

How Zenity Helps Financial Institutions Meet FDIC Regulations

Financial institutions must adhere to stringent regulations set forth by the Federal Deposit Insurance Corporation (FDIC) to ensure the security and confidentiality of customer information. Title 12, Chapter 3, Subchapter B, Part 364 of the Code of Federal Regulations is of particular note, and outlines the standards for information security that these institutions must follow; particularly surrounding how customer information and data is handled. Zenity, a leader in securing Enterprise Copilots and Low-Code Development, offers comprehensive tools to help financial institutions meet these regulatory requirements effectively.

Context for Enterprise Copilots and Low-Code Relating to Customer Information

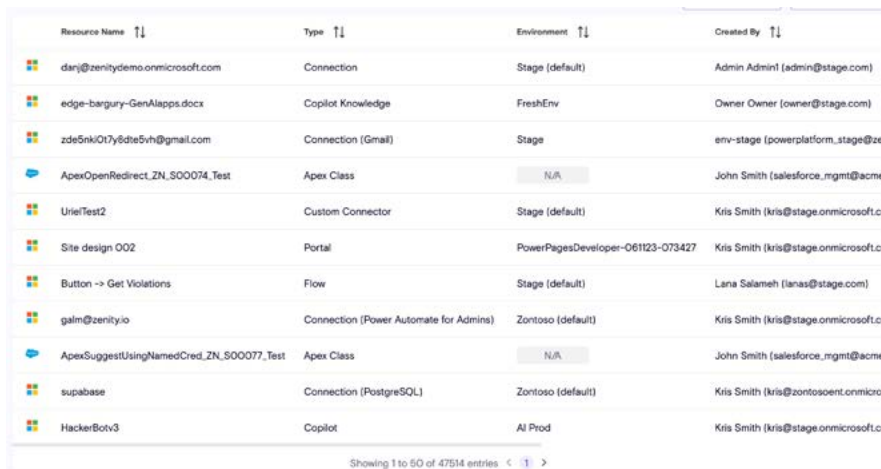
Enterprise copilots and low-code development platforms are increasingly adopted by enterprises to empower business users of all technical backgrounds. Unfortunately, they also enable business users to build apps and process data that they shouldn't due to a lack of guardrails and ease of misconfiguration. With the average enterprise now creating nearly [80,000 apps, copilots, and bots across various platforms](#), with upwards of 11,000 of them possessing access to sensitive data, this is a massive attack surface¹.

Furthermore, these apps are undetectable by traditional code scanning AppSec and CI/CD pipeline tools. Security teams need to be aware of which apps and resources are touching sensitive data. Only then can they go about securing those apps.

Ensuring Security and Confidentiality of Customer Information

Objective 1: Ensure the security and confidentiality of customer information.

Zenity provides robust security measures that integrate seamlessly with enterprise copilots and low-code development platforms via APIs to maintain continuous inventory of all apps, copilots, and bots, and how they are used throughout the enterprise. By implementing application security controls around these tools, Zenity ensures that customer information remains confidential and protected from unauthorized access including locking down apps that contain access to sensitive data so that they are only used by authorized, authenticated, and necessary personnel. Zenity's platform continuously monitors data access patterns and flags any anomalies, ensuring that only authorized personnel can access sensitive information through applications that are built outside of the traditional software development lifecycle (SDLC).



Resource Name	Type	Environment	Created By
darj@zenitydemo.onmicrosoft.com	Connection	Stage (default)	Admin Admin! (admin@stage.com)
edge-bargury-GenAlapps.docx	Copilot Knowledge	FreshEnv	Owner Owner (owner@stage.com)
zde5nk0t7y8dte5vh@gmail.com	Connection (Gmail)	Stage	env-stage (powerplatform_stage@zer
ApexOpenRedirect_ZN_500074_Test	Apex Class	N/A	John Smith (salesforce_rmgmt@acme
UriTest2	Custom Connector	Stage (default)	Kris Smith (kris@stage.onmicrosoft.cc
Site design 002	Portal	PowerPagesDeveloper-061123-073427	Kris Smith (kris@stage.onmicrosoft.cc
Button -> Get Violations	Flow	Stage (default)	Lana Salameh (lanas@stage.com)
galim@zenity.io	Connection (Power Automate for Admins)	Zontoso (default)	Kris Smith (kris@stage.onmicrosoft.cc
ApexSuggestUsingNamedCred_ZN_500077_Test	Apex Class	N/A	John Smith (salesforce_rmgmt@acme
supabase	Connection (PostgreSQL)	Zontoso (default)	Kris Smith (kris@zontosoeent.onmicr
HackerBotv3	Copilot	AI Prod	Kris Smith (kris@stage.onmicrosoft.cc

