**Edelweiss Applied Science and Technology**
*ISSN: 2576-8484*
*Vol. 9, No. 5, 2347-2354*
*2025*
*Publisher: Learning Gate*
*DOI: 10.55214/25768484.v9i5.7468*
*© 2025 by the authors; licensee Learning Gate*

# Integrating security into university operations: A case for TM forum's open digital architecture in higher education

Damir Regvart[1], Ivana Biškupić Ogrizek[2*], Ana Kapulica[3]
[1,3]Department of System Engineering and Cybersecurity Algebra Bernays University Zagreb, Croatia; damir.regvart@algebra.hr (D.R.) akapuli@algebra.hr (A.K.)
[2]Department of Interdisciplinary Sciences Algebra Bernays University Zagreb, Croatia; ivana.ogrizekbiskupic@algebra.hr (I.B.O.)

**Abstract:** Secure, scalable, and flexible digital ecosystems are becoming increasingly important as universities undergo a digital transition. The Open Digital Architecture (ODA) framework from the TM Forum provides a platform for modernizing digital services and telecommunications operations, with essential applications in higher education. This study investigates the effective use of ODA's cloud-native, modular, and interoperable components to improve security in university operations. This paper examines how ODA's security capabilities may address issues specific to higher education by connecting ODA components to essential university operations, including research data protection, student lifecycle management, and campus-wide applications.

***Keywords:*** *ODA, Security architecture.*

## 1. Introduction

The telecommunications sector is experiencing a significant shift, and the need for agility, flexibility, and improved consumer experiences is driving this transition. One crucial framework that helps service providers upgrade their processes is the Open Digital Architecture (ODA) developed by the TM Forum. Although ODA covers a wide range of digital transformation topics, its effects on network security stand out in particular [1].

This paper explores the benefits of ODA in the context of security, highlighting how its principal guidelines and practices contribute to a more secure digital ecosystem of Universities across various operational areas due to digital transformation. This paper study will show how they can meet essential needs like secure data management, compliance, and quick scalability by integrating essential ODA components, such as standardized APIs, microservices, data models, and secure cloud-native infrastructures in the day-to-day operations to create a safe digital environment in higher education. In the final notice, the latest version (v.5.0.0) of the ODA Component Definition was used in the discussion and other related documents.

## 2. Open Digital Architecture (ODA) Overview

ODA is a comprehensive framework designed to support the digital transformation of telecommunications and digital service providers. It provides a blueprint for integrating diverse systems and technologies, emphasizing modularity and interoperability. Organizations can decouple their legacy systems by adopting ODA, enabling them to respond quickly to market changes and customer demands.

Data models, operational procedures, and standardized APIs are fundamental elements of ODA. These components provide smooth system integration, increasing agility and efficiency. The ongoing evolution of cyberthreats and the increased security incidents [2] show the significance of security within the ODA framework context and the digital chain.

**History:** Received: 7 March 2025; Revised: 28 April 2025; Accepted: 5 May 2025; Published: 22 May 2025
* Correspondence: ivana.ogrizekbiskupic@algebra.hr

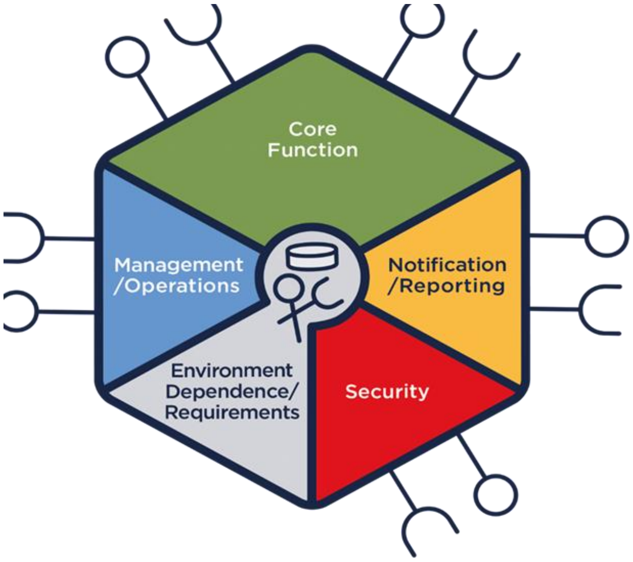

**Figure 1**
ODA Component illustration [3].

Figure 1 shows the main ODA components described by version 5.0.0 of the ODA Component. The following chapters explore component usage and possible roles in a university case study.

