ENTERPRISE ARCHITECTURE PROFESSIONAL JOURNAL

FEBRUARY 2024

IN THIS ISSUE

EDITOR'S WELCOME

by Darryl Carr, EAPJ Editor

Welcome to the February 2024 Edition of the Enterprise Architecture Professional Journal. We serve practicing and aspiring enterprise architects, as well as those who apply the holistic perspective of enterprise architecture to other disciplines. EAPJ informs their daily work and benefits their careers with content that is focused, concise, authoritative, practical and accessible.

In this edition we have two feature articles, sharing the work and perspectives from four authors. These papers cover diverse topics, ranging from Zero Trust Architectures to the use of Enterprise Architecture to guide the implementation of an Integrated Quality Management System. This apparent diversity highlights the broad applicability of an architecture-led approach to change in organisations, regardless of industry.

We also have a note from EAPJ Founder, Dr Steve Else, talking about evangelism in the EA discipline, and being an ambassador.

In other news across the Architecture world, there has been significant work over the past two years to address the age-old problem of gender equality within the discipline. The creation of the Women in Architecture forum, off the back of some material published on International Women's Day in 2022 has led to a renewed focus on this issue, and the creation of regional communities, including WIA Australia which is being co-chaired by EAPJ Advisor Dr Christine Stephenson. There's much more to do, but it's great to see this topic being addressed.

There's also news from Australia where a group of experienced practitioners met in October 2023 with a focus on how to address some of the challenges that have plagued the Enterprise Architecture discipline for the past few decades. Their hope is to build working groups to find solutions to these challenges, and to move EA toward professionalization. We wish them luck and look forward to hearing more.

The team at EAPJ hope you enjoy reading this edition. Please contact me at editor@eapj.org with your questions, comments, ideas and submissions. As always, I look forward to hearing from you!

Darryl Carr

Editor, Enterprise Architecture Professional Journal

FOUNDER'S NOTE

by Dr. Steve Else, EAPJ Founder

YEAEA!
Your Enterprise Architecture Evangelist and Ambassador

(Pronounced "Yay!")

The Enterprise Architecture Professional Journal (EAPJ) is a platform for sharing practical articles and case studies on Applied Enterprise Architecture. I founded it over 10 years ago because no such site existed for this type of work. Yes, LinkedIn has a wealth of diffuse items on EA, often of great value, but many of the most thoughtful and valuable blogs and essays have found their way onto EAPJ.org, where they have had a lot more visibility since the site receives over 3,000 hits a month, even though it is not advertised.

A couple of graduate school programs offering classes on EA have also found EAPJ.org to be a great channel for EA professors and graduate students to be published, knowing that our awesome editor, Darryl Carr, sometimes with my assistance, shepherds promising submissions through the review process.

I have pondered lately how EA lacks a pure spirit and modern outlook to be an authority, evangelist, and ambassador for the profession. Personally, I have been in the EA business for over 20 years and I don't know whom to engage in for enthusiastic, top-notch collaboration on EA besides Iver Band, Alex Wyka, Alain de Preter, Christoph Bergner, Dr. Brett Brunk, and Darryl Carr. However, because of my trust and confidence in them, I am happy to lean on them to consider all aspects of EA to help explain and promote it even as the EA Landscape is becoming increasingly disrupted and complex.

In short, I'm happy to nominate myself as **Your Enterprise Architecture Evangelist and Ambassador (YEAEA)!** As such, I will seek to be more available for public and private presentations and workshops on leading practices to succeed at EA. My knowledge base and connections is extensive and I want to make more of my time available to serve as a trustworthy expert and communicator for all EA-related endeavours. One channel of knowledge built up over 20 years is reporting on EA aspects related to hundreds of Gartner events in the U.S. My relationship with Gartner Events continues to provide access to wide-ranging business and technical expertise from Gartner and vendors at the events.

Of course, a major venue will still be EAPJ.org, but we are expanding our output and encouraging more community building and collaboration through a Substack publication being launched this Spring to complement EAPJ.org: **Creative Synthesis**.

To better understand EA and how to best apply it, we will be investigating and writing about the critical intersections Enterprise Architects must embrace to enhance their skills and the maturity of their EA practices, including deeper knowledge of:

- Major EA frameworks

- Various architecture domains/perspectives: Business, Application, Data, Infrastructure, Network, Cybersecurity, Solution, and Software
- Business Analysis, Business Strategy, Agility,
- GenAI/ML.

And enhanced abilities to:

- Create compelling work products (visuals, overall documentation, and stories), and
- Identify and apply champion Architecture Patterns, Reference Models/Architectures, and transformation workflows for a variety of sectors and use cases.

In conclusion, The Enterprise Architecture Professional Journal, and my main collaborators and I, want to be Your EA Evangelists and Ambassadors, so please reach out to us with any ideas, content, questions and requests. We will do our best to provide you with our best objective yet passionate support.

Dr. Steve Else

Founder, Enterprise Architecture Professional Journal.

FEATURE ARTICLE

Designing the Future of Quality

A Business-Improvement Focused, Digital Integrated Quality Management System Powered by Enterprise Architecture

By Giovanni Traverso, Nan Zhao, Riccardo Bausola

Summary

This article walks through the processes, challenges, and rewards of transitioning from a quality management system (QMS) owned by the Quality department to a business owned IQMS. Highlighting key strategies like adopting the ABACUS Enterprise Architecture tool and standardized language, it showcases how this shift enhances engagement, efficiency, and customer experience.

Key benefits:

- **Business Ownership:** Moving quality from siloed processes to an integrated, business-owned system.
- **Improved Communication:** Engaging all levels with a clear, "business language" Quality Manual.
- **Efficiency & Agility:** Leveraging tools like ABACUS® for easy browsing, auditing, and scenario analysis.
- **Standardization & Consistency:** Aligning internal operations and interaction with customers & suppliers.
- **Benchmarking & Sharing:** Facilitating best practice sharing and fostering continuous improvement.
- **Standardized Notations:** Adopting Archimate® and APQC PCF® for cross-organizational process clarity.

Business Outcomes:

- **Internal User & Auditor Satisfaction:** Improved engagement, transparency, and information access.
- **Enhanced Customer Experience:** Consistent quality assurance across all locations.
- **Boosted Business Agility:** Streamlined compliance evaluation and scenario analysis.

Abstract

This article provides a step-by-step guide to how Enterprise Architecture (EA) approaches were successfully applied to design and implement a scalable, improvable Integrated Quality Management System (IQMS). This approach also aligns with a broader digital transformation strategy, where quality, sustainability, security, and specific customer requirements are being addressed holistically.

This method also addresses three key concerns regarding Quality Assurance in today's industry:

- The goal here was to realize a Quality Manual as a live document, engaging business owners with a "business language". This transcended the traditional compliance-oriented approach to QMS as Quality Manuals can often be perceived as formal, static documents.
- This method creates a single Integrated Quality Management system (IQMS) that combines and improves quality, safety, security, and customer/internal requirements – all working together (people, processes, technology, and data) for overall success.
- The approach also serves as a bridge between how the organization improves quality over time and how it digitizes its processes.

The discussion shows how the architecture-based approach assures compliance with multiple standards while maintaining the organization focused on one common, integrated, model of the business. It simplifies and facilitates the engagement of stakeholders and drives successful digital transformation initiatives.

This article offers:

Enterprise Architecture teams: a real-world example of applying EA in Quality Assurance.
Quality Assurance leaders: a robust approach to driving a path to digitalization within their organizations.

Unify Your Assurance Efforts: Achieve Quality, Sustainability, and Security with a Holistic EA Approach

The introduction describes the challenges faced by organizations in the trend towards diverse assurance requirements (such as quality, environmental sustainability, safety, security etc.). At the same time, organizations need to drive operations consistently through procedures, (digital) tools, metrics, skill provisions.

We walk through the benefits of an EA approach, specifically the TOGAF® ADM methodology. We also cover how the Archimate® modeling language and a standard process taxonomy such APQC PCF can provide a foundation for quality assurance methods.

We include practical examples to illustrate the implementation, including the use of an EA tool to support both business scenario design (based on value streams and service blueprint diagrams), quality manual (including procedures, policies, rules) and digitalization.

We conclude by exploring the key challenges and potential rewards in more detail and highlight useful practical considerations for adapting this approach within a dynamic and evolving environment.

Implementation of a modern Integrated QMS

From a Quality Management System (QMS) to an Integrated Quality Management System (IQMS)

Among current trends in the way organizations conceive their Quality Management System, perhaps the most important is the one towards an Integrated Quality Management System, reflecting a continuous push towards integration, efficiency, and alignment to the overall organization's strategy.

> *"An integrated quality management system (IQMS) is a system that combines quality control, quality assurance, and performance management for different purposes and standards …by aligning the common points of different aspects of the organization." [GLEM21]*[1]

[1] [GLEM21] – "Increasing the value of quality management systems", by Gremyr, I., Lenning, J., Elg, M., & Martin, J.: (2021). International Journal of Quality and Service Sciences

In the case described, the business scope of the desired IQMS encompasses all functions within the organization: all organization branches distributed in all locations worldwide, all compliance standards relevant for the business (for quality: ISO 9001, IATF 16949 and related Customer Specific Requirements; for Environment Health and Safety: ISO 14001, ISO 14006, ISO 45001, ISO 26262; for Security: ISO 27001, TISAX, IEC 62443) and other reference de-facto standards.

Using an integrated view, the IQMS facilitates the convergence of resources to achieve the desired business outcomes. It allows organizations to streamline their processes and avoid duplications enabling a more business-oriented approach to quality management. This is in addition to the traditional aims of compliance oriented QMS such as assuring predictability and quality control due to standardization.

Business-Improvement Focused Quality Management

In a recent survey, [GLEM21] found that "a compliance-oriented QMS usage will more likely lead to a view of quality management as costly and of little respect, than a business or improvement-oriented QMS usage".

The key focuses of an IQMS are comprehensiveness and alignment. The implementation of IQMS requires a structured approach that renders a live representation of the business including its context, value delivery goals, objectives, organizational structure, business processes, and information needs. Business Architecture is the discipline that conveys such representation [GTetA17][2], proven in the field by organizations for managing process improvements [GT15][3].

Using Value Streams to Map Goals to Functions

To realize such a live representation of the business using the "business language", the authors borrowed the concept of End-to-End Value Stream from Business Architecture. Overall, fourteen End-to-End Value Streams were defined, in order to render a purposeful representation of the business, based on value creation mechanisms and oriented to the organization's stakeholders.

Each Value Stream was associated with its goal and with the main functions involved. The system building blocks describing People, Process, (IT)Platform were then mapped to each Value Stream, as to convey the ultimate purpose for each building block in the system.

[2] [GT17etA] – "Open Business Architecture (O-BA) Standard Part I and Part II", by The Open Group, G.Traverso, et al., (2016-2017). https://publications.opengroup.org/standards/business-architecture

[3] [GT15] – "The Business Architecture Journey at Huawei: Importance of a Metamodel", by G.Traverso, OMG Business Architecture Summit 2015, OMG Document -- basig/15-03-11