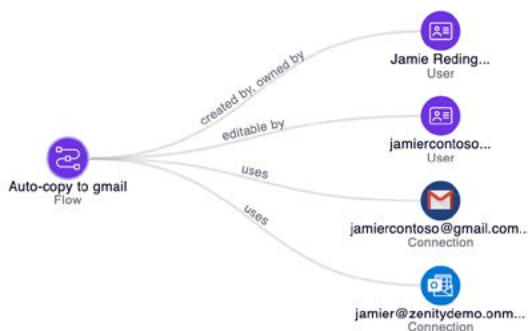
¹ Zenity Research Report: The State of Enterprise Copilots and Low-Code Development, September 2024

Objective 2: Protect against any anticipated threats or hazards to the security or integrity of customer information.

Zenity employs a multi-layered security approach to protect against both internal and external threats. This includes real-time threat detection, automated risk assessments, and proactive vulnerability management for any application that is built outside of the SDLC that interacts with customer data. As apps, copilots, and bots are built by business users of all technical backgrounds with no guardrails as far as what data they interact with, security teams need ways to ensure that any threats to customer information are detected and snuffed out immediately. Zenity's AI-driven analytics identify potential threats before they can cause harm, allowing financial institutions to mitigate risks promptly using playbooks and policies to enforce guardrails silently, so as to meet compliance without hindering productivity.

Objective 3: Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

One of the most common misconfigurations in low-code application development is building an app or copilot that either uses an insecure method to authenticate users, or doesn't use one at all. In our research, we have found the average enterprise has roughly 8,400 apps or copilots that do not have proper authentication. This is a clear path to unauthorized access when apps are overshared, under-authenticated, and unseen by security. Zenity is able to detect when applications are built that have improper or non-existent authentication mechanisms and place guardrails to enforce proper controls automatically or with integrations to ITSMs, SOARs, or other tooling. Additionally, Zenity's platform prevents employees from inadvertently sharing sensitive data with unauthorized parties through automated policy enforcement and real-time alerts.



Risk Assessment and Management

Another piece of meeting FDIC mandates is to ensure access controls are in place to prevent unauthorized access, as stated in Section III.C: Manage and Control Risk. Zenity's risk assessment engine helps financial institutions identify and evaluate potential threats to customer information via faulty access controls. By conducting continuous risk assessments and providing detailed reports, Zenity enables institutions to analyze the business context of their enterprise copilots and low-code apps and enforce proper guardrails around meeting FDIC regulations.

In the event where an app is leaking data, Zenity's playbooks and policies ensure automated remediation is in place. Zenity's platform provides detailed audit logs and guidance on remediation steps. This helps financial institutions minimize the potential of data breaches and maintain customer trust.

Conclusion

Zenity's comprehensive security solutions are designed to help financial institutions meet FDIC regulations effectively. By ensuring the security and confidentiality of customer information, protecting against threats, preventing unauthorized access, and providing robust risk assessment and management tools, Zenity enables financial institutions to maintain compliance and safeguard their customers' data.

For more information on how Zenity can help your institution meet FDIC regulations, please visit <https://www.zenity.io/use-cases/business-needs/compliance/>.



About Zenity

Zenity, the world's first company focused on securing and governing low-code/no-code and Generative AI based development, protects organizations from security threats, helps meet compliance, and enables business continuity. Established in 2021, many of the world's leading organizations trust Zenity to help configure security guardrails, generate prioritized lists of vulnerabilities, and accurately pinpoint and remediate vulnerabilities by continuously scanning all connected low-code/no-code and GenAI development platforms with centralized visibility, risk assessment, and governance. For more information, visit us at <https://www.zenity.io>