PCI Security Standards Council®

Optimizing Cloud Security Compliance

An overview of how Palo Alto Networks manages their complex cloud security compliance and certification program through an optimized approach.

Agenda

1. Palo Alto Networks Cloud Security Certification Program
2. Common Challenges of Cloud Security Compliance
3. Optimized Approach to Cloud Security Compliance

PCI Security Standards Council®

Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations. Powered by Precision AI, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection.

Peter Ngo

Peter leads the Product Management, Global Certifications organization at Palo Alto Networks which oversees global cloud security compliance efforts to various frameworks and standards including SOC 2, ISO, PCI DSS, BSI C5, ISMAP, IRAP and more for 22+ cloud products.

Peter holds various security and professional certifications, including the CCSP, CISSP, PCI ISA, CISA, CISM, CDPSE & ISO Lead Auditor, in addition to a Master of Science degree in Information Assurance.

Cloud Certification Team

The Cloud Compliance & Attestation Program is intended to facilitate and optimize the Palo Alto Networks attestation process for cloud security and compliance efforts. Our team's goal is to reduce implementation timeframes, identify enterprise-wide efficiencies, and minimize the impact on Product Teams, allowing them to stay focused on day-to-day operations and product development.

The GCAT Cloud Certification Team provides:

- Certification subject matter expertise
- Technical program management (TPM) of certifications
- Internal and cross functional resourcing
- Engagement of outside vendors and management of contracts
- Certification efficiencies and automations

PCI Security Standards Council

Palo Alto Networks Cloud Security Certification Program

PCI Security Standards Council®

Benefits of Cloud Security Compliance

- **Competitive Advantage**
- **Customer Assurance**
- **Proactive Security**
- **Marketing Differentiation**
- **Brand Protection**
- **Regulatory Compliance**
- **Peace of Mind**
- **Optimized Sales Response**

PCI Security Standards Council®

Cloud Security Compliance Growth

SOC 2
40% growth seen from 2021 to 2022.

BSI C5
German standard 60% growth

IRAP
AU standard 50% growth

ISO
ISO 27001, 27017, 27018, 27701, & 27032 covering 25 products.

ISMAP
JP standard 30% growth

VPAT Sec 508
Accessibility standard.

PCI DSS
SAQ D

TISAX
German automotive.