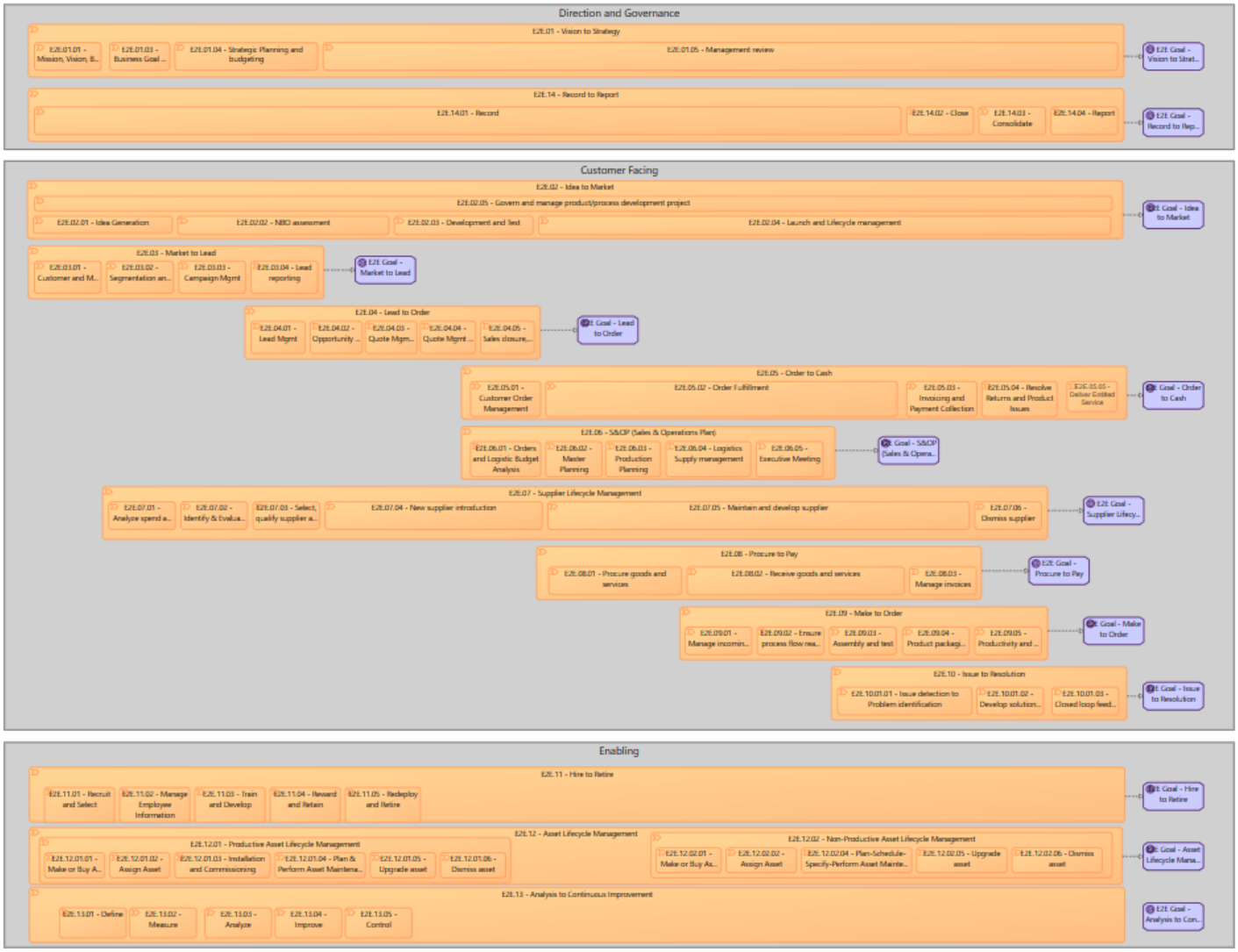


Figure 1 - Top-level Value Streams Representation

QMS Involvement in Industry 4.0/5.0 and Enterprise Architecture Methodology and Tools

Industry 4.0 is a widely accepted paradigm characterized by the integration of advanced technologies such as connectivity, advanced analytics, robotics, and automation. In this context, Quality 4.0 has been defined by the American Society for Quality (ASQ), referencing the future of quality and organizational excellence, as "the leading role for quality professionals to drive successful digital transformation initiatives" [NMR20][4] through the lenses of continuous improvement. More recently, the concept of Industry 5.0 has been introduced, emphasizing a wider integration scope including sustainability issues.

IT and process digitalization is fundamental for a modern IQMS which aspires to drive and inform an organization's continuous improvement in an Industry 4.0 environment. The representation of Business Architecture alone would not be enough without a focus on digitalization.

Leveraging the structured approach of Enterprise Architecture, enterprises can easily align the Business Architecture view with IT aspects. The purpose of Enterprise Architecture is to integrate an organization's business processes, information technology (IT) infrastructure, and human capital with its overall strategy.

[4] [NMR20] – "Connected, Intelligent, Automated", by N. M. Radziwill, 2020, edited by ASQ Connected, Intelligent, Automated | ASQ

Streamline IQMS Development & Operations with the TOGAF Framework

The Open Group's TOGAF®[5] framework offers a comprehensive approach for Enterprise Architecture, while TOGAF ADM is a proven development method conceived for Enterprise Architecture, matching the IQMS implementation needs.

Details are given in the following chapters about the adoption of an Enterprise Architecture framework for the realization of an IQMS. In particular, this paper will show that TOGAF ADM is suitable in two ways: firstly, it can guide the development of the IQMS; secondly, it is a useful reference for the "run-time" operations of the IQMS itself, as a model for continuous improvement initiatives.

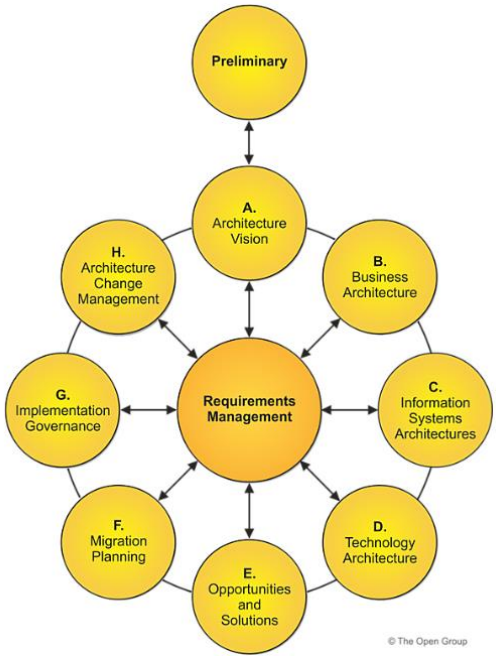


Figure 2 - TOGAF ADM

We found the steps of the TOGAF ADM could be used successfully to guide the construction of the IQMS. It was valuable in outlining and sharing the establishment of a vision based on IQMS with all business owners and in the construction of the first business architecture views against which the IT architecture was mapped, along with technology.

Migrating from the old QMS to the new IQMS offered both an opportunity for improvement and a significant challenge. The transition was characterized by a radical shift in architecture, moving from a geographically dispersed system with implementation at a plant-level to a vertically integrated scheme based on corporate and subsidiary functions coordinated under one system.

Throughout the transformation journey, requirements, developed from the integration of multiple compliance clauses of various standards, played a pivotal role. Using the enterprise architecture map of the organization as a baseline, every requirement was associated with its related element: process, object, event, or application.

Following this system, a tight control of compliance standards was able to be maintained. Similarly, the mapping of KPIs and risks allowed for the close control of performance and risk management.

[5]The Open Group Architectural Framework (TOGAF®) 10th Edition, by The Open Group: TOGAF® The New Release | opengroup.org

From Static to Dynamic: Real-Time Quality Manual with Real-Time Architecture

This real-time architecture and compliance model, implemented using ABACUS®, moves beyond a static document to become a live, interactive Quality Manual. The system forms a basis for what-if analysis, process improvement planning, application evolution planning, KPI and risk analysis.

With a solid foundation in place, it is now possible to run continuous improvement cycles. By employing the TOGAF ADM as a guide, the system can also be incrementally refined.

Benefits of Enterprise Architecture for IQMS

The integration of Enterprise Architecture principles into the development of an integrated Quality Manual is a strategic approach to enhancing quality management within organizations.

This chapter explores the advantages and synergies that result from aligning EA with the creation of a comprehensive quality manual.

A key argument in favor of integrating EA with a Quality Management System is its seamless ability to align with QMS modeling. EA provides a structured framework for understanding an organization's structure, processes, systems, and their interrelationships. This makes it an ideal fit for the holistic modeling and documentation required in a quality manual.

The holistic perspective offered by EA is invaluable when crafting a quality manual. It grants a comprehensive and structured framework for understanding an organization, ensuring that all aspects, from processes to systems, are accounted for. This depth of understanding is critical in developing a quality manual that leaves no critical component overlooked.

Enterprise Architecture excels in ensuring that the quality manual aligns closely with an organization's overarching business objectives and strategies. Further, it aids in the seamless integration of quality management practices and an organization’s strategic direction. This ensures that the quality manual becomes a strategic asset that directly contributes to the achievement of the organization's business goals.

An often-overlooked advantage is the scalability that EA provides. As organizations evolve, an enterprise architecture-based quality manual can be easily adapted to accommodate changes. This adaptability ensures that the quality management system remains relevant and appropriate for the organization's needs.

One of the significant challenges in quality management is ensuring that various quality management systems across different parts of the organization can work together seamlessly. EA plays a vital role in this by facilitating the integration of these systems. This promotes interoperability, reduces data silos, and enhances collaboration, fostering a more effective quality management environment.

The EA model provides support for resolving typical QMS issues related to continuous improvement. It helps with Root Cause Analysis (RCA), identification of key performance indicators, and assessing the

impacts of changes. These features are instrumental in maintaining and enhancing the quality of an organization's products or services.

An intriguing byproduct of integrating EA within an organization is increased agility. This allows the organization to adapt its QMS quickly to new requirements, which is critical in today's dynamic business environment. For example, the team was able to easily update requirements and contextually identify in real time the impacts related to compliance requirements to ISO 26262.

Additionally, the EA model can serve as a blueprint for digitalization efforts, providing a solid foundation for modernizing and streamlining quality management processes. For example, in redesigning Human Resources processes, digitizing the management of employee requisition, performed by a hiring manager, reduced paper waste, and allowed for better oversight of all requests by the process owner. Such digitization was made possible by EA blueprinting, that allowed to map all stakeholders' goals, behaviors, dependencies, as well as relevant compliance requirements, in a comprehensive view.

The integration of enterprise architecture principles into the development of a quality manual represents a forward-thinking approach that brings a multitude of advantages. These include comprehensive understanding, alignment with business objectives, scalability, interoperability, support for continuous improvement, and the byproduct of increased agility and a digitalization blueprint. Organizations embracing this approach are poised to enhance their quality management capabilities, adapting to evolving business landscapes more effectively.

Reference Standards: TOGAF®, Archimate®, BPMN™, APQC PCF®

About Enterprise Architecture and TOGAF®
While EA was originally conceived as a process for organizations to standardize and organize IT infrastructure in alignment with business goals, The Open Group developed a standardized framework for its implementation: TOGAF®. TOGAF is a multi-phase, iterative approach to develop and use an enterprise architecture to shape and govern business transformation and implementation projects. The framework provides the methods and tools for assisting in the acceptance, production, use, and maintenance of an EA.
An abundance of examples exist documenting TOGAF®'s adoption as a structured approach for designing, planning, implementing and governing across any type of architecture. Therefore, its application for IQMS development would be a natural progression.

About Archimate®
Besides the development framework, the adoption of standard building blocks for Enterprise Architecture modeling is beneficial for clarity of communication inside and outside the organization. Archimate®[6] has been chosen as a modeling language; it consists of several sets of building blocks, along with their possible relationships. The building blocks are organized by domains: Business (e.g. Business Process, Business Object), Application (e.g. Application Service, Data Object), Technology (e.g. System Software, Device), Motivation (e.g. Goal, Requirement, Assessment), Implementation and Migration.

[6] The Archimate® Enterprise Architecture Modeling Language, by The Open Group: The ArchiMate® Enterprise Architecture Modeling Language | opengroup.org

In some cases, although not semantically required, specializations had been introduced for practicality. For example, the specialization of certain building blocks allows simplifying their identification easing respective queries.

About APQC PCF®

Using the APQC PCF provides access to a standardized taxonomy of processes and industry benchmarks [7]. The framework consists of "a taxonomy of business processes that allows organizations to objectively track and compare their performance internally and externally with organizations from any industry".

This taxonomy is structured by levels, where each item decomposes in finer granularity on the next level.

