International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

COMPLIANCE AUTOMATION IN AZURE: ENSURING REGULATORY COMPLIANCE THROUGH DEVOPS

Satheesh Reddy Gopireddy
Azure DevOps Engineer

Abstract

In today's rapidly evolving digital landscape, organizations face increasing pressure to comply with a multitude of regulatory standards while maintaining agility and speed in software delivery. The integration of compliance automation within DevOps practices presents a strategic approach to addressing these challenges. This paper explores how Microsoft Azure facilitates compliance automation through its robust suite of tools and services, enabling organizations to seamlessly integrate regulatory compliance into their DevOps workflows. We examine the key components of compliance automation in Azure, discuss best practices for implementation, and analyze the benefits and potential challenges associated with this approach. Through this exploration, the paper underscores the critical role of compliance automation in enhancing security, efficiency, and reliability in modern cloud-based environments.

Keywords: Compliance Automation, Azure, DevOps, Regulatory Compliance, Continuous Integration, Continuous Deployment, Security Compliance, Cloud Governance

I. INTRODUCTION

1.1 Background

In an era where digital transformation is pivotal for business success, organizations are increasingly leveraging cloud computing to enhance scalability, agility, and innovation. However, the adoption of cloud services introduces complex challenges related to regulatory compliance, security, and governance. Regulatory frameworks such as GDPR, HIPAA, and PCI DSS impose stringent requirements on how organizations manage and protect data, necessitating robust compliance strategies.

Traditional compliance approaches, often manual and reactive, are insufficient in keeping pace with the dynamic nature of cloud environments and agile development methodologies like DevOps. Compliance automation emerges as a critical solution, integrating compliance checks and controls seamlessly into the development and operational processes, thereby ensuring continuous adherence to regulatory standards.

Microsoft Azure, a leading cloud service provider, offers a comprehensive suite of tools and services designed to facilitate compliance automation. By leveraging Azure's capabilities within a DevOps framework, organizations can embed compliance into their workflows, enabling proactive, consistent, and efficient management of regulatory obligations.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

1.2 Purpose and Scope

This research paper aims to provide an in-depth exploration of compliance automation in Azure within the context of DevOps practices. The paper seeks to:

- Explore the concepts and importance of compliance automation and its integration with DevOps methodologies.
- Examine the specific Azure tools and services that support compliance automation.
- Discuss the implementation strategies, benefits, challenges, and best practices associated with compliance automation in Azure.
- Present real-world case studies illustrating successful applications of compliance automation in various industries.

The insights presented are intended to guide IT professionals, DevOps engineers, compliance officers, and organizational leaders in understanding and implementing effective compliance automation strategies using Azure.

1.3 Methodology

The research methodology involves a comprehensive review of existing literature, technical documentation, industry reports, and case studies related to compliance automation, DevOps practices, and Azure services. The paper synthesizes information from authoritative sources to present a coherent and practical perspective on the subject matter. Additionally, hypothetical scenarios and examples are utilized to illustrate key concepts and implementation approaches.

II. UNDERSTANDING COMPLIANCE AUTOMATION

Compliance automation refers to the use of automated tools and processes to ensure that an organization's IT systems and operations adhere to relevant laws, regulations, and standards. Automation streamlines compliance tasks such as policy enforcement, monitoring, reporting, and remediation, reducing the reliance on manual processes that are often time-consuming, error-prone, and inefficient.

Importance of Compliance Automation:

1. **Efficiency:** Automating repetitive compliance tasks frees up resources and reduces operational overhead.
2. **Consistency:** Automated processes ensure uniform application of compliance policies across the organization.
3. **Real-Time Monitoring:** Continuous monitoring enables immediate detection and response to compliance breaches.
4. **Scalability:** Automation supports the scaling of compliance efforts in line with organizational growth and evolving regulatory landscapes.
5. **Audit Readiness:** Automated documentation and reporting facilitate smoother and more transparent audit processes.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

6. **Risk Reduction:** Proactive compliance management minimizes the risk of regulatory penalties, reputational damage, and security breaches.