The Open Digital Architecture (ODA) is a revolutionary framework that reconfigures the IT systems of telecommunications companies to enhance agility, interoperability, and automation. It is structured around open APIs, standardized data models, and modular components that facilitate expedited integration of services and suppliers, minimizing complexity and expense. ODA facilitates transitioning from traditional, monolithic systems to microservices-oriented, cloud-native architectures, enabling Communication Service Providers (CSPs) to react more effectively to market demands.

Numerous recent studies underscore the pivotal importance of ODA in modernizing telecommunications infrastructure. Smidovych et al. demonstrate how ODA enables a shift from multichannel to omnichannel engagement by utilizing modular, functional components to enhance user experience and operational efficiency [4]. Mochalov et al. propose a distributed management system that conforms to the TM Forum's ODA framework to automate business processes and improve component-level optimization through microservices and Petri nets [5]. Xia et al. illustrate the efficacy of a function block methodology in ODA-based automation systems, enhancing interoperability and system scalability [6]. Diagne and Gervais propose an agent-based model based on open distributed processing principles, reinforcing ODA's focus on modular and flexible design [7].

Moreover, numerous implementations confirm the architecture's applicability. Siciarek and Wiszniewski [8] introduce an interactive variant of ODA to represent executable, layered documents [8] whereas Marti et al. offer a coder/decoder for medical multimedia records based on ODA standards [9]. HyperODA and similar extensions facilitate decentralized processing and multimedia integration, catering to the evolving demands of content [10]. The application of telecommunications persists, with reference models facilitating system transitions and competitive differentiation [11-13].

### *2.1. Key components of ODA*

Below are some of ODA's key components, and they go as follows:

- Core Function: Implements requirements limited by the information/data generated, processes/tasks, and functions (the tasks or actions the component is intended to accomplish).

- Supporting Functions - Addresses security, management, and operations requirements, as well as notification and reporting. Also included are Security Functions, Management and Operations Function, and Notification and Reporting Function
- External Interfaces / Component Functionality Exposure - provide the functionalities based on Application Programming Interface (API) operations

The above components highlight an adaptable, standards-based approach to designing digital infrastructure. This allows organizations to create solutions with modular parts that promote integration, reduce redundancy, and encourage automation throughout business procedures.

### *2.2. ODA Example Flow*

When a customer signs up for a service, data is transferred to several microservices (billing and CRM services) using standardized APIs. Real-time service provisioning and record updating allow the relevant service to promptly handle issues without requiring manual intervention across multiple processes. In the scenario utilizing the ODA modular approach, with every module serving a critical part or role in building an adaptable and efficient system, as shown in Figure . And discussed below.