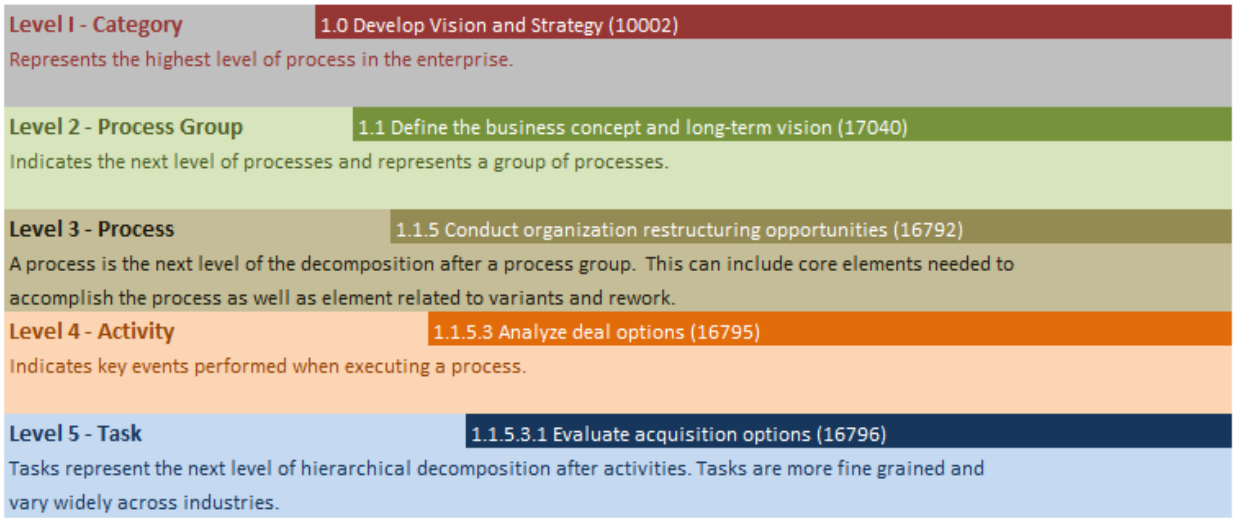


Figure 3 - APQC PCF levels classification

It starts with the following 13 process categories:

Hierarchy ID	Name
1.0	Develop Vision and Strategy
2.0	Develop and Manage Products and Services
3.0	Market and Sell Products and Services
4.0	Deliver Physical Products
5.0	Deliver Services
6.0	Manage Customer Service
7.0	Develop and Manage Human Capital
8.0	Manage Information Technology (IT)
9.0	Manage Financial Resources
10.0	Acquire, Construct, and Manage Assets
11.0	Manage Enterprise Risk, Compliance, Remediation, and Resiliency
12.0	Manage External Relationships
13.0	Develop and Manage Business Capabilities

Figure 4 - APQC PCF process categories

APQC also provides benchmarking facilities[8], based on the same process taxonomy, by industry.

About BPMN™

For the detailed description of processes at activity (level 4) and task (level 5), [9] had been adopted. BPMN is also suitable for the implementation of digital processes in low-code or zero-code platforms.

[7] APQC's Process Classification Framework (PCF)®, by American Productivity and Quality Center (APQC): Process Frameworks | APQC

[8] APQC Open Standard Benchmarking: What is Benchmarking? | APQC

[9] Business Process Model and Notation (BPMN™), by the Object Management Group: BPMN Specification - Business Process Model and Notation

Better Governance with Metamodels

Like construction codes for buildings, metamodel standards dictate the content (materials) and structure (rules) for creating consistent and accurate models.

We chose the Archimate®[6] standard as a baseline for the metamodel. It fits with the goal of the IQMS to be business-oriented, while allowing for modeling of governance concepts.

To render IQMS more comprehensive and easily understandable, it should possess the following beneficial characters:

- From the developer perspective, it guides and standardizes the development of the IQMS, especially on how to describe things in a comprehensively conversational manner.
- From the user perspective, it offers a useful reference, a kind of handbook, to gain basic knowledge on IQMS navigation to visualize a functional view by customization.

Hence as expected the metamodel is being set up to simply the complexity with:

- A set of definitions of elements used to describe Process, People, (IT)Platform and Risk Management aiming to convey the ultimate purpose for each building block in the system.

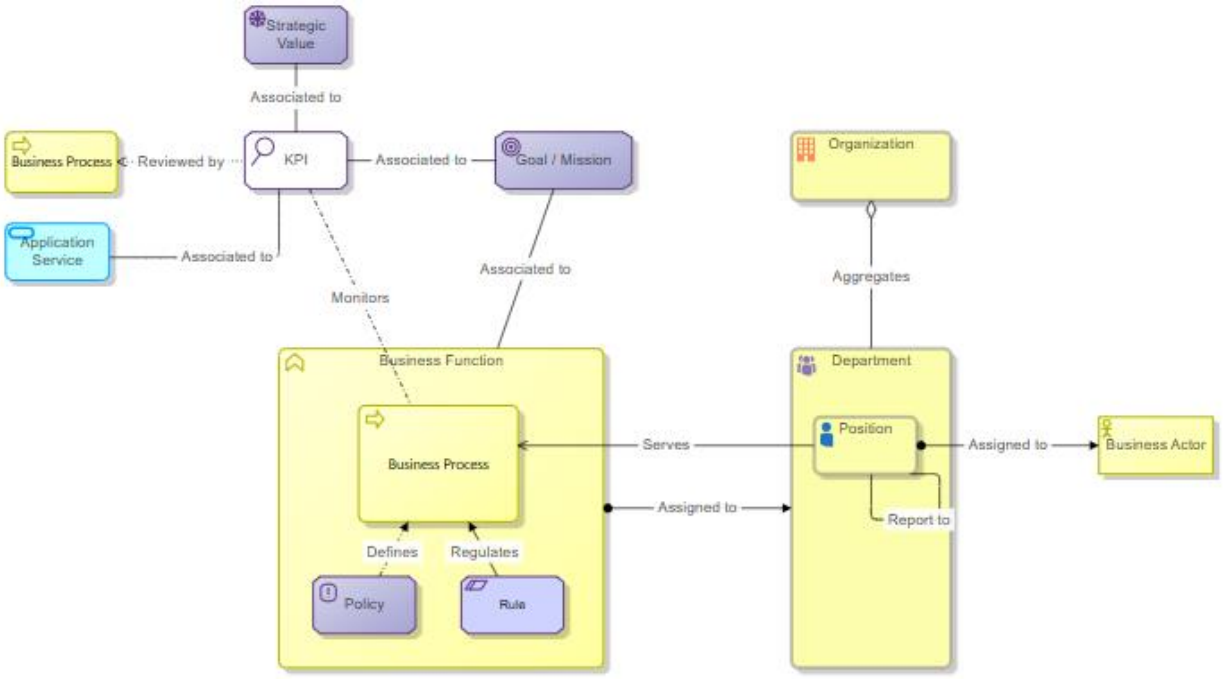


Figure 5 - Metamodel, motivation and responsibility part

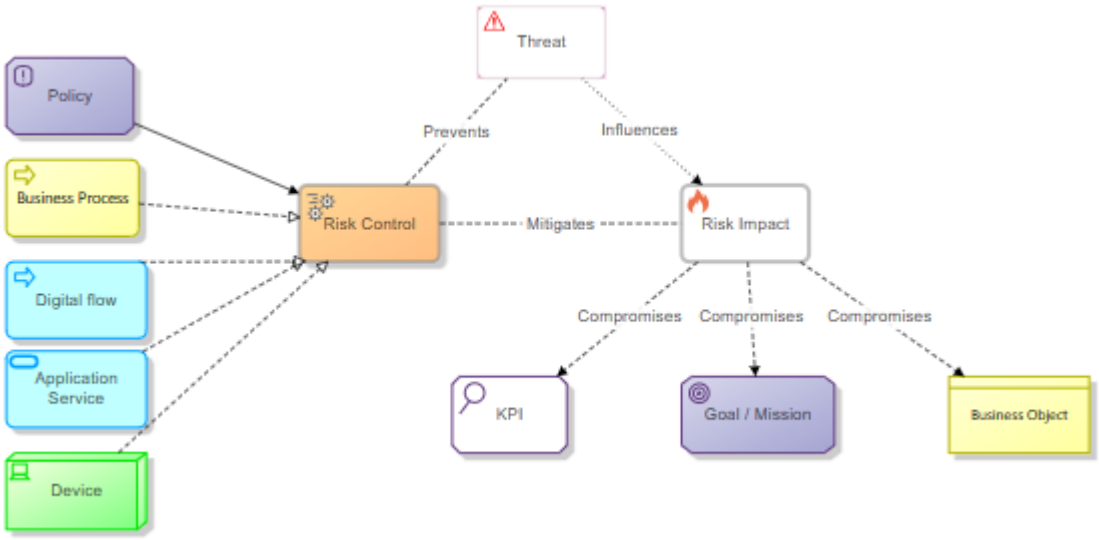


Figure 6 - Metamodel, risk management part

- A set of definitions for relationships among elements, those are Business (e.g. Business Process, Business Object), Application (e.g. Application Service, Data Object), Technology (e.g. System Software, Device), Motivation (e.g. Goal, Requirement, Assessment), Implementation and Migration.

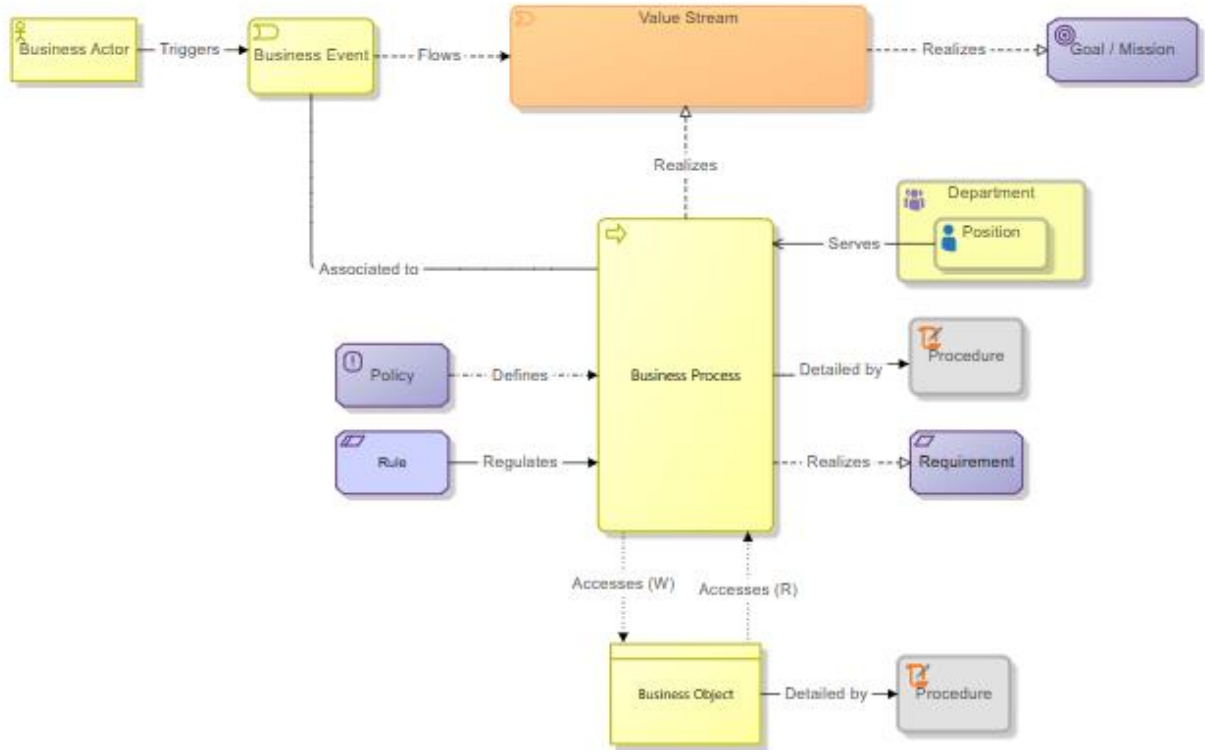


Figure 7 – Metamodel, value stream and operational part

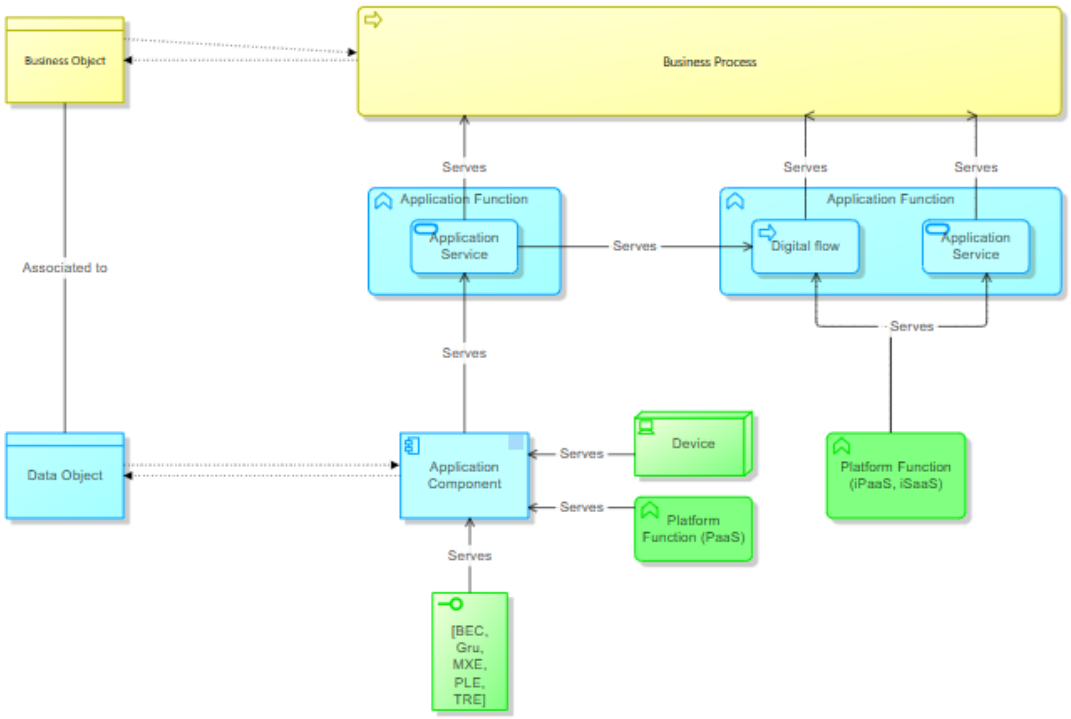


Figure 8 – Metamodel, application part

- A set of definitions of elements specified by various maturity levels which are seamlessly aligned with business needs.