III. THE ROLE OF DEVOPS IN REGULATORY COMPLIANCE RESEARCH DESIGN

3.1 DevOps Principles

DevOps is a set of practices that combines software development (Dev) and IT operations (Ops) to shorten the systems development life cycle while delivering features, fixes, and updates frequently and reliably. Core principles of DevOps include:

1. **Collaboration and Communication:** Breaking down silos between development and operations teams.
2. **Automation:** Streamlining processes through automated tools for building, testing, deploying, and monitoring applications.
3. **Continuous Integration and Continuous Deployment (CI/CD):** Ensuring code changes are automatically tested and deployed to production environments.
4. **Monitoring and Feedback Loops:** Continuously monitoring systems and incorporating feedback for continuous improvement.
5. **Infrastructure as Code (IaC):** Managing and provisioning infrastructure through machine-readable definition files rather than manual processes.

3.2 Integrating Compliance into DevOps Practices

Integrating compliance into DevOps, often referred to as DevSecOps, embeds security and compliance considerations throughout the development and operations lifecycle. This approach ensures that compliance is not an afterthought but a fundamental component of the development process.

Key Strategies for Integration:

1. **Shift-Left Compliance:** Incorporating compliance checks early in the development process to identify and address issues promptly.
2. **Policy as Code:** Defining compliance policies through code that can be version-controlled, tested, and automated.
3. **Automated Compliance Testing**: Integrating compliance checks into CI/CD pipelines to ensure continuous adherence to regulatory standards.
4. **Continuous Monitoring:** Utilizing monitoring tools to detect and report compliance violations in real-time.
5. **Collaboration and Training**: Ensuring that all stakeholders understand compliance requirements and their roles in maintaining compliance.

Benefits of Integrating Compliance into DevOps:

1. **Reduced Time to Market:** Streamlined compliance processes reduce delays in software delivery.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

2. **Enhanced Security:** Early detection and remediation of compliance issues improve overall security posture.
3. **Cost Savings:** Preventing compliance breaches reduces potential fines and associated remediation costs.
4. **Improved Quality:** Consistent compliance checks lead to higher quality and more reliable software products.
5. **Regulatory Confidence:** Demonstrates to regulators and customers a commitment to maintaining high compliance standards.

IV. AZURE TOOLS AND SERVICES FOR COMPLIANCE AUTOMATION

Microsoft Azure offers a comprehensive suite of tools and services designed to facilitate compliance automation within DevOps workflows. The following sections detail the key Azure services that support this objective.

4.1 Azure Policy

Azure Policy is a service that enables organizations to create, assign, and manage policies that enforce and control the properties of resources. It ensures that resources comply with corporate standards and regulatory requirements by evaluating resources for non-compliance and taking corrective actions.

Key Features:

1. **Policy Definitions:** Predefined and custom policies that specify the rules and effects for resource compliance.
2. **Initiatives:** Collections of policies grouped together to achieve a specific goal, such as compliance with a particular regulation.
3. **Compliance Assessment:** Continuous evaluation of resources against policies with real-time compliance reports.
4. **Remediation:** Automatic or manual remediation tasks to bring non-compliant resources into compliance.
5. **Integration with CI/CD Pipelines:** Policies can be evaluated during deployment processes to prevent non-compliant resources from being provisioned.

Use Cases:

- Enforcing resource tagging standards.
- Restricting the deployment of specific resource types or locations.
- Ensuring encryption standards are met for data storage.
- Auditing and enforcing network security configurations.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

4.2 Azure Blueprints

Azure Blueprints enable organizations to define a repeatable set of Azure resources that implement and adhere to standards, patterns, and requirements. Blueprints facilitate the deployment of compliant environments at scale.

Key Features:

1. **Composable Artifacts:** Combining Azure Resource Manager (ARM) templates, policies, role assignments, and resource groups into a single blueprint.
2. **Versioning:** Maintaining different versions of blueprints to track changes and support continuous improvement.
3. **Locking Mechanisms:** Protecting critical blueprint resources from accidental modification or deletion.
4. Deployment Automation: Simplifying the provisioning of compliant environments through automated deployment processes.

