

Information Security Update

Christian Johnson
Chief Information
Security Officer





Information Security at ARIN

Overview

Compliance Initiatives

General Updates

Roadmap Impacts on Security

Information Requests

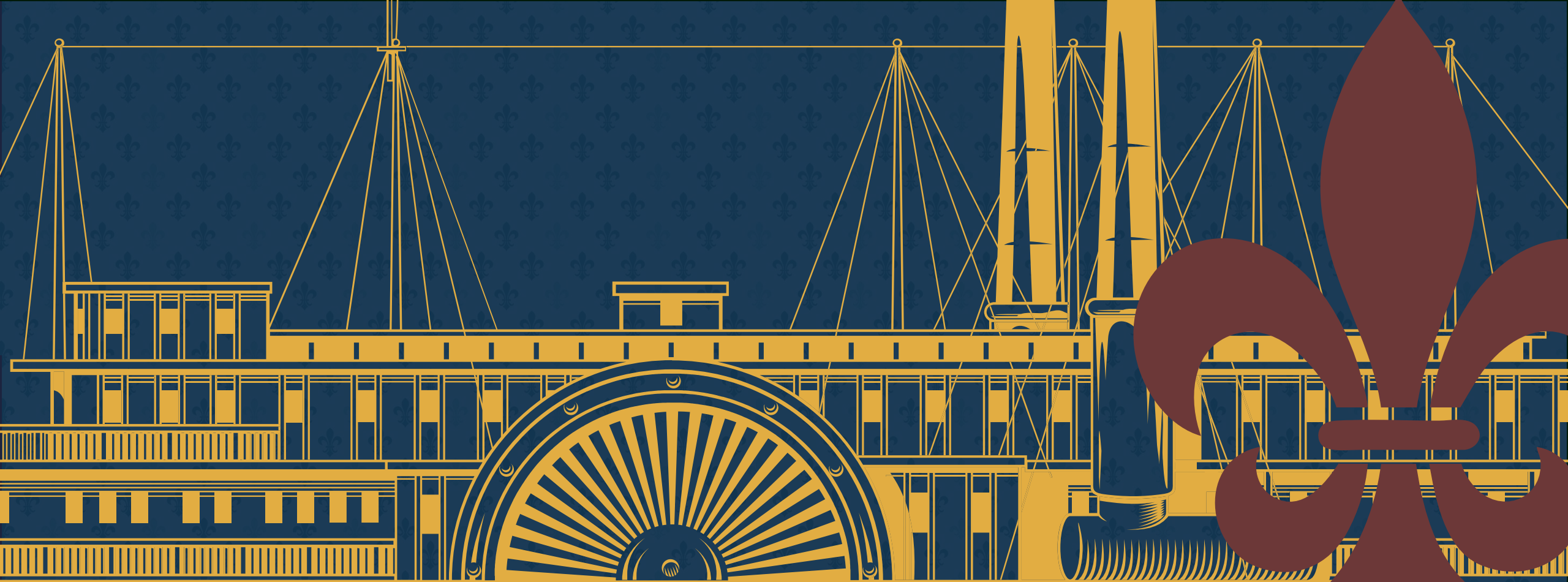
Overview

Focus on the basics

- Maintain up-to-date, security-minded infrastructure
- Sensitize users to security threats and expectations
- Enhance reporting capabilities
- Enable threat identification
- Remove threats and remediate vulnerabilities

What we're doing

- Building security-conscious architecture, reducing tech debt, ensuring vendor security
- Providing policies and training
- Facilitating easy reporting
- Improving logging, scanning, identification, and remediation
- Conducting regular continuity, recovery, and response drills