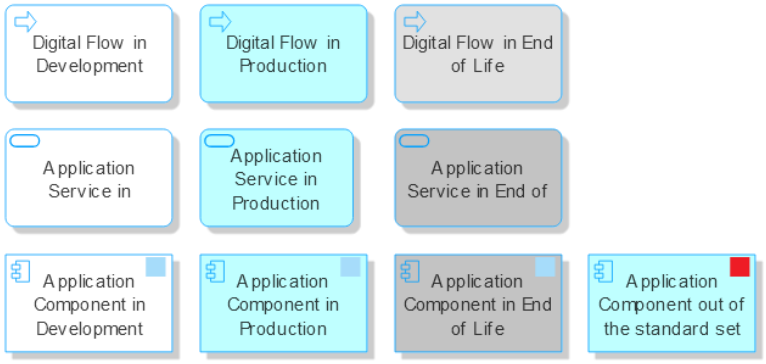


Figure 9 – Metamodel, application maturity mapping

Quality Manual Implementation: Some Examples

ABACUS® by Avolution was selected for the implementation due to its flexibility and embedded features.

Users access browsing from a front page, which presents a familiar menu layout, designed to mirror the index of a traditional Quality Manual. The links on the front page provide quick access to dedicated dashboards. Users can navigate from one page to any content thanks to links that are implemented by the tool automatically.

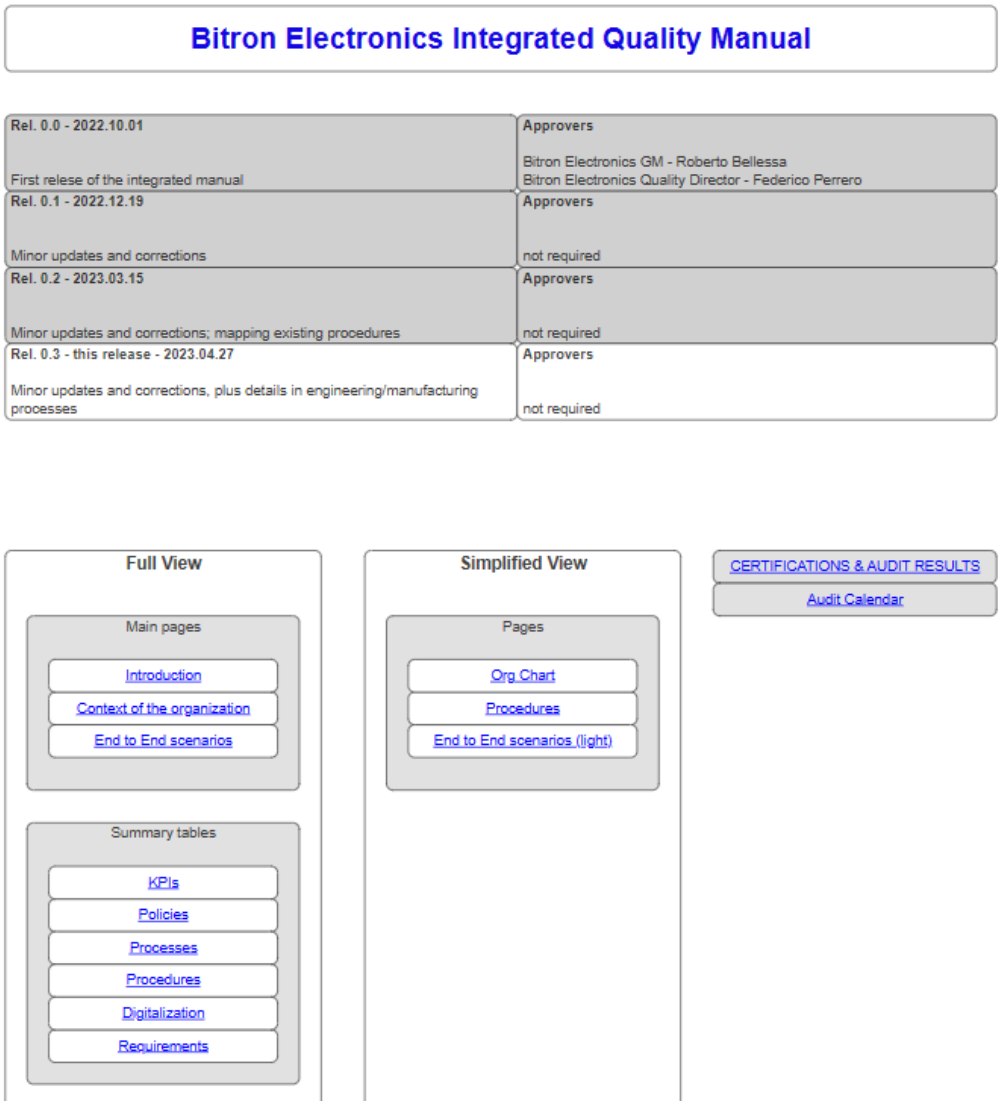


Figure 10 - Quality Manual front page

General navigation can start from the end-to-end business scenarios (see Figure 1 - Top-level Value Streams Representation) or from the functional view (through the “context of the organization” page). The model had been built starting from the end-to-end scenarios (value streams), while all other views are produced automatically.

Here is a portion of an end-to-end diagram, where processes that realize a stage of the value stream are mapped, along with relevant KPIs, supporting applications, input/output objects, applicable requirements, policies, and procedures. In such a way everything gets contextualized in a practical business scenario that users can recognize.

This approach allowed the engagement of business owners in the creation of each diagram.

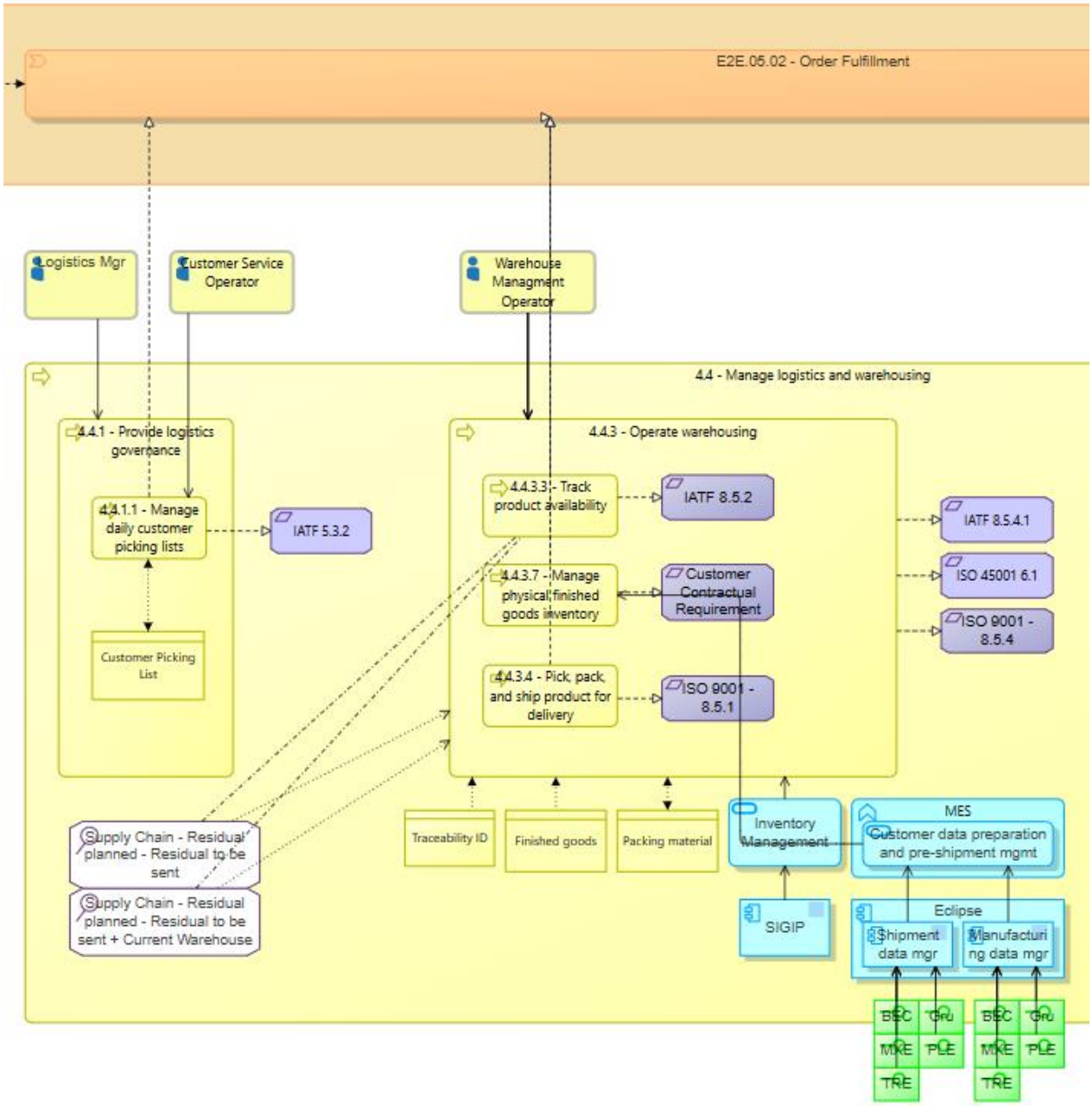


Figure 11- Portion of an end-to-end value stream mapping

Once done with the mapping of all elements in context, the “live” Quality manual is available for navigation, through the links among elements. By selecting any building block, the tool automatically provides active links pointing to where it is used, what other elements it is connected to, in which contexts. This way, users can follow the links and check for example any specific requirement or rule, procedure, template, or open the page of another end-to-end where the same element is instanced.

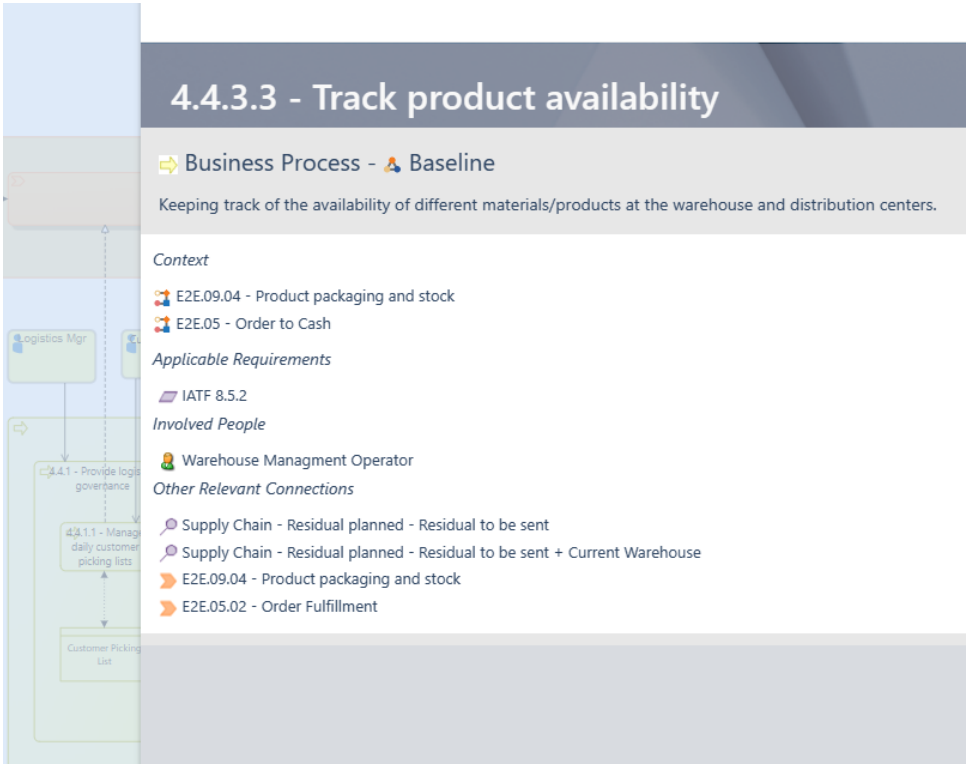


Figure 12- Pop-up with information and active links related to the selected element

Another way for navigating the IQMS is through a functional view, where, for each function, a "turtle map" is provided, whose content is automatically generated.