Use Cases:

- Deploying standardized environments for development, testing, and production.
- Implementing compliance frameworks such as ISO 27001, HIPAA, or PCI DSS.
- Accelerating onboarding processes for new projects or teams.
- Ensuring consistency across multiple subscriptions and environments.

4.3 Azure Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of data centers and provides advanced threat protection across hybrid workloads.

Key Features:

1. **Security Posture Management:** Assessing security configurations and providing recommendations for improvement.
2. **Threat Protection:** Detecting and responding to threats with integrated security alerts and incident response capabilities.
3. **Compliance Management:** Monitoring compliance status against various regulatory standards with built-in compliance dashboards and reports.
4. **Integration with Azure Defender**: Extending protection to servers, data, and services across Azure and on-premises environments.

Use Cases:

- Continuous security assessments and compliance monitoring.
- Detecting and responding to security incidents.
- Managing security policies and controls across hybrid environments.
- Ensuring compliance with industry and regulatory standards.

4.4 Azure Monitor

Azure Monitor collects, analyzes, and acts on telemetry data from Azure and on-premises environments to maximize the availability and performance of applications and services.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

Key Features:

1. **Data Collection:** Gathering metrics and logs from various sources for comprehensive monitoring.
2. **Analysis Tools:** Utilizing queries and analytics to derive insights from collected data.
3. **Alerts and Notifications:** Setting up automated alerts based on specific conditions or thresholds.
4. **Visualization:** Creating dashboards and reports to visualize performance and compliance data.
5. **Integration with Automation**: Triggering automated actions based on monitoring data to enforce compliance and remediate issues.

Use Cases:

- Monitoring resource utilization and performance metrics.
- Detecting and responding to compliance violations and security anomalies.
- Providing audit trails and logs for compliance reporting.
- Supporting proactive maintenance and optimization efforts.

4.5 Azure DevOps Services

Azure DevOps Services provide development teams with tools for planning, developing, delivering, and maintaining applications. It supports the integration of compliance automation into the DevOps lifecycle.

Key Features:

1. **Azure Pipelines:** Automating builds and deployments with CI/CD pipelines that incorporate compliance checks.
2. **Azure Repos:** Hosting Git repositories for source control with policies to enforce code quality and compliance standards.
3. **Azure Test Plans:** Managing and executing test plans to ensure application quality and compliance.
4. **Extensions and Integrations:** Supporting a wide range of extensions and integrations for enhanced functionality, including security and compliance tools.

Use Cases:

- Implementing CI/CD pipelines with integrated compliance validations.
- Enforcing code quality and security standards through automated checks.
- Managing and tracking compliance-related tasks and issues.
- Facilitating collaboration between development, operations, and compliance teams.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

V. IMPLEMENTING COMPLIANCE AUTOMATION IN AZURE

Implementing compliance automation in Azure requires a strategic approach that aligns regulatory requirements with DevOps practices. This section outlines the key steps involved in successfully automating compliance within an Azure environment.

5.1 Establishing Compliance Requirements

The first step in implementing compliance automation is to clearly define the compliance requirements that apply to your organization. These requirements are often dictated by industry regulations, internal policies, and customer obligations. Common regulatory frameworks include GDPR, HIPAA, PCI DSS, and ISO/IEC 27001.

Key Activities:

1. **Identify Applicable Regulations:** Determine the specific regulations and standards that apply to your organization based on the industry, geographic location, and business activities.
2. **Define Compliance Objectives:** Translate regulatory requirements into specific, measurable objectives that align with your organization's goals.
3. **Engage Stakeholders**: Involve key stakeholders, including legal, compliance, security, and IT teams, to ensure a comprehensive understanding of the compliance landscape.
4. **Document Requirements:** Create a detailed compliance matrix that maps each regulatory requirement to specific controls, processes, and metrics.

5.2 Designing Compliance-as-Code

Compliance-as-Code is a practice that applies the principles of Infrastructure-as-Code (IaC) to compliance management. It involves codifying compliance policies, controls, and checks into version-controlled scripts that can be automatically enforced throughout the DevOps lifecycle.