HIPAA - GDPR - NCSC
Privacy

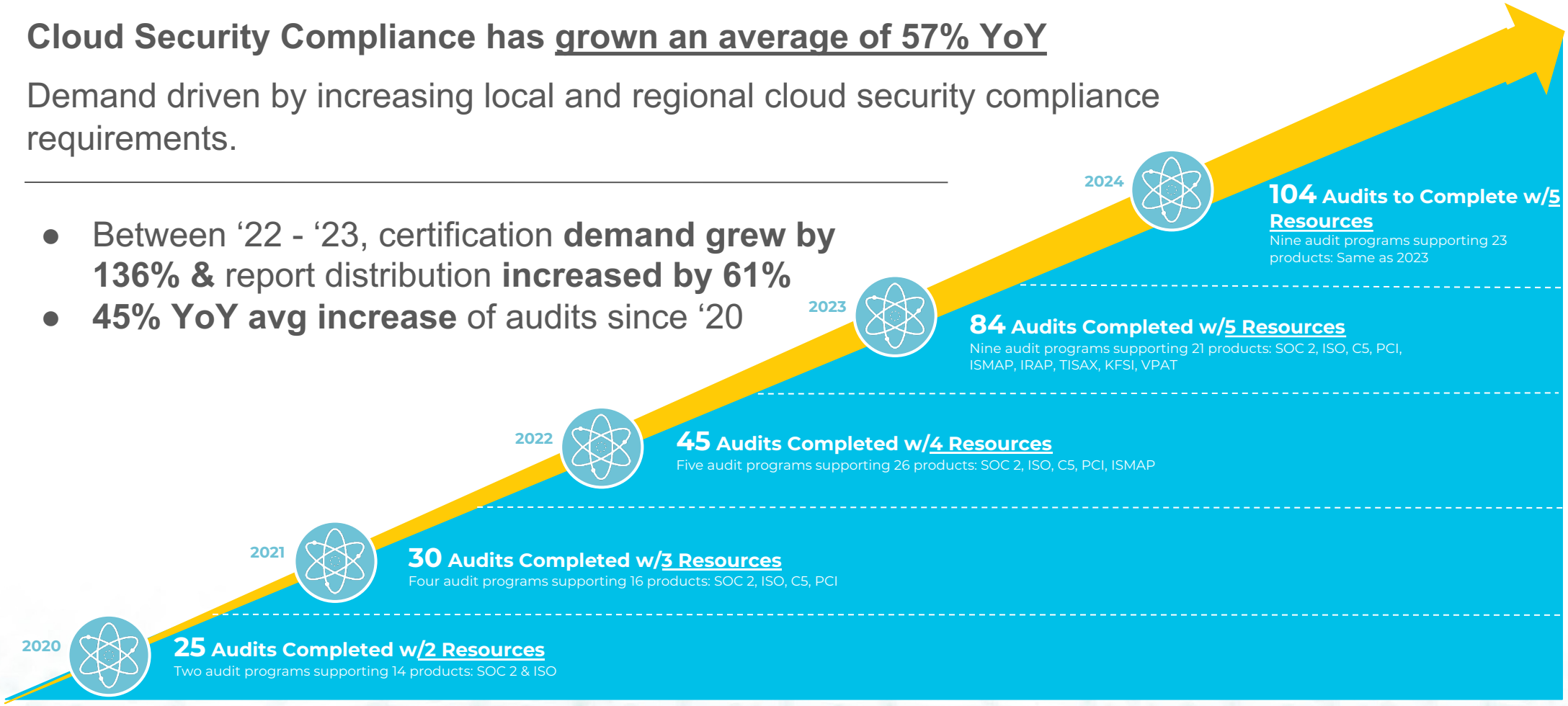
PCI Security Standards Council

Cloud Certification Growth

Cloud Security Compliance has grown an average of 57% YoY

Demand driven by increasing local and regional cloud security compliance requirements.

- Between ‘22 - ‘23, certification **demand grew by 136% &** report distribution **increased by 61%**
- **45% YoY avg increase** of audits since ‘20