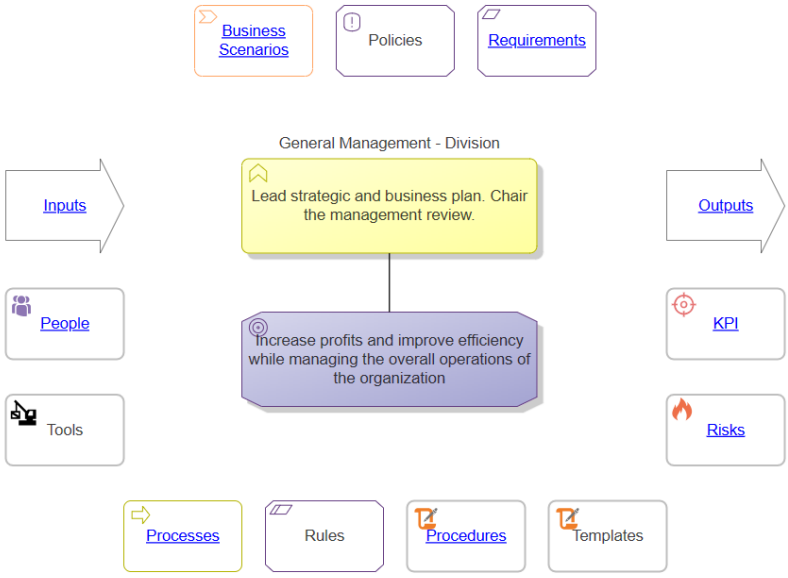


Figure 13- Turtle map of a function

By clicking on each box of a turtle map, the tool generates a table or a specified visualization for the respective collection of items related to that function.

Input	Description	From Function
<Show All>	<Show All>	<Show All>
Customer AVL		Purchasing
Customer Claim case	Refer to local procedure for exact description of respective functions involvement	Facility Management, Manufacturing, Purchasing, Quality & Process Digitalization, Quality Assurance
List of secure custom component/COTS/third parties	List of secure custom components, off-the-shelf components and third parties.	R&D
LOA	All information related to the supplier, included the status of the supplier (idoneo/non idoneo), audit score,.	
Market analysis		Purchasing
Market reports		
New supplier request	Coming from the Purchasing DEvelop sourcing and categeory management strategis or from a internal client need (e.g: Cost Engineering, Quality, ...): -New supplier request for local material (plastic and metal); -New business extension for local material (plastic and metal); -Sourcing proposal.	Purchasing

Figure 14 - Table summarizing inputs to a function

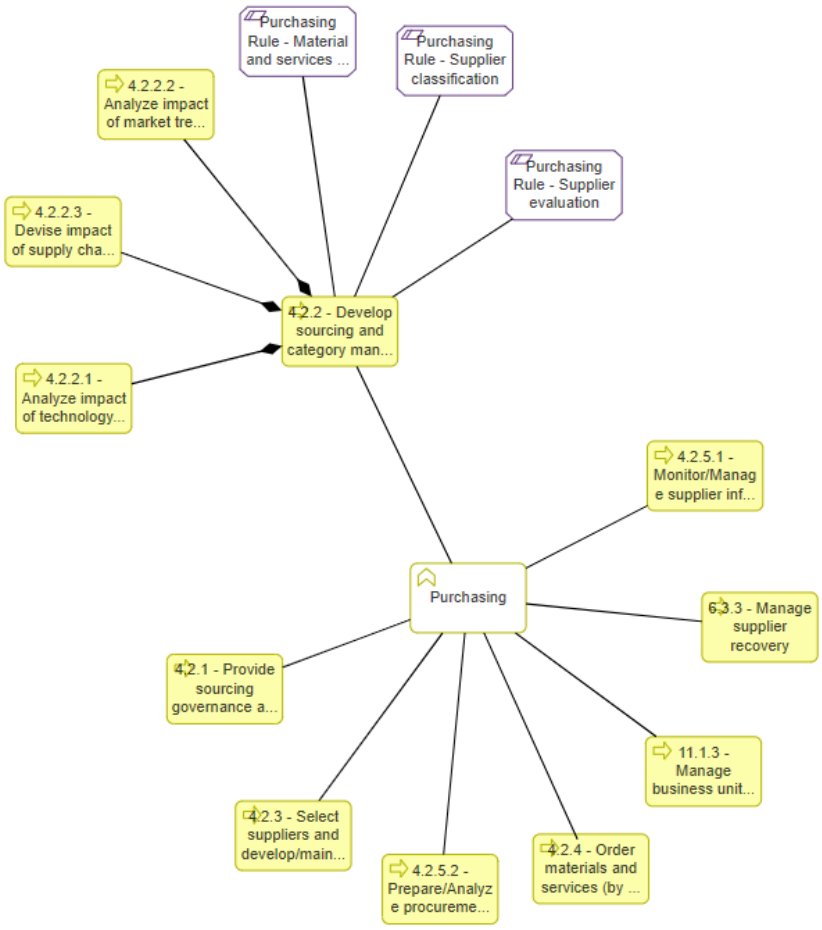


Figure 15- Active graph visualization of processes related to a function

Dedicated summary dashboards with tables (e.g. searchable summary of all procedures, etc.) or visualizations are also accessible from the main page.

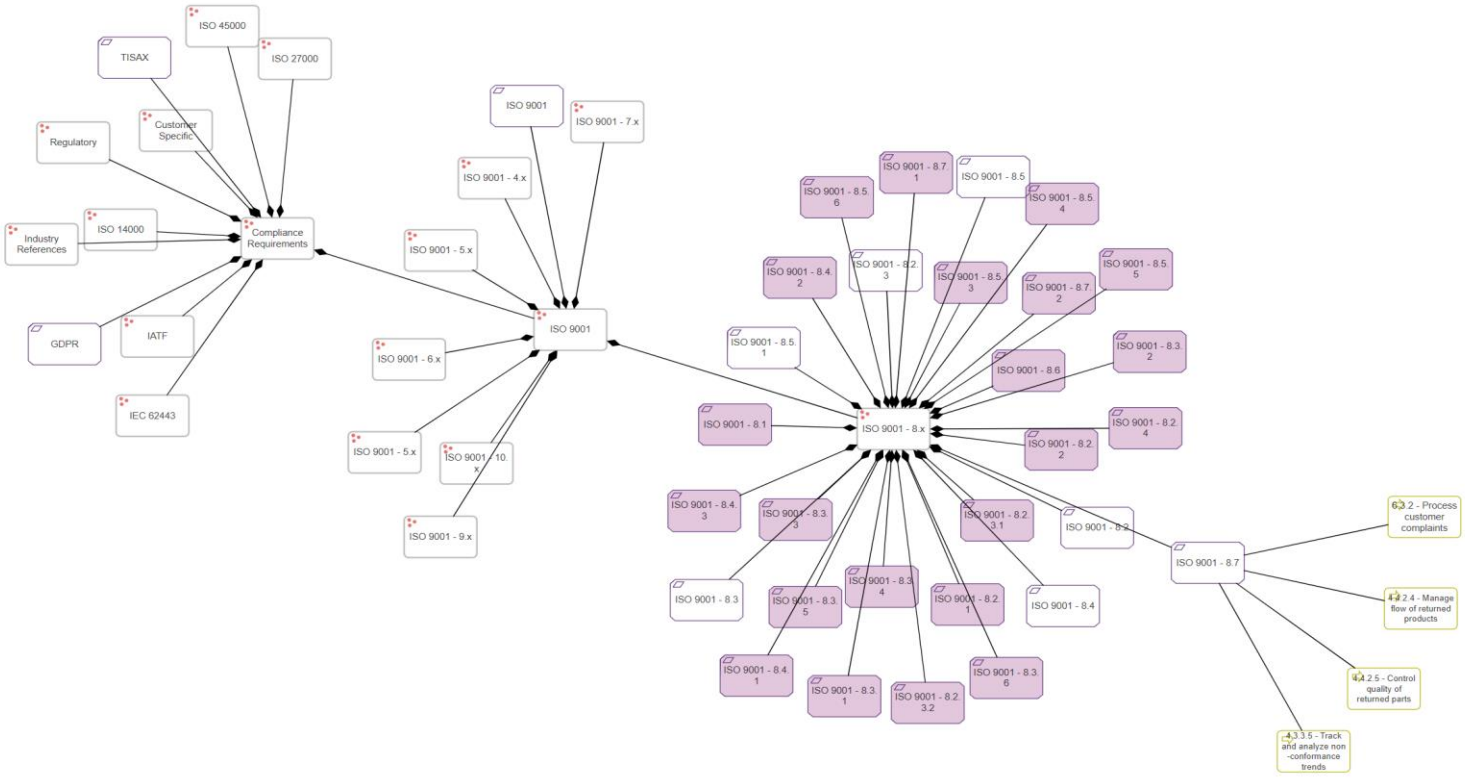


Figure 16- Active graph visualization showing which processes are impacted by a certain requirement

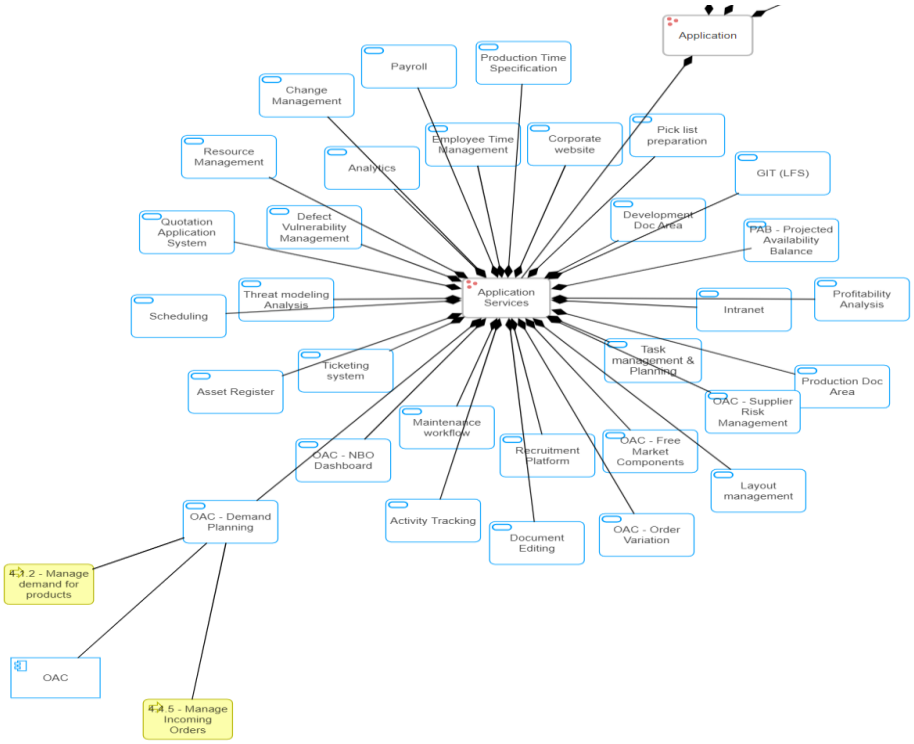


Figure 17- Active graph visualization showing which processes are supported by a certain application

Rewards and Challenges of a Unified IQMS5r4

On the path to Quality 4.0, organizations will encounter challenges, but also reap significant rewards, as seen in our experience [NMR20]. Here are some examples:

Moving from QMS owned by Quality Dept to IQMS owned by the Business

Compliance-oriented QMS implemented in the early times would be conducive to assuming that quality is a matter for the Quality team: see [GLEM21] “a compliance-oriented QMS usage will more likely lead to a view of quality management as costly and of little respect, than a business or improvement-oriented QMS usage”.

A business-oriented QMS entails the concept of “quality owned by the business”, which might sound revolutionary for some.