Key Activities:

1. **Develop Policy Definitions:** Use Azure Policy to create custom policy definitions that enforce your organization's compliance requirements. These policies can cover areas such as resource configurations, data protection, and network security.
2. **Integrate with CI/CD Pipelines:** Incorporate compliance checks into your CI/CD pipelines using Azure DevOps. This ensures that code and infrastructure changes are automatically validated against compliance policies before deployment.
3. **Version Control:** Store compliance scripts and policies in a version-controlled repository, enabling continuous improvement and auditability.
4. **Automated Testing:** Implement automated tests that verify compliance with policies during the development and deployment processes.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

5.3 Continuous Compliance Monitoring

Continuous monitoring is essential for maintaining compliance in a dynamic cloud environment. By continuously assessing resources and configurations, organizations can identify and address compliance issues before they escalate.

Key Activities:

1. **Deploy Monitoring Tools:** Utilize Azure Monitor, Azure Security Center, and other tools to continuously collect and analyze telemetry data related to compliance.
2. **Set Up Alerts:** Configure alerts for non-compliance events, such as policy violations or unauthorized access attempts. These alerts should trigger automated or manual remediation actions.
3. **Compliance Dashboards:** Create real-time dashboards that provide visibility into compliance status across your Azure environment. Use Azure Monitor and Azure Policy to visualize compliance metrics and trends.
4. **Incident Response Plans:** Develop and document incident response procedures to address compliance breaches. Ensure that your team is trained to respond quickly and effectively to compliance incidents.

5.4 Incident Response and Remediation

Even with automated compliance controls in place, incidents may occur that require swift remediation. Establishing a robust incident response framework is crucial for minimizing the impact of compliance breaches.

Key Activities:

1. **Incident Detection:** Leverage Azure Security Center and Azure Sentinel to detect and analyze security incidents that may impact compliance.
2. **Automated Remediation:** Implement automated remediation scripts that can be triggered by policy violations or security incidents. These scripts should restore resources to a compliant state or isolate affected systems to prevent further damage.
3. **Post-Incident Review:** Conduct thorough post-incident reviews to identify root causes and improve compliance controls. Document lessons learned and update compliance policies as necessary.
4. **Reporting and Documentation:** Ensure that all incidents and remediation actions are thoroughly documented to support audit and reporting requirements.

VI. IMPLEMENTING COMPLIANCE AUTOMATION IN AZURE

6.1 Define Compliance Requirements

- Identify Regulations: Pinpoint applicable regulations like GDPR, HIPAA, or PCI DSS.
- Set Objectives: Convert regulations into clear, measurable compliance goals.
- Collaborate: Engage legal, compliance, and IT teams to ensure alignment.
- Document: Create a compliance matrix linking requirements to controls.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

6.2 Design Compliance-as-Code

- Policy Creation: Use Azure Policy to codify and enforce compliance rules.
- CI/CD Integration: Embed compliance checks into CI/CD pipelines for automated validation.
- Version Control: Store and manage compliance scripts in a version-controlled repository.

6.3 Continuous Monitoring

- Deploy Tools: Use Azure Monitor and Security Center for real-time compliance tracking.
- Set Alerts: Automate alerts for non-compliance incidents.
- Dashboard Visibility: Build dashboards to visualize compliance status and trends.

6.4 Incident Response

- Detection: Leverage Azure Security Center for prompt incident identification.
- Remediation: Implement automated scripts for swift remediation.
- Post-Incident Review: Analyze incidents to strengthen future compliance efforts.

VII. CHALLENGES AND CONSIDERATIONS

While compliance automation offers significant benefits, organizations must also address the challenges and complexities associated with its implementation. This section discusses the potential obstacles and considerations that must be navigated to ensure successful adoption.

7.1 Complexity of Regulations

Regulatory frameworks are often complex and vary across industries and geographies. Automating compliance in such an environment requires a deep understanding of the specific regulations and how they apply to cloud-based operations.

Key Considerations:

- Diverse Regulations: Organizations operating in multiple industries or regions may need to comply with a wide range of regulations, each with unique requirements.
- Dynamic Regulatory Landscape: Regulatory requirements are constantly evolving, requiring organizations to stay updated and adapt their compliance strategies accordingly.
- Custom Compliance Policies: Predefined policies may not fully cover the specific needs of an organization, necessitating the creation of custom policies and controls.