PCI Security Standards Council®

Common Challenges of Cloud Security Compliance

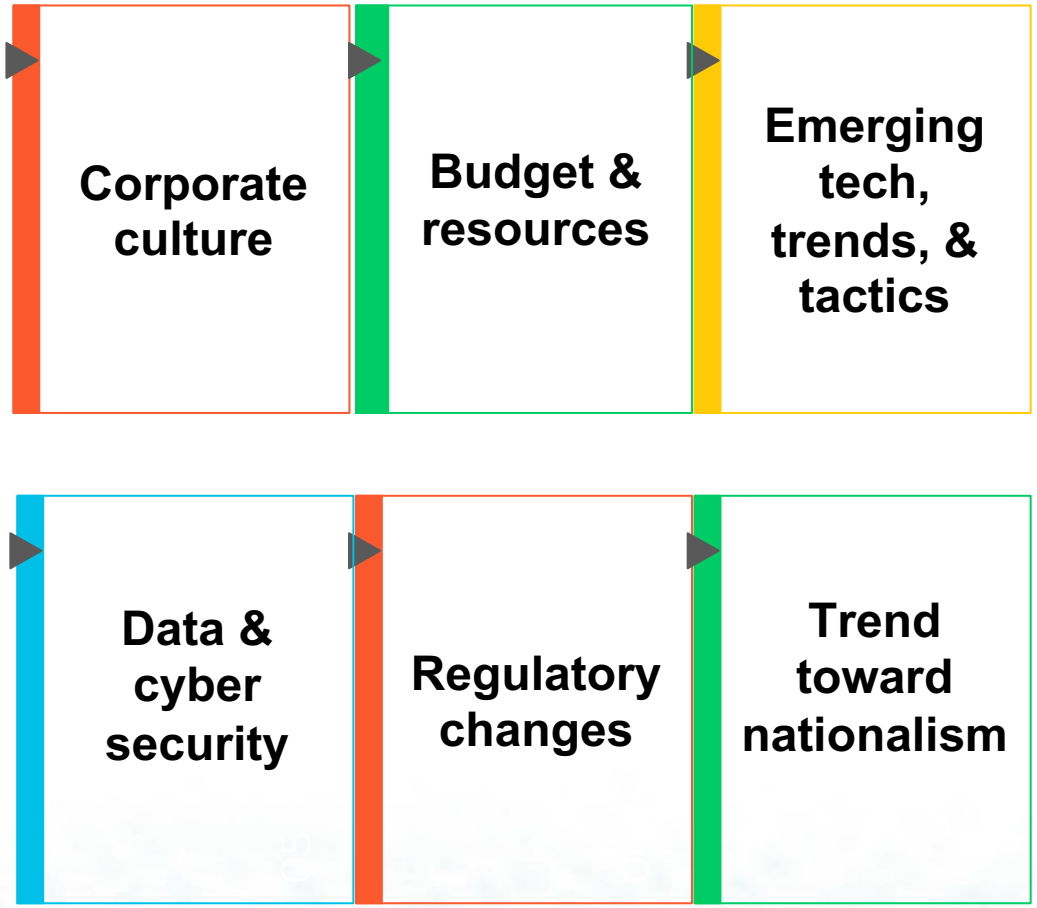
PCI Security Standards Council®

Challenges to Cloud Security Compliance

Challenges to Achieving and Maintaining Cloud Security Compliance

Palo Alto Networks, like any other company, is not immune to the challenges of cloud security. Developing secure practices and aligning to an industry-recognized framework, while necessary, is a challenging task and is not a one-time effort. It requires major shifts in the way organizations and personnel operate and often times is faced with obstacles.

Teams have to stay knowledgeable and flexible in order to ensure cloud security compliance is maintained throughout the year and quickly respond to change so that products and services remain compliant to new and existing requirements.