Such a change will require effort in engaging the business, at all levels. This also requires changes in the way the Quality team operates and communicates. For example, The Quality Manual must be a live document, conveying information that is practical for users, adopting a “business language”.

The adoption of an Enterprise Architecture tool such as ABACUS®, along with an architecture based on Value Streams representing the end-to-end business was instrumental. The Quality Manual is then positioned as a working tool for easy browsing of useful information, including links to digital procedures, processes, templates, dashboards etc.

Audit practices

While an integrated view is quite efficient for overall governance, its information will still need to be tailored for the needs of third-party auditors, who typically focus on a specific domain/standard.

Also, the representation style, based on end-to-end value streams or business scenarios, differs from the traditional audit practices that follow a process “silo” approach.

This issue was solved by leveraging the capabilities of the Enterprise Architecture tool (ABACUS®), to sort and regroup information within the EA database, presenting it in a way more consumable by auditors and quality professionals. More specifically, ABACUS® was set to parse the end-to-end diagrams and create a set of “turtle map” representations, organized by function (see Figure 13- Turtle map of a function).

Adoption of standard notation (Archimate®) and taxonomy (APQC PCF®)

The adoption of a standardized taxonomy of processes was instrumental for achieving a common way to describe processes across the diverse branches of the organization.

This was a true enabler for a swift move from local certifications to a corporate-wide certification approach by the organization. This directly improved the level of quality assurance perceived by customers.

The construction of an Enterprise Architecture model can only be based on standardized building blocks in a reference metamodel. Archimate® was the reference that allowed us to use terms recognizable by the business. It did require some training for people used to describing things in a conversational manner. The effort was rewarded by an improved clarity within the organization.

Standardization was crucial to pursue certifications according to the corporate scheme, evolving from separate certification of individual branches. In fact, the introduction of a standardized language allowed to converge every branch of the organization towards a common process, for the benefit of internal stakeholders (best practice sharing) and external stakeholders (who could regard at the organization as a single trustable entity).

Consistency Towards Customers and Suppliers

Besides the certification level, convergence to one common QMS allows us to standardize the way the organization interacts with third parties like customers and suppliers, aligning all offices and locations.

Benchmarking and Sharing Best Practices

Another benefit of standardization was the ability to easily benchmark and share best practices among different branches. This was made possible by relying on a common definition of processes and KPIs, easily accessible and browsable thanks to the EA tool Abacus®, which is available in the cloud to all employees.

Business Agility

Business agility had been noticeably boosted by this IQMS as it was possible for example to quickly evaluate the impacts of a newly required compliance, just by enriching the model with the new requirements and extracting a summary of impacted processes, visualized on relevant end-to-end streams. Likewise, the tool is now frequently used for the analysis of what-if scenarios regarding, for example the pursuit of new markets versus impacted processes.

Final recognition

Beyond internal users, the new IQMS was praised by third-party auditors who appreciated the level of quality control that it gives the organization, the focus on business owners engagement and the freshness of the digital implementation. The auditors also noted how such implementation supports the goals of information security and sustainability by ensuring that all employees always have access to up-to-date secured information in real time, according to respective security profile, and eliminates waste of paper.

Beyond Siloed Systems: Unifying Operations with a Standardized Quality Approach

This unified approach did require each branch to give up the local quality manual and embrace the global one. Effort had to be spent initially at central level, to build a first implementation and communicate systematically the benefits of it to all business owners.

The process of adoption is a journey that started from standardization of the highest levels of the processes and now is gradually standardizing some low-level activities (those independent of the local environment). A measure of the penetration of the new system is reflected by the number of users who have access to ABACUS®: that reached 25% of the employee population in 15 months.

The team is constantly working to improve the user-friendliness of the model and ease of access and consumption.

Continuous Improvement: Evolving a Global Quality System for User Success

Navigating the evolving landscape of the IQMS, several key areas emerge as focal points for future improvements. These aspects, integral to the enhancement of our system, require strategic attention and continuous efforts for sustained excellence.

IQMS: A Blueprint for Sharing Best Practices

IQMS will be instrumental in shaping the future, serving as a dynamic platform for sharing best practices in quality management. This visual representation will need to capture successful methodologies and efficient processes within the IQMS framework, paving the way for the dissemination of knowledge across departments. Embracing a culture of continuous improvement and standardization, IQMS is destined to become our guide for cultivating excellence in quality practices.

Managing HR Challenges: Workloads and Skills Optimization

In the journey towards a more optimized future, IQMS assumes a pivotal role in addressing HR challenges related to workloads and skills optimization. The IQMS could offer insights into resource allocation, allowing us to identify workload imbalances and skill gaps. Armed with this information, strategic HR planning becomes a crucial facet of our future endeavors, ensuring that the right skills are deployed to the right tasks. This strategic approach ultimately will enhance the efficiency of our quality management processes, creating a workforce finely tuned to meet the demands of the future.

Incorporating NLP Technologies for Insightful Analysis

In the future, the integration of Natural Language Processing (NLP) technologies into the EA framework will play a crucial role in making IQMS more user-friendly, thereby increasing knowledge and awareness among users. NLP will serve as a key tool for conducting insightful analyses of unstructured data in quality management. By harnessing the capabilities of NLP, we can extract valuable insights from textual documents, customer feedback, and qualitative data sources.

As a result, users will be better equipped to leverage the power of language for strategic insights, driving continuous improvement in our quality practices. This evolution towards a more user-friendly IQMS, facilitated by NLP integration, reflects the commitment to enhancing the overall user experience and promoting greater engagement among our stakeholders.

Data Management: Precision and Accessibility

The future of our IQMS necessitates an optimized approach to data management. Enterprise Architecture extends its influence to guide and optimize data management strategies. The IQMS shall become a guide for the organization in managing and standardizing data repositories for enhanced accuracy and accessibility.

KPI/Indicators: A Holistic Approach to Performance Measurement

The IQMS serves as a foundational element for future improvements in the systematic definition, measuring, and monitoring of Key Performance Indicators (KPIs). Using the IQMS as a guide future target is to define, collect and more importantly standardize all KPIs across the organization.

As the organization focuses on these areas for future improvement, we lay the groundwork for a quality management system that not only meets the challenges of today but is also agile and adaptive to the demands of tomorrow. Through strategic planning, technological integration, and a commitment to continuous improvement, an organization can forge a path towards sustained excellence in quality management.

Acronyms

APQC: American Productivity and Quality Center
BA: Business Architecture
BPMN: Business Process Model and Notation
CI: Continuous Improvement
EA: Enterprise Architecture
I4R: Industry 4.0, or the 4th Industrial Revolution
IQMS: Integrated Quality Management System
KPI: Key Performance Indicator
NLP: Natural Language Processing
OMG: Object Management Group
QMS: Quality Management System
RCA: Root Cause Analysis
TOG: The Open Group
TOGAF: The Open Group Architecture Framework
TOGAF ADM: TOGAF Architecture Development Method

References

[GLEM21] – "Increasing the value of quality management systems", by Gremyr, I., Lenning, J., Elg, M., & Martin, J.: (2021). International Journal of Quality and Service Sciences

[GT17etA] – "Open Business Architecture (O-BA) Standard Part I and Part II", by The Open Group, G.Traverso, et al., (2016-2017). https://publications.opengroup.org/standards/business-architecture

[GT15] – "The Business Architecture Journey at Huawei: Importance of a Metamodel", by G.Traverso, OMG Business Architecture Summit 2015, OMG Document -- basig/15-03-11

[NMR20] – "Connected, Intelligent, Automated", by N. M. Radziwill, 2020, edited by ASQ Connected, Intelligent, Automated | ASQ

The Open Group Architectural Framework (TOGAF®) 10th Edition, by The Open Group: TOGAF® The New Release | opengroup.org

The Archimate® Enterprise Architecture Modeling Language, by The Open Group: The ArchiMate® Enterprise Architecture Modeling Language | opengroup.org

APQC's Process Classification Framework (PCF)®, by American Productivity and Quality Center (APQC): Process Frameworks | APQC

APQC Open Standard Benchmarking: What is Benchmarking? | APQC

Business Process Model and Notation (BPMN™), by the Object Management Group: BPMN Specification - Business Process Model and Notation

About Bitron and Bitron Electronics

Bitron is a global privately held company leader in research, development and manufacturing of mechatronic devices and systems for the automotive, appliance, HVAC and energy industries. Established in 1955, Bitron Group has 17 manufacturing plants and development centres (in Italy, Spain, Poland, Turkey, China, México). Within the group, Bitron Electronics specializes in the design and manufacturing of electronic systems and devices for the above markets.

About the Authors

Giovanni Traverso is a consultant who formerly held leading roles in R&D, product management, supply chain, business transformation, service delivery and management consulting, working in the high-tech industry for 30+ years. Sourcing from his management and technical experience, he published various contributions to standards and industry forums such as The Open Group, Business Architecture Guild, TM Forum, as well as conferences and reviews, regarding digital transformation, business architecture, enterprise architecture, customer experience management and service design, supply chain and R&D.

Nan Zhao, certified on knowledge acquisition about FCA risk management handbook and IATF 16949, plays the role of Quality System Engineer focusing on Central Quality organization for quality management, primarily for Process Description and Problem Solving, in Automobile and Electronic industry applications, where she developed a series of skills on Customer Quality Management, Continuous Improvement etc.

Riccardo Bausola is a seasoned Quality System Engineer with several years of experience in managing complex projects within international organizations with intricate structures. His expertise lies in process standardization, optimization, and digitalization, encompassing the systematic improvement of processes, compliance with legal standards, and effective project leadership.

FEATURE ARTICLE

Why do organizations need to implement the Zero Trust Security Strategy and execute the strategy with careful planning and thought?

By David Pui

Enterprise Architect – Digital Transformation Architect

Digitalwhizkid Pty Ltd

Email: davidpui@digitalwhizkid.com

Why? What are the Problems? Market Trends?

This article is based collectively on my experiences gained working as a Trusted Advisor – as Enterprise Architect and Senior Solutions Architect across a wide range of industries and business verticals – mainly focusing on Digital, Data, Cloud, and Security Transformation Business Initiatives and articles that I read during my R&D on Zero Trust Security Strategy Implementation. The main sources are Gartner, Coherent Market Insights, and others.

It's not just about technology solutions, we need to consider People, Processes, and Data too.

With increasing Cloud Adoption across the globe, due to a massive paradigm shift of market trends in the provision of highly resilient, highly scalable, high performance, and highly performant Cloud Platforms, Security, Networks, and Infrastructure, the business systems ecosystems have changed from the traditional On-Premises Data Centre solutions to Multi-Cloud Multi Tenanted on Premise Ecosystems.

Added to the complexities of Digital Transformation, user devices such as Mobile Phones, Tablets, and Laptops across different geographical locations are becoming an increasing norm for a single user. Because of the diverse users' devices and touchpoints, how do you properly supply safe and secure access to the organization's mission-critical business systems, along wth access to personal SAAS applications? Users and Customers all want the flexibility of BYOD (Bring Your Own Device) and CYOD (Choose Your Own Device), so how do you develop a secure E2E Authentication and Authorisation Security Implementation Strategy, Controls, and Policy, and at the same time adhere to PIM (Privileged Identity Management) and PAM (Privileged Access Management) to secure business sensitive information as well as private and confidential information.

This gives rise to the need for organizations to define, develop, and implement a Zero Trust Architecture Strategy, and re-think a roadmap to achieving their Digital Security Transformation.

It is an Enterprise Architecture initiative where Enterprise Architects and Business Architects need to work closely with C-Level Executives, Board of Directors, Business Sponsors, Business Leads, and Key Business and Technology Stakeholders to get everyone to understand the issues, complexities of the problem, and the difficulties in executing the digital security transformation.

However, it is still a Business Decision whether the organization can start to embark on the Zero Trust Strategy Implementation Journey, as there are many business program initiatives that need funding, and a Zero Trust Strategy initiative needs to be on the priority list. Hence, it needs to be driven by the C-Level Executives and buy-in from the Board of Directors to ensure full organizational support, commitment, and alignment with strategic & operational drivers.

The total costs of shifting to a Zero Trust paradigm are extremely high and the approach to tackling the problems needs to be discussed. Focus on Enterprise Security Planning and Approach to the realization of Zero Trust Network Architecture (ZTNA) is critical to the success of the modernization goals.

According to R&D companies such as Grand View Research, the global market size of Zero Trust Security is estimated to be USD 24.84 Billion, and the expected Compound Annual Growth Rate (CAGR) is 16.6% from 2023 to 2030.