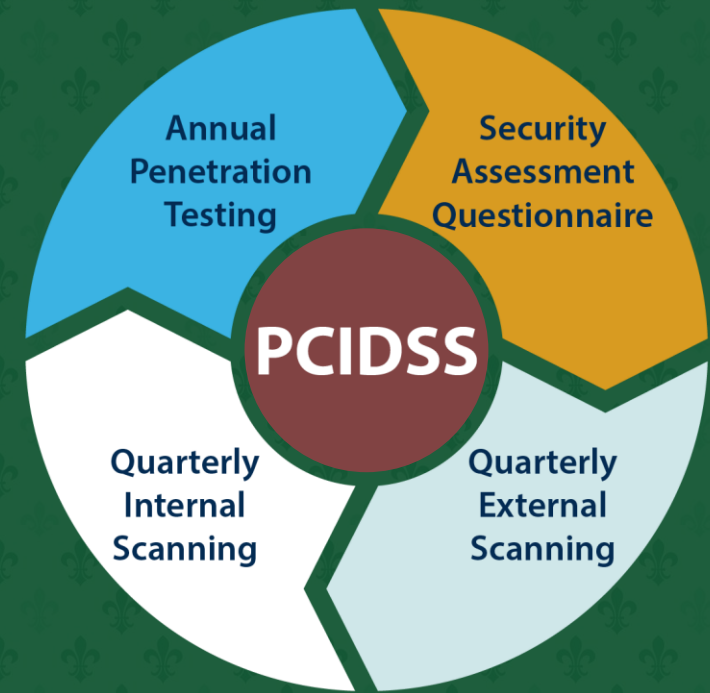


Compliance Initiatives

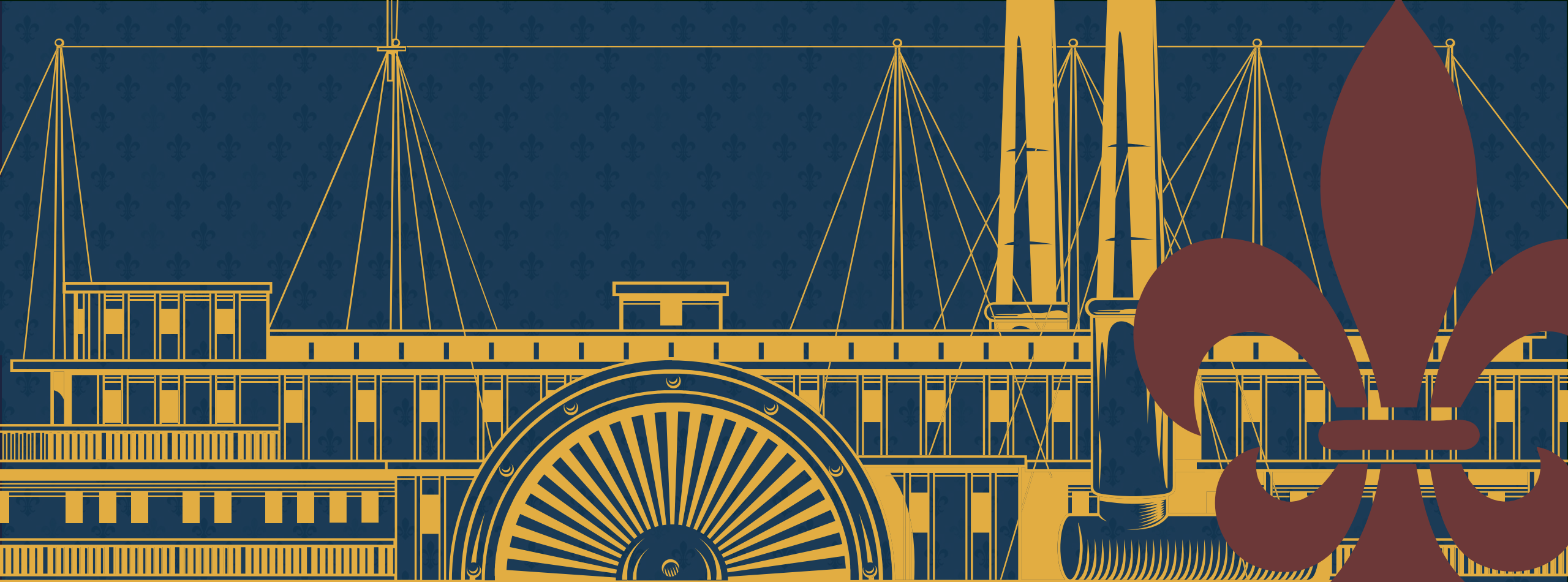
Compliance Initiatives



- RPKI and Organization
- Current cycle: 2025-2026
- ARIN Online also in this cycle