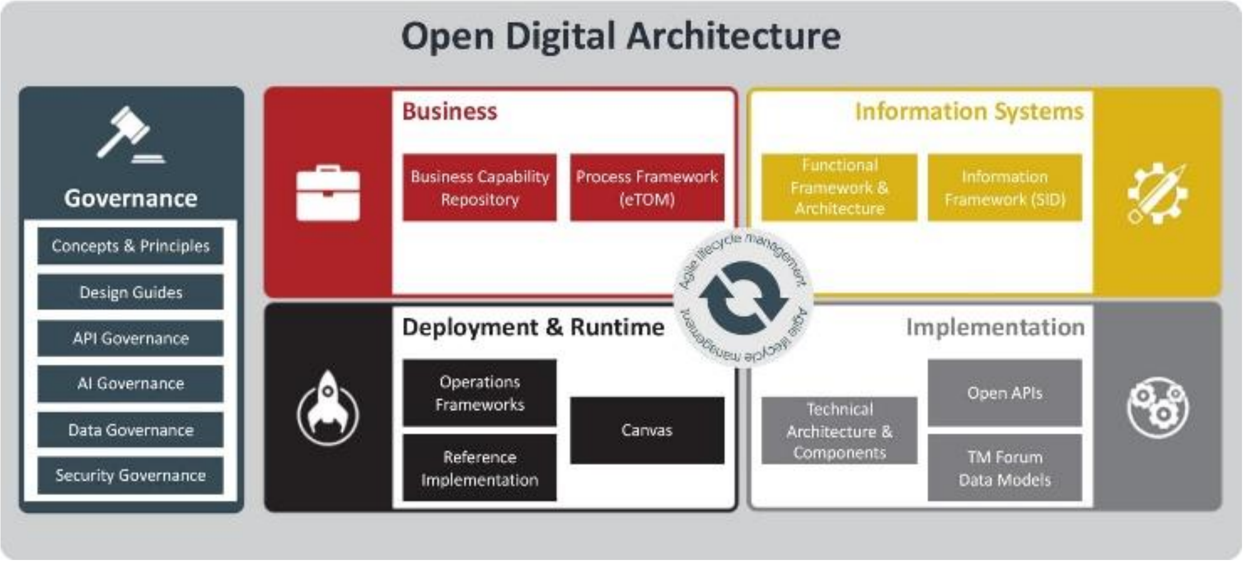

**Figure 2.**
ODA Architecture.

Governance provides a framework for ensuring architecture is consistent with company goals, regulatory constraints, and industry standards. It monitors the application of uniform rules, security measures, and compliance processes, ensuring responsibility at all levels of the architecture. This layer makes monitoring and auditing easier and critical for maintaining confidence and operational integrity. The business architecture defines and organizes processes and capacities according to strategic goals. It gives workflows a defined structure, encouraging flexibility and operational efficiency. Businesses can react quickly to shifts in the market or technological landscape.

The Information systems layer is the foundation of interoperability in ODA, as it offers frameworks for the seamless management and sharing of data across systems. Leveraging standardized data models and APIs, this layer enables real-time data exchange and ensures that applications and components can work together effectively. Its emphasis on data consistency supports analytics, decision-making, and operational visibility. The operational environment in which components function is addressed by

*DOI: 10.55214/25768484.v9i5.7468*

deployment and runtime. This section focuses on scalability to ensure systems adjust to changing needs while retaining high availability. It enables enterprises to grow resources effectively and attain dependable performance under various operating situations by providing cloud-native and modular deployments.

Implementation connects the practical deployments with architectural design. This layer uses standardized APIs, technical architecture, and reusable software components to produce composable solutions. It strongly emphasizes scalability and interoperability, enabling businesses to deploy simple modular systems to integrate and maintain.

### *2.3. Comparison with Traditional Architecture*

Traditional IT designs are typically based on rigid frameworks with closely coupled systems and applications, which frequently result in environments that are rigid and divided into separate sections. It may be challenging to accomplish interoperability or real-time data sharing between functions in the above configuration since each department or application may function independently with its own separate database and operating procedures [14]. Since various systems may need different resources for development and maintenance, this structure leads to redundancy and complicates integration. Traditional architectural scaling is sometimes expensive and time-consuming, including hardware upgrades and human configuration modifications for regular upkeep [15].

Traditional designs can be inconsistent and uniform in security, increasing the risk of vulnerabilities and making it more challenging to comply with current policies. In practice, systems are often guarded separately without a unified framework, especially with IoT-based architecture and security requirements [16].

## 3. ODA Framework

TM Forum's ODA consists of several modular component frameworks designed to create a flexible, scalable, and secure digital infrastructure:

- Business Process Framework - standardizes and organizes core business processes, enabling streamlined operations and automated workflows.
- Information Systems Framework: This framework provides a unified data model to organize and manage critical information assets, offering a single source of truth across systems.
- Implementation and API Framework: This framework enables interoperability and integration using standardized APIs to connect different systems and applications seamlessly.
- Security Framework - ensures consistent data protection, access control, and compliance with regulatory standards. It provides a centralized approach to securing the architecture's data, applications, and processes.
- Technology Architecture - enables rapid scalability and adaptability using virtualized infrastructure and microservices.
- Application Framework: This framework ensures that applications within the ODA environment are optimized for interoperability and can be deployed seamlessly within the larger system.
- Governance and Collaboration Framework enables secure and structured information sharing between stakeholders and external partners.