This also stems from the COVID-19 pandemic where remote working became the norm and organizations are seeing this as a major advantage to reduce procurement infrastructure costs by moving towards a BYOD or CYOD strategy, hence driving the growth of zero trust security.

The rise of the use of BYOD and CYOD allows employees to access business-critical information and Cloud SAAS applications thereby increasing the chances of data theft and data loss. This new user landscape increases the number of potential threat actors who are continuously watching and finding ways to penetrate corporate networks. Hence, implementing BYOD and CYOD security strategies, solutions, standards, and policies is particularly important.

Cybersecurity Threats are continuing to increase, exploring any opportunities to seek vulnerability endpoints within organizations' ICT infrastructure. Cyber Threat Actors continue to launch attacks such as faking login pages, running persistent campaigns, introducing advanced malware, and consistently executing phishing in any possible touchpoints – endpoints, cloud applications, and network infrastructure.

According to Zscaler Ransomware Report between April 2022 and April 2023, the number of ransomware attacks has surged by 37.75%. With ransomware extortion attacks, the number of infected victims soared by 36.68%. There is also an emergence of encryption-less ransom attacks.

Importance of Data and Information Classifications

The traditional approach to Enterprise Security is all about setting up Perimeter Security and safeguarding data and information from cyber attacks and inadvertent network infrastructure penetrations.

Most organizations are too busy to keep the lights on and continue to work on Digital Transformation Business Strategies that enhance their business through:

- Increasing ROI (Return on Investment),
- Improving CX (Customer Experience),
- Improving business operations through business automation, and
- Improving EX (Employee Experience) to improve productivity as well as keeping them happy.

Data and information from various sources, including:

- Different systems,
- B2B,
- Government Agencies,
- Consumers,
- Customers,
- IOT Streaming,
- Social Media,
- Regulatory Compliance Bodies, and more.

Some are Commercial Business Sensitive Information, some are Customers' Private & Confidential information, and some are shareable between business partners only whilst some are shareable between customer only and others are publicly available information.

Data and Information are available in all shapes and forms – Structured Data, Semi Structured Data, and Unstructured Data. They come with different Variety, Velocity, and Volume. Many organizations are struggling to clearly know where they are and often must spend time discovering which assets and what type of data to be compliant with regulatory compliance bodies such as ASD ACSC ISM, NIST, ISO27001, GDPR, CDR, Open Banking PSD2, PII, HIPAA, HL7, PCI/DSS, FATCA/CRS, AML/CTF, KYC, etc.

Data and Information are not just from business systems, but they exist in emails, MS Access, SharePoint sites, Content Management Systems, Files, Archives, and many more. Do all organizations have a clear snapshot of all their assets and mapping to all their data and information? I would say NO.

There are many Data and Information Classification tools out there using AI and ML that can help to classify the massive Data and Information Landscape, and therefore able to implement better and more granular data security controls depending on their classifications, whilst adhering to the Data Security Regulatory Compliance mandates.

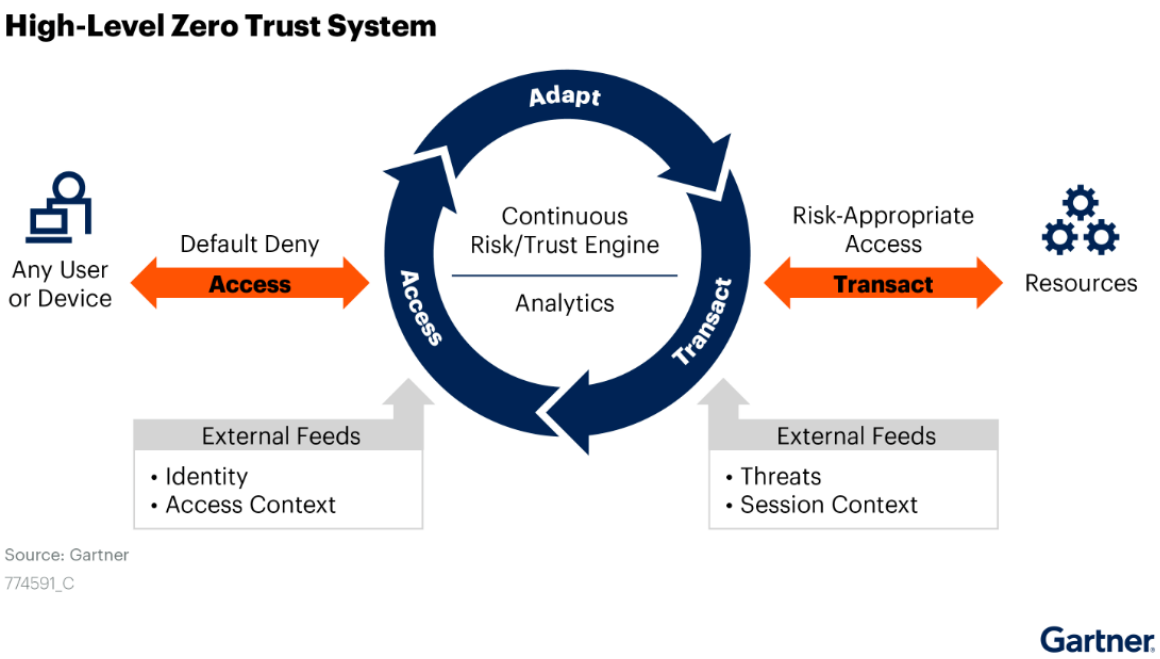
Implementing Zero Trust Security Strategy and Transformation

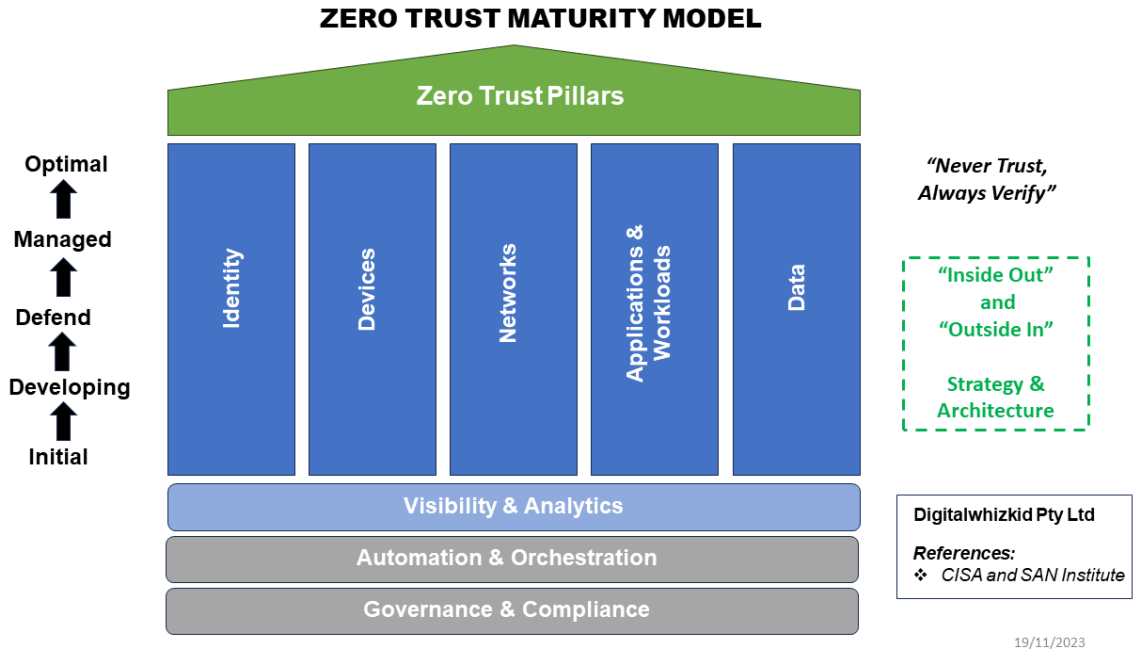
Development of an organization's Zero Trust Security Strategy and Transformation is not as easy as one would think.

You need to carefully analyse, learn, and devise a strategy of how to replace your current security technology solution stacks or overlay the legacy security solutions – would this create a monster and introduce more complexities, or do you start from nothing? What's the ROI? Why do we need to do this?

Implementing a Zero Trust Security Strategy still requires all the existing implementations of security controls such as Enterprise IAM, SSO, MFA, Phishing Prevention and Awareness, IDP (Intrusion Detection Prevention), IPS (Intrusion Prevention Systems), Data Security, DLP (Data Loss Prevention), SOC 1 & 2 and other compliance mandates.

Below is a diagram from Gartner showing a High-Level Zero Trust Security System – A Simplistic Viewpoint





Current State

- Heavily focused on perimeter security controls.
- Organisations' Culture of "Implicit Allow".
- Lack of Enterprise Corporate Policies which enforce Least Privileged Access.
- Coarse-grained security access.
- Network segmentation is at a high level, broadly segmented between network tiers.
- Applications are allowed to be rolled out in Production with limited security controls.
- Authentication is still based on weak single-factor authentication. In many cases, applications are still being developed using basic username and password authentication.
- Traditional network connectivity is still being used.
- "Implicit Allow" access across different business systems workloads (East-West Traffic).
- Some application securities are still not using Enterprise Users Directories such as Azure AD or Microsoft AD despite best practices that are widely available.
- Islands of disparate security directories, LDAP directories as legacy systems are still not being decommissioned.

Target State

- Finer grain access and authorization to resources after Authentication.
- Continually performing trust assessments to minimize risks.
- Micro-segmentation of access boundaries between users, applications, and workloads.
- Full encryption of network connections to protect data in transit.
- Explicit allow access to applications and workloads for fully authenticated and authorized users.
- Full logging and monitoring of user activities across all devices and locations.
- Strict adherence to the latest Top 10 OWASP Security Vulnerabilities and ensure proper DevSecOps principles and standards are being applied.
- Use of Confidential Computing environment for highly commercially sensitive information, in particular accounting and finance.
- Start implementing decentralization of databases and distributed data ecosystems security solutions as new Digital Ecosystems such as Microservices Containerisation Style Architecture

and Distributed Digital Block Chain Ledgers have been developed across new DEFI Decentralised Finance and NFTs Digital Platforms.

- Start collaboration with Multi-Cloud Multi Tenanted Hybrid on Premise Ecosystems Data Exchange Fabric Providers such as Equinox to take advantage of their E2E security control capabilities in the Next Generation landscape.

Strategic Core Technologies for Zero Trust Strategy Enablement

- **Data Classifications and Information Security Protection Technologies**

  Limiting the scope of data security protection, in my view, will help organizations speed up and enhance their protection from malicious attacks, stealing of sensitive information, and exposing customer privacy information. By applying data and information classifications, organizations can first focus on these Data/Information Classes and ensure that these classes are well-protected, continuously watched and risks are constantly being assessed and therefore provide business confidence to both the organizations and the customers.

  Varonis, Enterprise Data Security Platform solutions are one of the popular data security platform products in the marketplace. According to Forrester, Varonis was named as the Leader in Data Security Platforms in Q1, 2023.

  Here are key features provided by the Varonis Data Security Platform:

  - DSPM – Data Security Posture Management
  - Data Discovery & Classification
  - Data Activity & Auditing
  - Data-Centric UEBA
  - SSPM – SAAS Security Posture Management Software
  - Automated Data Remediation
  - Data Access Governance
  - Compliance Management
  - DLP Data Loss Protection
  - Active Directory Security
  - Insider Risks Management

  Amazon Web Services (AWS) supplies a data classification service called AWS Macie. This service provides discovery, data cataloguing, assessments of data types, labelling, handling of classification tiers, and continuous monitoring of the labelled datasets.

- **ZTNA (Zero Trust Network Architecture)**

  Cloud-based solutions such as Zscaler provide Zero Trust Network Access (ZTNA) where users of any organization's business applications can be accessed from anywhere in the world, with apps moving from inside the data centre to outside the network perimeter. Network and security

teams now must shift their focus that it is not about protecting their networks but it's about protecting users, devices, and business resources.

ZTNA solutions such as Zscaler ZTNA provide controlled access to organizations' resources by reducing the surface area for attack. The isolation afforded by ZTNA improves connectivity, removing the need to directly expose applications to the internet, which is an untrusted transport. Instead, application access occurs via an intermediary, which can be a cloud service controlled by a third-party provider or a self-hosted service.

Common features of ZTNA solutions:

- **Verify Identity**
  Instead of trusting an IP address, establish the identity of the user and device using an identity provider (IDP) first.

- **Set Contextual Policies**
  Access policies are defined based on user, device posture, location, and app, and they all rely on a cloud service to enforce them.