7.2 Integration with Existing Systems

Integrating compliance automation into existing IT and DevOps workflows can be challenging, particularly in organizations with legacy systems or siloed operations. Ensuring seamless integration and avoiding disruption to ongoing operations is critical.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

Key Considerations:

- Legacy Systems: Older systems may lack the necessary interfaces or capabilities to support automated compliance processes.
- Cross-Platform Integration: Organizations using multiple cloud providers or on-premises systems must ensure that compliance automation is consistent across all platforms.
- Change Management: Implementing compliance automation may require significant changes to existing processes and workflows, necessitating careful planning and execution.

7.3 Organizational Culture and Skills

Successful implementation of compliance automation requires a shift in organizational culture and the development of new skills. Teams must be trained to work with automated tools and processes and to collaborate effectively across departments.

Key Considerations:

- Skill Gaps: IT and DevOps teams may need additional training to effectively implement and manage compliance automation tools.
- Cultural Resistance: Resistance to change is common in organizations, particularly when new technologies and processes are introduced. Building buy-in and fostering a culture of continuous improvement are essential.
- Collaboration: Compliance automation requires close collaboration between IT, DevOps, security, and compliance teams. Ensuring effective communication and alignment is critical for success.

VIII. BEST PRACTICES FOR SUCCESSFUL IMPLEMENTATION

To maximize the benefits of compliance automation in Azure, organizations should adopt best practices that align with their unique needs and regulatory requirements. This section outlines key recommendations for successful implementation.

8.1 Collaboration between Teams

Effective compliance automation requires collaboration between development, operations, security, and compliance teams. Breaking down silos and fostering a culture of shared responsibility is essential for achieving continuous compliance.

Recommendations:

- Cross-Functional Teams: Establish cross-functional teams that include representatives from all relevant departments to ensure alignment and collaboration.
- Regular Communication: Hold regular meetings and workshops to discuss compliance goals, challenges, and progress.
- Shared Responsibility: Promote a culture where compliance is viewed as a shared responsibility, with everyone playing a role in maintaining regulatory adherence.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

8.2 Continuous Learning and Improvement

Compliance automation is not a one-time project but an ongoing process that requires continuous learning and adaptation. Organizations must stay informed about regulatory changes, emerging technologies, and best practices to remain compliant.

Recommendations:

- Continuous Training: Provide ongoing training and development opportunities for teams to stay updated on the latest compliance tools and practices.
- Feedback Loops: Implement feedback loops to gather insights from compliance audits, incidents, and performance metrics. Use this feedback to refine and improve compliance processes.
- Staying Informed: Monitor regulatory developments and industry trends to ensure that compliance policies and practices are up-to-date.

8.3 Leveraging Automation and AI

Advanced automation and artificial intelligence (AI) can significantly enhance compliance processes by improving accuracy, efficiency, and responsiveness. Organizations should explore and integrate these technologies to optimize their compliance automation strategies.

Recommendations:

- AI-Powered Compliance: Utilize AI and machine learning to analyze compliance data, predict potential risks, and recommend remediation actions.
- Automation of Routine Tasks: Automate routine compliance tasks, such as policy enforcement, reporting, and remediation, to reduce manual effort and minimize errors.
- Scalable Automation Solutions: Implement scalable automation solutions that can grow with the organization and adapt to new regulatory requirements.

IX. CASE STUDIES

To illustrate the practical application of compliance automation in Azure, this section presents two hypothetical case studies from different industries.

9.1 Healthcare Industry Example

A large healthcare organization operates in multiple regions and must comply with regulations such as HIPAA and GDPR. By implementing compliance automation using Azure, the organization was able to:

- Automate Data Protection: Azure Policy and Azure Key Vault were used to enforce encryption standards and protect sensitive patient data across all environments.
- Continuous Monitoring: Azure Security Center provided continuous monitoring of security configurations, detecting and remediating compliance issues in real-time.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023 ISSN No: 2348-9510

- Scalable Compliance: Azure Blueprints were used to deploy standardized, compliant environments across multiple regions, ensuring consistent adherence to regulatory requirements.