These ODA framework components are essential to building a safe, resilient, and flexible digital environment. Organizations can move away from old, monolithic IT systems and implement an architecture that can adapt to shifting technology environments by standardizing and modularizing essential operations like information management, security, and business processes. To guarantee effectiveness and uniformity throughout activities, the Business Process Framework and Information Framework, for example, arrange processes and data management. With the help of these frameworks, departments may collaborate more easily and make better decisions by having real-time access to correct data in a streamlined, coherent system.

## 4. Transition To ODA

As universities increasingly confront the limitations of traditional IT systems, the transition to more agile and secure digital frameworks has become a concern.

### *4.1. Research Problem*

Traditional University IT architectures are often characterized by packed, monolithic systems that manage various functions such as student information/registry, research data storage, and financial operations. All the characterized functions operate as an independent system. These legacy systems typically lack interoperability, which makes data sharing and integration across departments challenging. The growing usage of system resources in legacy systems draws in parallel an increase in sophisticated cyber-threat that needs to be solved independently for each part of the system separately. During a cybersecurity incident, it can cascade from one system to another [17].

Updates or modifications often require significant time and resources, leading to a rigid and inflexible infrastructure that struggles to meet the fast-paced demands of digital transformation. Traditional IT architectures are typically bound to on-premises environments, which limits scalability and makes it harder to address a university's fluctuating needs, such as increased demand for online resources or expanded research data storage space. These limitations and the difficulty of embedding robust security measures across disparate systems can hinder universities' ability to protect sensitive information effectively and comply with evolving data protection regulations.

The above leads us to a pertinent question: "Is there an improved method or strategy that will integrate substantial advancements in service delivery concerning digital development and the rise in cybersecurity threats?"

### *4.2. ODA Cloud-Native Approach*

TM Forum's ODA provides a modular, cloud-native, and API-centric framework that enables universities to integrate various systems, improve real-time data exchange, and augment agility throughout their digital services. Universities may install, update, and grow services, like learning management systems, research data management, or student portals, independently and without interfering with other systems using microservices architecture.

The ODA approach enables security integration at every architecture level by enabling system interoperability through standardized APIs and a flexible data model. By executing this principle, vulnerabilities are decreased and, hence, adherence to data privacy laws such as GDPR is improved [18]. Due to its cloud-based nature, ODA enables Universities to augment resources as necessary to meet demands for research storage, online learning, and secure remote access without incurring substantial hardware expenditures.

**Table 1.**
Comparison between traditional and Oda architecture.

| **Aspect** | **Architecture** | |
|---|---|---|
| | **Traditional** | **ODA** |
| Structure | Monolithic and tightly coupled | Modular and loosely coupled |
| Interoperability | Limited, vendor-specific | High, standardized APIs |
| Development and Deployment | Slow, resource-intensive | Agile, rapid development cycles |
| Scalability | Difficult to scale and adapt | Easily scalable through microservices |
| Data Handling | Rigid data formats, siloed data | Flexible data models, accessible analytics |

In contrast to traditional architecture, shown in Table 1, ODA emphasizes a modular, flexible architecture that promotes interoperability and agility. It builds an ecosystem that can quickly adjust to new services and technologies using standardized components and APIs.

## 5. ODA Components and University Use Cases

Understanding its foundational components and how they translate into practical, real-world implementations is essential for effectively applying Open Digital Architecture (ODA) within the university context.

### *5.1. Components*

TM Forum's ODA comprises several key components that can be effectively adapted to the diverse needs of a university environment, improving operational efficiency and security. The Business Process Framework as a core function is a key element that enables universities to optimize procedures, including student lifecycle management, course registration, and admissions. By organizing and automating these workflows, universities can reduce redundancies and improve coordination across departments, improving the student and staff experience.

Another critical component is the Information Framework, which creates a unified data model to consolidate student information, research data, and financial records into a centralized, accessible system. This system enables better decision-making, enables real-time data access across faculty departments, and increases the efficacy of data sharing and retrieval while offering a comprehensive perspective of university operations. ODA's API Framework is essential for integrating several campus applications, including research data platforms, student information systems (SIS), and learning management systems (LMS). Universities can connect these systems quickly and securely with defined APIs, enabling smooth data transfer and better application interoperability.

