

North America Community Meeting 2023



Introduction



DUSTIN RICH
PCI Practice Lead

Dustin Rich is the PCI Practice Lead at A-LIGN and has performed PCI DSS assessments over the past 17 years. As an IT professional with over 25 years of IT experience, Dustin has the technical background and experience to manage large complex IT environments. Dustin has worked with Fortune 500 companies, large retail environments, higher education, contact centers, cloud service providers, independent sales organizations (ISO), payment gateways, and both acquiring and issuing banks. With over 17 years of QSA experience, Dustin is a great resource and has had opportunities to speak at conferences for higher education, card industry vendors, and the PCI SSC annual community meetings.



Get Audit-Ready In A Fraction of The Time By Leveraging Powerful Automation

A-SCEND for PCI DSS Compliance

About A-LIGN

The A-LIGN Advantage

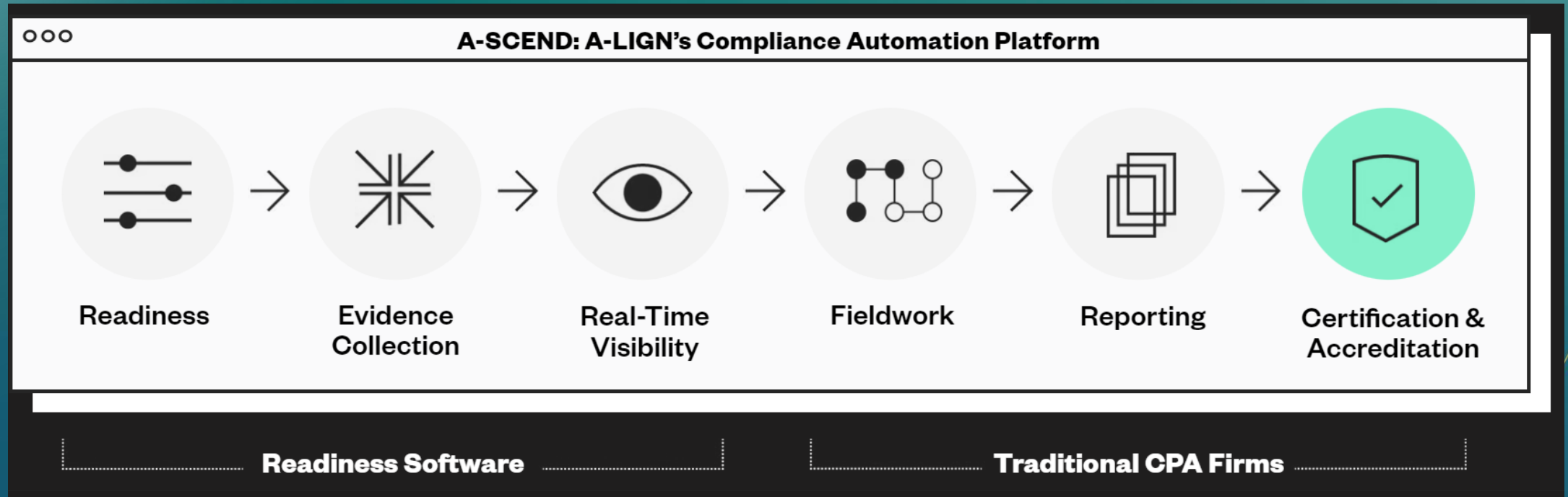
We mitigate cybersecurity risk worldwide:

- 4k+ global customers
- 1k+ PCI DSS assessments completed
- 97% client satisfaction rating
- 10+ years of experience
- Intuitive automation software + Trusted auditor experience



A-SCEND

Streamlined Compliance with A-SCEND



- **End-to-End Compliance Management:** Perform audit preparation, automated readiness, automated evidence collection, and controls testing all in one system of record

Streamlined Compliance with A-SCEND



Standardized Information Requests:
Reduce the total number of requests required from each additional audit by comparing common security frameworks and creating one request



Centralized Evidence Collection:
Quickly upload evidence to a single location either through manual upload or automation