The organization achieved a significant reduction in compliance management costs, improved security posture, and faster audit preparation.

9.2 Financial Services Industry Example

A financial services company faced challenges in managing compliance with PCI DSS and other financial regulations across its hybrid cloud environment. By adopting compliance automation in Azure, the company:

- Integrated Compliance Checks: Azure DevOps Services were used to integrate automated compliance checks into CI/CD pipelines, ensuring that code and infrastructure changes met regulatory standards before deployment.
- Real-Time Reporting: Azure Monitor and Azure Policy provided real-time visibility into compliance status, enabling the company to address issues proactively.
- Improved Audit Readiness: Automated reporting and documentation through Azure Compliance Manager streamlined the audit process, reducing the time and effort required for compliance verification.

The company experienced enhanced operational efficiency, reduced risk of regulatory penalties, and greater confidence in its compliance posture.

X. CONCLUSION

Compliance automation in Azure represents a strategic approach to managing regulatory compliance in today's complex and dynamic cloud environments. By integrating compliance into DevOps workflows, organizations can achieve continuous compliance, reduce operational overhead, and enhance their security posture.

Microsoft Azure provides a comprehensive set of tools and services that support compliance automation, enabling organizations to automate policy enforcement, monitoring, reporting, and remediation. While challenges such as regulatory complexity, integration with existing systems, and organizational culture must be addressed, the benefits of compliance automation far outweigh the obstacles.

By adopting best practices, fostering collaboration, and leveraging advanced automation and AI technologies, organizations can ensure that their compliance efforts are proactive, scalable, and aligned with their business goals. Compliance automation is not only a key driver of security and efficiency but also a critical enabler of digital transformation in the cloud.

REFERENCES

1. Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (2018). Regulated software meets DevOps. Inf. Softw. Technol., 97, 176-178. https://doi.org/10.1016/J.INFSOF.2018.01.011.
2. Rios, E., Iturbe, E., Larrucea, X., Rak, M., Mallouli, W., Dominiak, J., Muntés, V., Matthews, P., & Gonzalez, L. (2019). Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems. IET Softw., 13, 213-222. https://doi.org/10.1049/IET-SEN.2018.5293.
3. Elgammal, A., Türetken, O., Heuvel, W., & Papazoglou, M. (2016). Formalizing and appling compliance patterns for business process compliance. Software & Systems Modeling, 15, 119-146. https://doi.org/10.1007/s10270-014-0395-3.
4. Beach, T., Hippolyte, J., & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. Automation in Construction, 118, 103285. https://doi.org/10.1016/j.autcon.2020.103285.
5. Michener, J., & Clager, A. (2016). Mitigating an Oxymoron: Compliance in a DevOps Environments. 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 1, 396-398. https://doi.org/10.1109/COMPSAC.2016.155.
6. Soliman-Junior, J., Tzortzopoulos, P., & Kagioglou, M. (2022). Designers' perspective on the use of automation to support regulatory compliance in healthcare building projects. Construction Management and Economics, 40, 123 - 141. https://doi.org/10.1080/01446193.2021.2022176.
7. Vuppalapati, C., Ilapakurti, A., Chillara, K., Kedari, S., & Mamidi, V. (2020). Automating Tiny ML Intelligent Sensors DevOPS Using Microsoft Azure. 2020 IEEE International Conference on Big Data (Big Data), 2375-2384. https://doi.org/10.1109/BigData50022.2020.9377755.
8. Becker, J., Delfmann, P., Eggert, M., & Schwittay, S. (2012). Generalizability and Applicability of Model-Based Business Process Compliance-Checking Approaches — A State-of-the-Art Analysis and Research Roadmap. Business Research, 5, 221-247. https://doi.org/10.1007/BF03342739.
9. Soliman-Junior, J., Tzortzopoulos, P., Baldauf, J., Pedó, B., Kagioglou, M., Formoso, C., & Humphreys, J. (2021). Automated compliance checking in healthcare building design. Automation in Construction, 129, 103822. https://doi.org/10.1016/j.autcon.2021.103822.