The Security Framework is essential in a university setting where protecting sensitive information, like student records and research data, is paramount. A security framework can help organizations better comply with legal obligations such as GDPR and state regulations by offering consistent security measures across all platforms, such as access controls and encryption. The Technology (Architecture) Framework component uses cloud-native infrastructure, allowing universities to easily grow their resources while reducing their dependency on expensive physical hardware.

Since universities require detailed reporting for audits and regulatory compliance, the Notification and Reporting Function is crucial for ensuring logs and statistical data, such as login attempts, data access frequency, and error logs, are captured and available for review. This is important for data compliance and security audits, as it provides insight into system usage and potential security vulnerabilities, enabling proactive adjustments.

### *5.2. Case-Study*

A basic flow example for a university case study would be student enrollment in a particular university course. The following paragraphs show the university's course registration process involving multiple stakeholders and systems.

The process begins with a student logging into the university portal, where the User Authentication Component verifies identity using multi-factor authentication and role-based access controls. The Student Information Management Component retrieves the student's academic records and eligibility through secure APIs defined by the Information Framework. The Course Catalog Management Component then checks course availability and interacts with a Reservation Management Component to temporarily secure seats for the student. The Schedule Management Component validates prerequisites and identifies overlapping course times to prevent scheduling conflicts, providing real-time feedback. Once the validation is complete, the system updates the student's academic record and confirms registration through the Notification and Communication Component. Financial calculations for tuition are handled by the Financial Management Component, which integrates with external payment gateways for secure transactions. Throughout the process, the Notification and Reporting Function logs activities for auditing and generates insights into registration trends. Real-time updates are pushed to dependent systems, such as faculty scheduling, ensuring end-to-end process synchronization.

This ODA-based approach's key features include standardized APIs for seamless integration, a Security Framework for secure data transmission and access, and cloud-native infrastructure for scalability during peak registration times.

## 6. Future Work

While this study demonstrates the applicability of TM Forum's Open Digital Architecture to modernizing university IT systems, several areas remain open for further exploration. Future research could focus on developing specific implementation roadmaps tailored to different types of academic institutions, such as large research universities versus smaller teaching-focused colleges, to evaluate the scalability and customization of ODA in varying environments. Another potential direction involves conducting longitudinal case studies that monitor the long-term impact of ODA adoption on security posture, operational efficiency, and compliance performance in higher education institutions. This would provide empirical evidence on cost-effectiveness, performance improvements, and reduction in incident response times.

Further investigation is needed into integrating AI and machine learning tools with ODA's Security Framework to enable predictive threat detection and automated policy enforcement. Moreover, research can explore how ODA's modular structure could support hybrid architectures that blend on-premises systems with cloud-native solutions, especially in data-sensitive academic settings. Finally, collaborative efforts between academia and industry could help refine the ODA components for the education sector, introducing new standards or extensions specifically designed to meet academic governance, pedagogical, and research-related needs.

## 7. Conclusion

TM Forum's ODA represents a transformative approach for telecommunications and digital service providers and can affect any digital infrastructure or service. By embracing the principles of modularity, interoperability, and cloud-native technologies, organizations can enhance their agility, reduce time to market, and deliver superior customer experiences.

Integrating TM Forum's Open Digital Architecture (ODA) into a university's course registration process demonstrates the transformative potential of a modular, interoperable, and secure digital framework. ODA enables seamless functionality and real-time coordination by decomposing the complex operations of student authentication, course catalog management, schedule validation, and financial processing into specialized components.

Standardized APIs provide uniform data interchange across systems, removing potential barriers and increasing operational efficiency. Using standardized APIs ensures secure integrations and prevents unauthorized access across the system on the Government ODA layer. Incorporating supporting functions, such as security, notification, and reporting, underscores ODA's ability to address critical challenges in higher education, including data protection and compliance with government regulations like GDPR. The scalability of cloud-native infrastructure. Allows universities to adapt dynamically to high-demand periods, such as registration enrollment deadlines. This paper's case study highlights ODA's role in modernizing institutional operations, reducing complexity, and fostering a secure and user-centric environment.

## Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

## Copyright:

## References

[1] M Forum, "Open digital architecture, White Paper," Retrieved: https://www.tmforum.org/resources/whitepapers/open-digital-architecture/. [Accessed Dec. 1, 2024], 2024.

[2] M. Repetto, A. Carrega, and R. Rapuzzi, "An architecture to manage security operations for digital service chains," *Future Generation Computer Systems*, vol. 115, pp. 251-266, 2021. https://doi.org/10.1016/j.future.2020.08.044

[3] TM Forum, "ODA component map," Retrieved: https://www.tmforum.org/oda/directory/components-map. [Accessed Dec. 1, 2024], 2024.

[4] L. Smidovych, Y. Kulyk, and M. Momot, "Telecommunication operator's transition to the omnichannel architecture," *Innovative Technologies and Scientific Solutions for Industries*, vol. 4, no. 30, pp. 165-174, 2024. https://doi.org/10.30837/2522-9818.2024.4.165

[5] V. P. Mochalov, N. Y. Bratchenko, S. V. Yakovlev, and D. V. Gosteva, "Distributed management system for infocommunication networks based on TM Forum Framework," in *CEUR Workshop Proceedings*, 2018, vol. 2254, pp. 81-93.

[6] F. Xia, H. Yin, Z. Wang, and Y. Sun, "Function block oriented architecture for open distributed automation," presented at the Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No. 04EX788), 2004.

[7] A. Diagne and M.-P. Gervais, "Building telecommunications services as qualitative multi-agent systems: The ODAC project," presented at the IEEE GLOBECOM 1998 (Cat. NO. 98CH36250), 1998.

[8] J. Siciarek and B. Wiszniewski, "IODA-an interactive open document architecture," *Procedia Computer Science*, vol. 4, pp. 668-677, 2011. https://doi.org/10.1016/j.procs.2011.04.070

[9] V. Marti *et al.*, "An ODA-based coder/decoder for multimedia medical documents," in *Proceedings of the Annual Symposium on Computer Application in Medical Care*, 1993, p. 849.

[10] W. Appelt and A. Scheller, "HyperODA-Going beyond traditional document structures," *Computer standards & interfaces*, vol. 17, no. 1, pp. 13-21, 1995. https://doi.org/10.1016/0920-5489(92)E0062-S

[11] R. Hunter, P. Kaijser, and F. Nielsen, "ODA: a document architecture for open systems," *Computer Communications*, vol. 12, no. 2, pp. 69-79, 1989. https://doi.org/10.1016/0140-3664(89)90060-1

[12] R. Carr, "ODA-The ISO standard for electronic document interchange," *Computer Standards & Interfaces*, vol. 7, no. 3, pp. 297-301, 1988. https://doi.org/10.1016/0920-5489(88)90090-6

[13] I. Campbell-Grant, "Update on the open document architecture standard and the work of the ODA consortium," *Information Management & Technology*, vol. 27, no. 2, pp. 71-74, 1994. https://doi.org/10.1108/imt-04-1994-0045

[14] J. Fishenden and M. Thompson, "Digital government, open architecture, and innovation: Why public sector IT will never be the same again," *Journal of Public Administration Research and Theory*, vol. 23, no. 4, pp. 977-1004, 2013. https://doi.org/10.1093/jopart/mus022

[15] S. Rudrakar and P. Rughani, "IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics," *Information Processing in Agriculture*, 2023. https://doi.org/10.1016/j.inpa.2023.09.002

[16] W. Hurst and N. Shone, *Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation* (Management and Engineering of Critical Infrastructures). Academic Press. https://doi.org/10.1016/B978-0-323-99330-2.00010-6, 2024.

[17] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies: Recent progress and future promise," *ACM Transactions on Management Information Systems*, vol. 12, no. 1, pp. 1-20, 2020. https://doi.org/10.1145/3389685

[18] A. Ziegler and M. Thomas, "Open digital architecture for cloud security and compliance: Integrating privacy principles," *Journal of Cloud Computing & Data Privacy*, vol. 14, no. 2, pp. 123-139, 2021. https://doi.org/10.1234/jccdp.2021.01456