- **Improve Visibility and Adapt**
  Logs are used to determine which users are accessing which apps, and auto-adapt based on any changes in context.

- **SASE (Secure Access Service Edge)**
  Security Access Service Edge solutions provide secure access to the web, mobile, cloud services, and private applications always, anywhere the users are and no matter what devices are used, irrespective of where the applications are hosted – On-Premises, Private Cloud, and Public Cloud. SSE (Security Service Edge) can be implemented as part of the SASE framework and usually includes an integrated or separate ZTNA Zero Trust Network Architecture capability. This means that hybrid workers can connect at any location, branches and the extended workforce can connect via allowable devices from any location. SSE and SASE services provide advanced analytics and risk-trust scoring capabilities that enable the implementation of an identity and context-based logical access boundary around private applications and SAAS services. Remote browser isolation capabilities can also be enabled via this SASE framework.

- **CASB (Cloud Access Security Broker)**
  The use of Netskope CASB, a core part of Netskope Security Service Edge (SSE) can provide organizations and businesses with more confidence in adopting cloud applications and services without compromising security. It provides the ability to manage unintentional or unapproved movement of sensitive data between cloud app instances and in the context of app risk and user risks. Basically, CASB prevents sensitive data from being exfiltrated from your environment by risky insiders or external cyber criminals who have breached your perimeter security boundaries. For example, it can stop malicious insiders from copying sensitive content from business email to personal email accounts. In short, CASB provides the visibility and control needed to mitigate the risks in using Public and Private Cloud Applications and Services

CASB also supplies capabilities to automatically audit your application traffic and discover the overall risk profile across tens of thousands of applications used within your Production environment. Risk scores are based on 50 Cloud Security Alliance (CSA) defined attributes and cover seven profiles including security, risks, privacy, and compliance, and have a +99% accuracy rate for accessing risks in applications.

- **Next Generation Zero Trust IAM**

  With the increase in Digital Transformation business initiatives globally, organizations have now shifted their paradigm from the traditional closed-loop network perimeter to the modern, open-loop perimeter where apps, mobile, and tablets can be accessed anywhere in the globe. In addition, organizations also need to be able to establish trust relationships to securely enable access for various people such as contractors, employees, partners, supply chain providers, etc). This new modern perimeter needs to be protected and this starts with Security Identity.

  Solutions such as OKTA IAM is an example of an IAM technology solutions provider that provides comprehensive solutions set for organizations to enable Zero Trust Secure Identity.

  More importantly, the world has just emerged from the COVID-19 pandemic, and organizations are forced to shift to the hybrid working model and distributed working force across the nation or across the globe. The resources working from anywhere are now increasing and they are all accessing resources and data (in the Cloud and On-Premises) from more devices and locations than ever before.

  IAM security features such as SSO (Single Sign-On) and MFA (Multi-Factor Authentication) are becoming more of a “Must Have” for most organizations. With the new modern workforce frontier, According to Gartner in 2017, mentioned in a paper published on CARTA (Continuous Adaptive Risks and Trust Assessment), the new modern frontier requires more than just authentication and authorization. It necessitates continuous monitoring and assessments of the customer experience through adaptive risk-based assessments to identify potential threats.

- **Micro-segmentation**

  Logical segmentation or identity-based segmentation, now known as micro-segmentation, provides a more granular, fine-grain access and more dynamic policies for controlling East-West traffic within a particular macro segmentation segment. Micro-segmentation can have software packages, hardware, or infrastructure overlays such as Hypervisor, and IAAS where the workloads are segmented from other systems/assets. Typically, dynamic security policies are enforced at Layer 7 of the OSI model which follows the “Explicit Allow” Zero Trust model and thereby helps in reducing the risk of lateral movement of information.

- **Advanced Analytics, Identification, Detection and Response Technologies – SIEM, IDR, EDR, NDR, XDR and SOAR**

  With an increasing number of users and customer touchpoints and the ever-changing user and customer behaviours, security monitoring and analytics are evolving as more and more data and information are being captured through API integration, Event-Based Streaming, IOT Streaming, Data Replication, Publish and Subscribed Messaging, Hub and Spoke Integration and Point to

Point Integration. SIEM (Security Information and Event Management) technologies are maturing, and more options are available in the marketplace for EDR (Endpoint Detection and Response), NDR (Network Detection and Response) and XDR (Extended Detection and Response). These advanced security intelligence analytics platforms provide comprehensive user behaviour analytics, alert correlation, and incident responses. Most of the higher-end security intelligence platforms now include SOAR (Security Orchestration, Automation, and Response) tools. Endpoints Applications Integrations touch points and infrastructure posture can now be readily and easily assessed and IOT telemetry data can be streamed into context-based access controls for further context-based, sentiment analytics, which ultimately forms the E2E foundation of Zero Trust Architecture.

Common Organisations Problems and Challenges for Digital Security Transformation – especially Zero Trust Security Strategy Implementation

Technical Debt

Legacy security solutions architecture and its implementation, such as traditional network segmentation and Layer 4 Firewall Filtering and the traditional On-Premises security principles of classifying users as "Trusted" and "Untrusted", has been proven to be insecure. The assumption that everything operating in the internal organization environment is considered safe and secure is no longer viable and valid. This is because of increased attack sophistication and increased insider threats. In today's new Digital Era, we must go into the "Zero Trust World" where the key principle of "Never Trust, Always Verify" must always apply, to every user, every device, every location, and for every context and situation. Zero Trust Network Security Approach is different from the traditional On-Premises Security Controls Implementation. A more granular micro-segmentation of networks, compute, and resources, with finer grain perimeter security control implementation of both Authentication and Authorization, are necessary.

With the implementation of Zero Trust Security, we need to think of the ***Inside Out*** Security Strategy as opposed to the ***Outside-In*** Security Strategy.

Lack of Single Source of Truths from User Identities Perspectives

There are so many IDAM solutions being deployed, some On-Premises and new ones in the Multi-Cloud Ecosystems. This opens more potential security vulnerability endpoints and touchpoints. These proliferations of security directories need to be resolved through IDAM solutions or Security Directories Consolidation and Simplifications. Deployment of Federated Security Architecture would help in security simplifications and reduce the number of potential security vulnerability endpoints.

Often with disparate IDAM solutions in an organization, legacy employee's identity access management is poorly maintained. Especially with employees constantly changing roles, security policies and enforcement are not being properly updated and therefore often violate the fundamental principles of least privileged access and least privileged identity management.

Organization's Resistance to Change

The exercise where External Security Providers are brought in to determine excessive security privileges for VIP end users, Senior IT Specialists, and Power Users and mitigating and changing access and authorization controls is often proven to introduce lots of friction. This is especially the case from those who are used to having ownership of highly privileged accounts, and suddenly getting their privileges removed results in them feeling a loss of control. This has an enormous impact on Change Management Workflows and Access Policies; therefore, careful planning and a considered approach must be employed.

Lack of Skilled, Talented Resources

Most organizations will not have sufficient staff who have the knowledge, skills, and capabilities to drive the transformation shift to the new Zero Trust Security Posture Paradigm. Even if there exists one or two who may be capable, internal resistance would prevent these staff from being usefully deployed. This is especially the case if Insider Threats may exist. Hence, an External Security Providers or Contractors engagement will be more favourable and easier to get started.

Recommendations

- A well-defined scope for Zero Trust Strategy Implementation is necessary to be successful in the Enterprise Security Transformation Program.
- Full Buy-In from CISO, C-Level Executives, and the Board of Directors will be needed so that full support and commitment will be given to the program.
- Top-down communications at all levels "Must Be" made by all Senior Managers from both Business and Technology to get everyone on board with the "Business and Enterprise Architecture Vision".
- Develop strategies to overcome organizational "Roadblocks" through People and Culture, instilling new mindsets, getting people to embrace change, and providing education & training.
- Identify business use cases based on clear "Threat Modelling" techniques and conduct workshops to brainstorm potential security vulnerabilities and threat models that pose greater number of risks from financial loss, reputation loss, data breaches, damages to assets and so forth.
- Identify legacy security solutions that can be decommissioned. plan for obsolescence and replace them with the new Zero Trust Strategy Security Controls.
- Build an HCM (Human Capital Management) Strategy on how to acquire new Digital Talents and uplift the existing employees' capabilities through training, seminars, and hands-on experiences.
- Identify trusted co-sourcing business partners and advisory into the journey to the realization of the complex business initiatives.

Conclusions

Organizations should start thinking about developing a Zero Trust Security Strategy soon, with the increasing global risks of the growing number of "Bad Actors" both externally as well as "Insider Threats".

Seek an External Security Provider or Trusted-Advisor such as an Enterprise Architect, Enterprise Security Architect or Enterprise Security Advisor to conduct thorough Current State Assessments and work with C-Level Executives and key business and technology stakeholders to produce a comprehensive Zero Trust Enablement Strategy Paper first.

Thereafter, work collaboratively on the priorities, the budget, the resources, and the scope of the security transformation initiatives.

References

Coherent Market Insights – Zero Trust Global Market Trends

https://www.coherentmarketinsights.com/market-insight/zero-trust-architecture-market-5853

Gartner Zero Trust Strategy and Roadmap

https://www.gartner.com/doc/reprints?id=1-2EPJFOUO&ct=230814&st=sb&submissionGuid=5af350f0-1f3f-4c47-8b2a-3472a8ac068c

Zscaler, Zero Trust Strategy, and Solutions

https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report-thank-you

https://www.zscaler.com/capabilities/zero-trust-network-access

Okta, Zero Trust Framework in the Modern Perimeter Frontier

https://www.okta.com/au/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/

Gartner, 2017, CARTA Framework

https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age

Data Security Platform - Varonis

https://www.varonis.com/?utm_campaign=Google-Brand-NAM-English-Search-Leads&utm_medium=paidsearch&utm_source=google.com&utm-content=Varonis-Brand-Exact&utm_term=varonis&gad_source=1&gclid=EAIaIQobChMIl-SVmL_RggMVA0KRBR2CrgdEEAAYASAAEgIOH_D_BwE

AWS Macie – Data Classification

https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-overview.html

About the Author

David Pui is a seasoned "Transformation Architect" who specializes in both Enterprise Architecture and Solutions Architecture. He has extensive skills, qualifications, and experience in helping organizations transform and modernize to the next level of maturity. He focuses on Digital, Data, and Security Transformation. He is passionate about applying Business Architecture, Capabilities Modelling, Enterprise Architecture Framework, Architecture & Design Patterns, and Architecture Principles in the development of Enterprise Architecture, Strategy, Roadmaps, and Business & Technology Solutions Blueprints.

Any transformation involves change that impacts "People, Process, Data and Technology", and the use of business systems and Digital Technologies are tools and components that help the journey of achieving the business vision. Security Transformation is no different from any other modernization, the impacts are large, and careful planning and use of the right approach to problem-solving are key.

David enjoys reading and learning about new emerging industries and business technology innovations and always loves to contribute through writing articles and guest blogging when he has spare time.

CALL FOR SUBMISSIONS

by Darryl Carr, EAPJ Editor

The Enterprise Architecture Professional Journal welcomes contributions in its fields of interest, which are enterprise, business, application, information, integration, technology and security architecture, as well as the strategic management of business and technology transformation. EAPJ publishes peer-reviewed material that advances its fields of interest and supports the careers of its readers.

EAPJ combines the strengths of peer-reviewed technical journals and professional newsmagazines. EAPJ invites submission of academic, feature, opinion, and interview articles. The editorial staff also considers other submissions, such as images, interactive graphics, video, and animations. Successful submissions contain actionable information that enhances the capabilities of professionals working within the EAPJ fields of interest.

Each issue consists of one or more main articles, centered on a theme introduced by the Editor's Welcome. Main articles are generally no more than 5,000 words in length, but can be longer in certain circumstances, with body text preferably interspersed with numerous callouts, graphics or tables.

EAPJ encourages submissions, readership and community participation from qualified individuals representing the widest possible variety of geographical regions, cultures, backgrounds and beliefs. Authors must properly attribute all referenced content and ensure that their submissions do not infringe upon any copyrights or intellectual property laws if published in the EAPJ. EAPJ encourages potential authors to contact the editor early on to receive guidance on developing material with the greatest likelihood of publication.

EAPJ also seeks expert reviewers to work with the editor and authors on developing and selecting main articles for the journal.

Please send expressions of interest, submissions, questions, ideas or comments to editor@eapj.org. Potential authors and reviewers should introduce themselves by describing their background briefly, supplying a resume or CV, or referencing an online profile.

You can also submit ideas for publication on our website. Visit https://eapj.org for details.