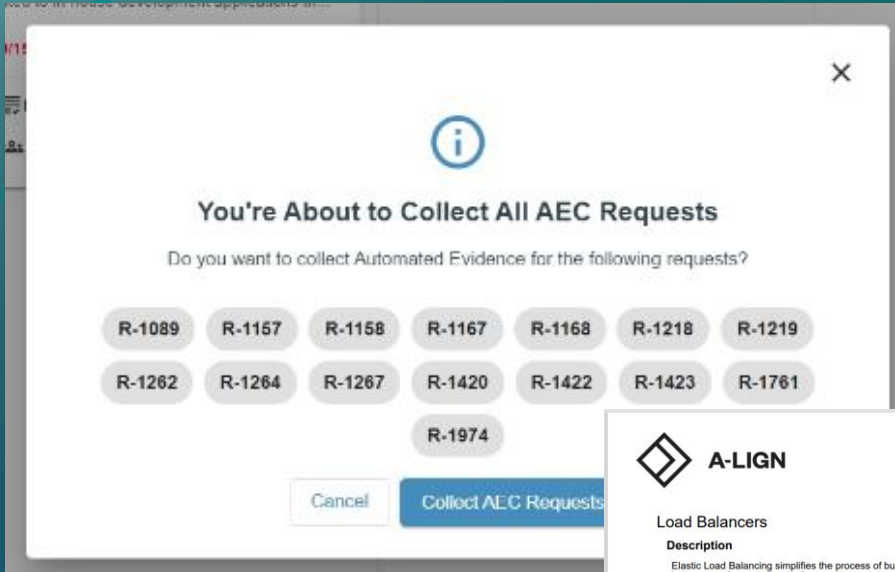


Consolidated Audit Dashboard:
Maintain visibility and oversight into the progress of your team's compliance efforts



Assignment Management: Assign information requests and manage evidence collection all in a single place

Simplified Evidence Collection



- ◆ Leverage **90+** integrations to automate the busy work
- ◆ The Automated Evidence Collection (AEC) engine **crawls the available APIs** of your integrated cloud and service providers to **collect data elements**
- ◆ Creates **human-readable** evidence and attaches evidence to the **correct request(s)**

A-LIGN A-SCEND Automated Evidence Collection

Load Balancers

Description

Elastic Load Balancing simplifies the process of building secure web applications by terminating HTTPS and TLS traffic from clients at the load balancer. The load balancer performs the work of encrypting and decrypting the traffic, instead of requiring each EC2 instance to handle the work for TLS termination. Application Load Balancers support HTTPS listeners. Network Load Balancers support TLS listeners. Classic Load Balancers support both HTTPS and TLS listeners.

It is recommended that the Load Balancer Listeners associated with the Load Balancers in the table of this report use these available protocols by attaching an IAM or ACM certificate to the listener.

References

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html>

Table

Name	Balancer Type	ARN	Region
demo-network-lb-tf	network	arn:aws:elasticloadbalancing:us-east-1:275789386687:loadbalancer/network/demo-network-lb-4f9d4dd77679d5f11c	us-east-1
awseb-AWSEB-13JL346X3ZQOP	application	arn:aws:elasticloadbalancing:us-east-1:275789386687:loadbalancer/app/awseb-AWSEB-13JL346X3ZQOP/11683bwebc6a9ddd	us-east-1

Load Balancer Listeners

Description

When you configure a secure listener, you specify the cipher suites and protocol versions that are supported by your application, and a server certificate to install on your load balancer. You can use AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM) to manage your server certificates.

It is recommended that all Load Balancer Listeners have an IAM or ACM certificate attached that uses HTTPS or TLS protocols.

AWS-003 | Page 3 of 6 07/24/2023

Simplified Policy Management

The screenshot displays the A-LIGN Policy Center interface. The main dashboard shows a 'Policy Status' bar with the following counts: Draft (6), In Review (1), Approved (1), Rejected (0), Overdue (0), Annual Review (0), and Total (8). Below this is a table of 'Selected Policies' with columns for Policy Name, Assignee, Approver, Type, Approved On, and Status. The table lists policies such as 'Access Control', 'Configuration Standards', 'Business Continuity and Disaster Recovery Policy', and 'HP Policy'. An inset window shows the 'Policy Center' editor for 'Configuration Standards', which includes a 'Purpose and Overview' section and a '1. Configurations Standards' section with detailed text and a 'Your Configuration Standards Policy' sidebar.

Policy Name	Assignee	Approver	Type	Approved On	Status
Access Control			Template Policy		In Review
Configuration Standards					
Business Continuity and Disaster Recovery Policy					
3b6ffaac-db21-4e23-a610-0285a9e87f1f					
HP Policy					
Human Resource Management					
Patching and Vulnerability Management Policy					

- Industry best practice policy guideline templates provided as examples to assist with new compliance programs

- Policy editor to track all changes from the original template

- Policy review and approval workflow

- Already have a policy? Upload your existing policies

- Quickly map approved policies to evidence requests

Real-Time Visibility

The screenshot displays the A-LIGN Compliance Hub interface. On the left is a dark sidebar with navigation options: Home, Compliance Engagements, Readiness Assessments, Policies, Integrations, AEC Reports, Compliance Hub (highlighted), and Settings. The main content area is titled 'Compliance Hub' and shows a 'Groups' section with '1 Test Groups' and an 'Add' button. A card for 'AWS Compla...' is visible, showing '52 Tests' and a status of 'Active'. The 'AWS Compliance Monitor' section shows 'AWS - 52 Tests (0 Selected)' with buttons for 'Refresh Connection', 'Start', 'Enable', and 'Disable'. Below this is a table of test results:

Category	Test Name	Status	Actions
Identity and access management	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Fail	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy requires at least one uppercase letter	Passed	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy requires at least one lowercase letter	Passed	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy requires at least one symbol	Passed	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy requires at least one number	Passed	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy requires minimum length of 14 or greater	Fail	Play, Edit, Toggle
Identity and access management	Ensure IAM password policy prevents password reuse	Fail	Play, Edit, Toggle
Identity and access management	Ensure MFA is enabled for the 'root' user account	Passed	Play, Edit, Toggle
Identity and access management	Ensure hardware MFA is enabled for the 'root' user account	Passed	Play, Edit, Toggle

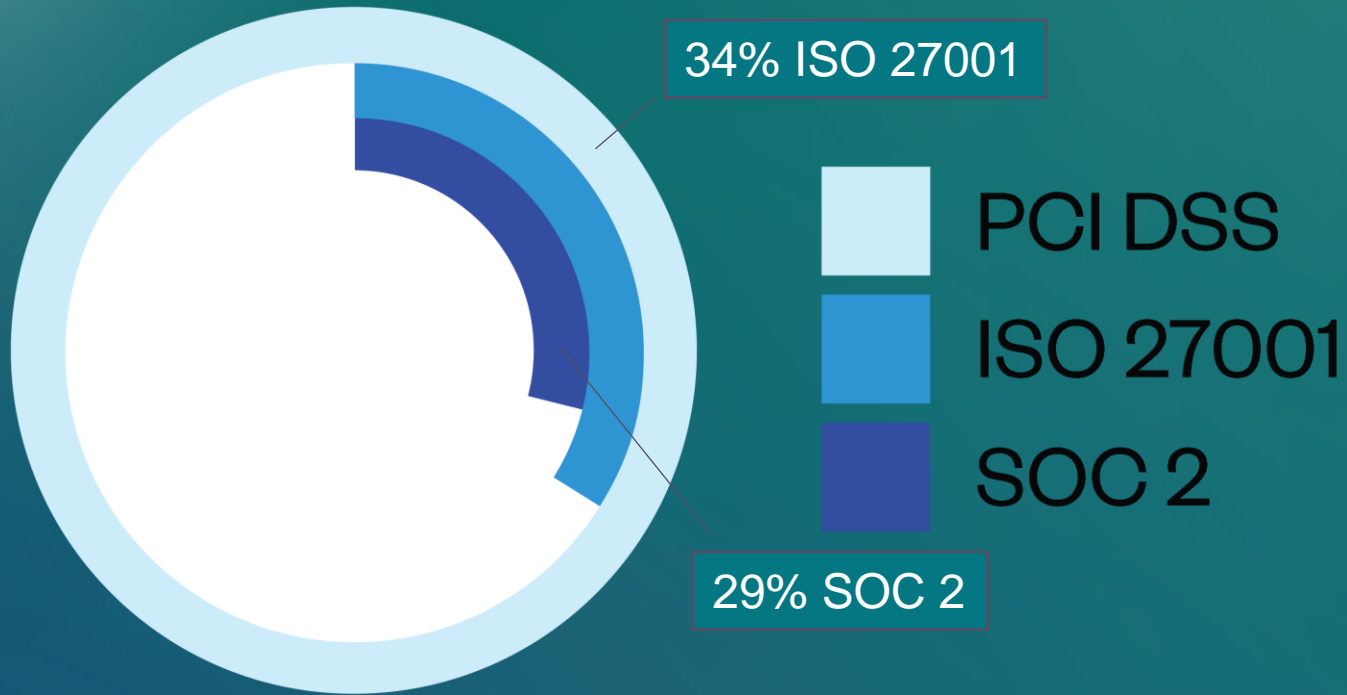
- Run **scheduled or ad hoc assessments** of your cloud and SaaS service providers

- Performs **tests against industry best practice configuration guidelines**

- Test results help identify and **provide the industry guidance necessary to remediate** any identified configuration issues

- Continuous monitoring provides **ongoing visibility and reporting** over time

Additional Audits in a Fraction of the Effort



• Completing a PCI DSS assessment with A-SCEND fulfills many requirements for future frameworks including:

- SOC 1
- SOC 2
- ISO 27001
- FedRAMP
- FISMA
- HIPAA
- Microsoft SSPA control



Thank you!

Dustin Rich

Dustin.rich@a-lign.com