- ARIN Online and Organization
- Current cycle: 2025-2026



General Updates

General Security Updates - 2025

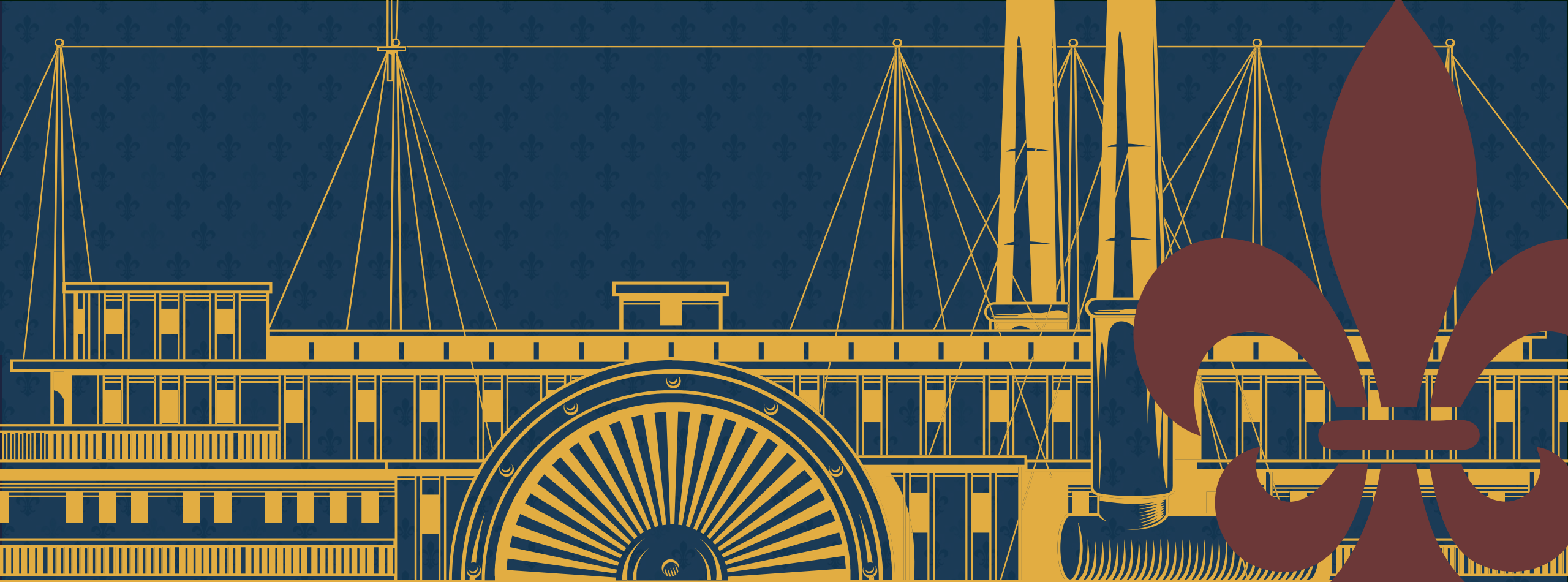


- ✓ ARIN's annual security assessment (penetration test)
- ✓ Monthly vulnerability scanning and patching
- ✓ Annual and new hire security training – 100% trained
- ✓ Monthly phishing defense training
- ✓ Work with SOC 2 auditors
- ✓ Prep work to add ARIN Online to our SOC 2 program
- ✓ Support to ARIN's Risk & Cybersecurity Committee

New and Upcoming Initiatives



- Enhanced monthly vulnerability scan reviews
- Monthly web malware scans of arin.net
- Social media monitoring of the Team ARIN Twitter account
- Background checks for all staff
 - Checks previously run on new hires & certain positions
 - Proceeding with a phased approach for all staff
 - Tentatively scheduled to be complete by end of year
- ARIN's 2026 SOC 2 audit will include RPKI and ARIN Online



Impacts on Security



Impacts on Security



Data center move and Kubernetes migration

Pros

- Resolves a number of tech debt items
- Removes a number of vulnerabilities
- Removes a significant amount of overhead

Opportunities

- Remapping our scanner agents for vulnerability scanning
- Redocumenting our architecture for SOC 2 and PCI purposes
- Reviewing/updating processes and policies, where appropriate
- Rescheduling our annual security assessment (penetration test)



Communicating With You

Information Security at ARIN

On this page

- » Certification
- » Security Practices at ARIN
- » What We Do to Secure Your Data
 - Security Audits
 - Internal Security Measures
 - Security for External System Users
- » What You Can Do to Secure Your Data
- » More Information
 - Requesting Security Information from ARIN
 - Bug Bounty Inquiries
 - ARIN Personal Data Privacy Principles

ARIN is committed to the security of your data. We have implemented various measures to protect your user account and record information and to ensure that your communication with ARIN is trusted.

Certification

ARIN understands customers' need to verify appropriate security baselines are being met. To meet this need, we pursue industry standard security certifications that attest to our ability to safeguard our systems and data.

Recognizing the global importance of cybersecurity and the value of Service Organization Control (SOC) 2 as a relevant framework to North America and our customer base, ARIN successfully completed the SOC 2 Type II audit of its Resource Public Key Infrastructure (RPKI) in October 2023. ARIN's SOC 2 compliance demonstrates its ongoing commitment to protecting sensitive customer and organizational data from unauthorized access via its infrastructure, tools, and processes. You may download our SOC 3 report (a publicly releasable version of our SOC 2 report) [here](#).