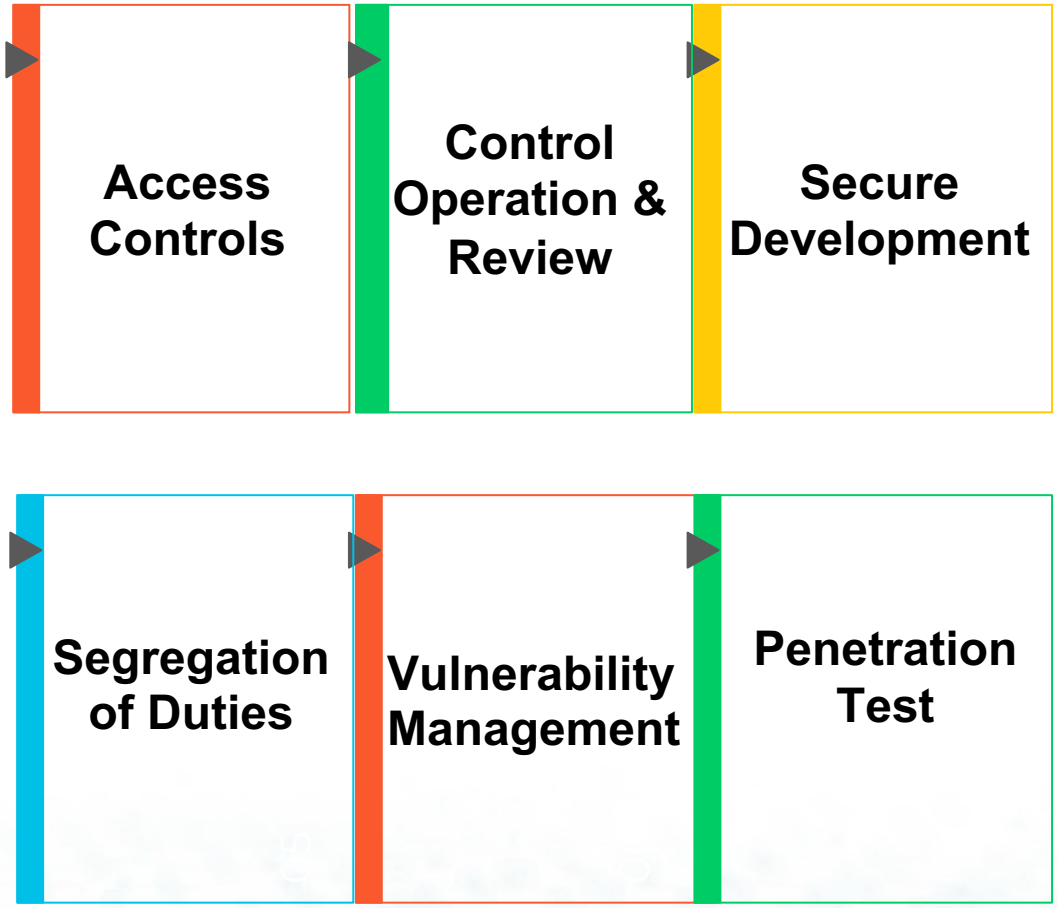
PCI Security Standards Council

Operational Controls - Year Round Audit Activities

Achieve and Maintain Compliance Compliance

Cloud security compliance is established through the implementation and maintenance of required documentation, procedures, and controls for the defined product/service scope.

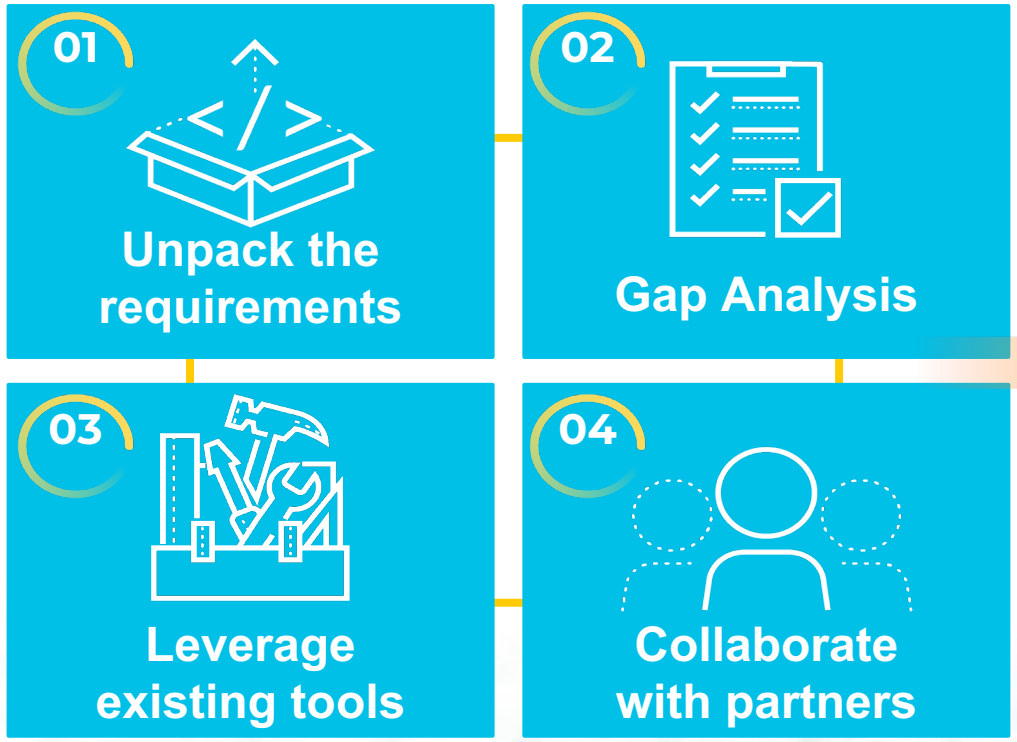
It is necessary to maintain cloud security compliance throughout the year to ensure the product/service remains aligned to the criteria and passes an annual external audit. **Successful annual attestations are dependent on yearly operations and a successful annual audit.**



