. (1995). Organizational transformation and renewal: a case for reframing management development. Leicester Business School, De Montfort University, Leicester. UK.

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

European Commission (2019). Digital Single Market. FACTSHEET / INFOGRAPHIC4 July 2019. European Commission.https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe

Farhoomand, A. (2004). *Managing (e)business transformation*. Palgrave. UK.

European Union (2014). Regulation (EU) No 910/2014 of the European Par lament and of the Council - on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC The European Par lament and of the Council – Regulation. European Union.

Fligstein, N., & Roehrkasse, A. F. (2016). The causes of fraud in the financial crisis of 2007 to 2009: Evidence from the mortgage-backed securities industry. American Sociological Review, 81(4), 617-643.

Fu, Zh., & Mittnight, E. (2015). Critical Success Factors for Continually Monitoring, Evaluating and Assessing Management of Enterprise IT. ISACA.

Gartner (2016). Gartner's 2016 Hype Cycle for ICT in India Reveals the Technologies that are Most Relevant to Digital Business in India Analysts to Explore Key Technologies and Trends at Gartner Symposium/ITxpo 2016, 15-18 November, in Goa, India. Retrieved April 3, 2018, from https://www.gartner.com/newsroom/id/3503417

Gray, P. (1997). Artificial legal intelligence. London: Dartmouth Publishing Co.

International Monetary Fund (2009). Switzerland: Financial Sector Assessment Program - Detailed Assessment of Observance of Financial Sector Standards and Codes. NY: International Monetary Fund.

IIA (2004). Enterprise Risk Management — Integrated Framework. The Institute of Auditors.

Jonkers, H., Band, I., & Quartel, D. (2012a). ArchiSurance Case Study. The Open Group.

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

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. NATO CCD COE Publications, Tallinn.

McCarthy, J. (1989). What is AI? Stanford University. USA. http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

Mees, W. (2017). Security by Design in an Enterprise Architecture Framework. Royal Military Academy, Department CISS. Renaissancelaan 30, 1000 Brussel. NATO. Belgium.

Murray (1996). 9 Ethical Principles. Queens Univeristy. Canada.
https://www.queensu.ca/teachingandlearning/modules/ethics/04_s2_01_nine_ethical_principles.html

OECD (2011). Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Review: Switzerland 2011, Phase 1. OECD Publishing, Paris.

OECD (2014). Country Case Study 1: Lebanon. MENA-OECD ECONOMIC RESILIENCE TASK FORCE RESILIENCE IN FRAGILE SITUATIONS. 4-5 December 2018. Islamic Development Bank. Jeddah, Kingdom of Saudi Arabia. OECD.

Ravanetti, A. (2016). Switzerland Bank on FinTech with Lighter Regulations. Crowd Valey. Retrieved September 2019, from https://news.crowdvalley.com/news/switzerland-bank-on-FinTech-with-lighter-regulations

Rob, M., & Roy, A. (2013). THE VALUE OF IT CERTIFICATION: PERSPECTIVES FROM STUDENTS AND IT PERSONNEL. Issues in Information Systems. Volume 14, Issue 1, pp.153-161, 2013.
https://iacis.org/iis/2013/192_iis_2013_153-161.pdf

Richardson Ch. (2014). Pattern: Microservices architecture, available online at:
http://microservices.io/patterns/microservices.html

SAP (2012a). Business Process Management Business Transformation Academy. Germany.

Schwantes, M. (2020). Research Uncovers the Value of the College Degree Choices of Jeff Bezos and Other Obscenely-Rich CEOs... INC. https://www.inc.com/marcel-schwantes/research-uncovers-college-degree-choices-of-jeff-bezos-other-obscenely-rich-ceos.html

Stempel, J. (2019). UBS must defend against U.S. lawsuit over 'catastrophic' mortgage losses. Yahoo Finance. Yahoo. USA. Retrieved September 2019, from https://finance.yahoo.com/news/ubs-must-defend-against-u-214743943.html

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

Swissinfo (2019). Swiss launch committee on slavery reparations. Swissinfo. https://www.swissinfo.ch/eng/history-_swiss-launch-committee-on-slavery-reparations-/45421506

The Open Group, 2011a. The TOGAF. The Open Group.

TOGAF Catalogs (2011). Sample catalogs, matrices and diagrams, available online at: http://www.opengroup.org/bookstore/catalog/i093.htm

Trad, A. (2021a). The Security Management Concept (SMC). STF Conference. Turkey.

Trad, A. (2021b). The Military Technology Strategy (MTS). STF Conference. Turkey.

Trad, A., & Kalpić, D. (2011). The Selection, Training, Follow and Evaluation STF for Managers in Business Innovation Transformation Projects-A Holistic Overview. IEEE, Conference on Information Technology Interfaces. Croatia.

Trad, A., & Kalpić, D. (2013a). *The Selection, and Training framework (STF) for Managers in Business Innovation Transformation Projects - Overview of the development of the empirical model*. IEEE 2013, BAME. Venice, Italy.

Trad, A., & Kalpić, D. (2013b). *3rd position Award. The Selection and Training Framework (STF) for Managers in Business Innovation and Transformation Projects - The Design and Implementation of the Research Model*, IMRA, Croatia.

Trad, A., & Kalpić, D. (2013c). The Selection, and Training framework (STF) for Managers in Business Innovation Transformation Projects - The Literature Review. IEEE 2013, Centeris. Portugal.

Trad, A., & Kalpić, D. (2014a). *The Selection and Training Framework (STF) for Managers in Business Innovation and Transformation Projects - The profile of an Architect of adaptive business systems*. IMRA, USA.

Trad, A., & Kalpić, D. (2014b) *The Selection, and Training Framework selection and training framework (STF) for Manager's in Business Innovation Transformation Projects – Educational Recommendations*. EDEN; Zagreb. Croatia.

Trad, A., & Kalpić, D. (2016). *The Business Transformation Framework for Managers in Business Innovation Transformation Projects-A heuristics decision module's design concept*. ABRMR.

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

Trading Economics (2017a). Switzerland - GDP Annual Growth Rate. Trading Economics. Retrieved from http://www.tradingeconomics.com/

VELLA, A., CORNE, D. and MURPHY, C. (2009), *Hyper-heuristic decision tree induction*. Sch. of MACS, Heriot-Watt Univ., Edinburgh, UK.

Zaiane, S. & Ben Moussa, F. (2018). Cognitive Biases, Risk Perception, and Individual's Decision to Start a New Venture. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET). IGI Global. DOI: 10.4018/IJSSMET.2018070102