ARIN takes the security of its customers' critical data and the payment process seriously. We have completed a review with our payment card vendor and verified ARIN Online's compliance with the Payment Card Industry Data Security Standard (PCI DSS). While PCI DSS focuses on the security of the cardholder data environment, there is a tremendous amount of security control validation that must be done across ARIN Online and the entire company to achieve this certification. We are proud to be able to confirm the security of ARIN Online and our customers' financial data.

Read [our post on the ARIN Blog](#) for more information on our SOC 2 and PCI DSS certifications.



Information Security at ARIN

- Application Programming Interface (API) Keys
- Multifactor Authentication (MFA)
- Pretty Good Privacy (PGP) Authentication

Information Security Webpage

- ARIN's information and data security practices
- What we do to secure your data
- What you can do to secure your data
- Download ARIN's SOC 3 report

Information Requests

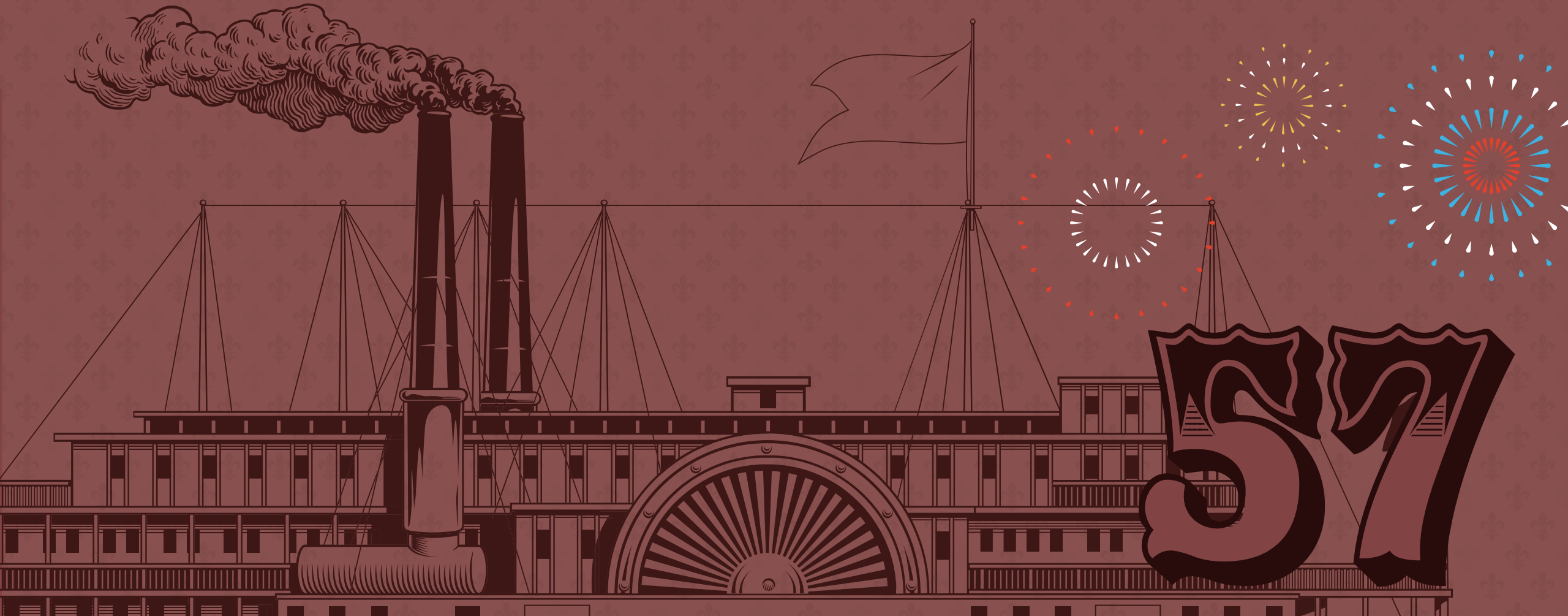
What is happening

- Customer compliance teams request ARIN manually complete a vendor security questionnaire.
- "Can't renew contract until ARIN's security info is provided."
- Most requests are answered by information on the InfoSec at ARIN page.

Improving the process

- Direct requestors to the InfoSec at ARIN webpage.
- Our SOC 3 report is publicly available on the page.
- Further requests should be submitted as a ticket in ARIN Online.

Questions and Comments?



57