PCI Security Standards Council

Responding to Cloud Security Compliance Demand

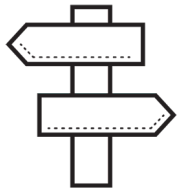
Palo Alto Networks' Process for Responding to Cloud Security Compliance Demand



PCI Security Standards Council

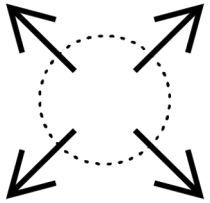
Relationship & Engagement Management are Key

Understand the Requirements



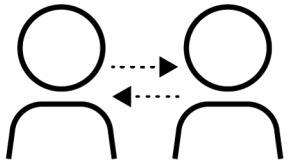
Build the relationship with your internal & external stakeholders to stay ahead of requirements.

Plan for Engagement



Work with stakeholders to plan for a response to the change.

Communicate



Communicate early & often.

Relationships of the Cloud Security Certification Engagement

PCI Security Standards Council

Partners of the Cloud Security Compliance Engagement

Working Partners & Dynamics

1. Ownership of Palo Alto Networks SOC 2 controls are split amongst three main groups: Product Team (37%); Information Security (32%);Supporting Orgs (31%)

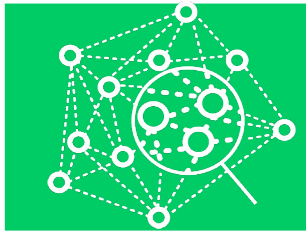
2. Palo Alto Networks maintains a collaborative engagement w/BDO throughout the year, working across various Palo Alto Networks products and certification/attestation efforts.

PCI Security Standards Council

Optimized Approach to Cloud Security Compliance

PCI Security Standards Council®

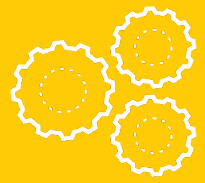
Palo Alto Networks Optimized Approach to Security Compliance



1 ›

Consolidated Control Framework

Consolidated control framework that maps several compliance frameworks to the Information Security Policy & Standards.



2 ›

Common Control Testing

Evidence gathering has been streamlined through identification of corporate controls that are tested at regular intervals.

3 ›

Optimized Engagement Approach

Each engagement with a stakeholder or resource is optimized and leveraged across efforts for time and effort savings.

395	# of controls within the CCF
100%	SOC 2 controls map to InfoSec Policy & Standards
10+	Compliance frameworks mapped in the CCF

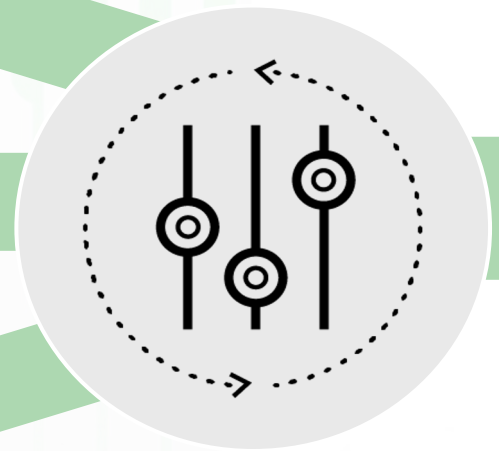
50%	SOC 2 controls are “Common Controls”
x15	Reduction in testing frequency
900	Hours saved

7	Orgs participate in SOC 2 audits
6-8	Meetings w/Product Teams to complete a SOC 2 audit
10	Average # of weeks to complete a SOC 2 audit

PCI Security Standards Council®

Automation Pursuits & Strategy

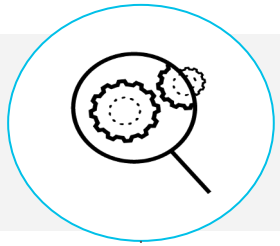
- Tools & Technology
- Process Optimization
- Program Optimization



- Time & cost savings
- Efficiency & accuracy
- Standardization
- Increased productivity
- Customer satisfaction
- Scalable processes

PCI Security Standards Council

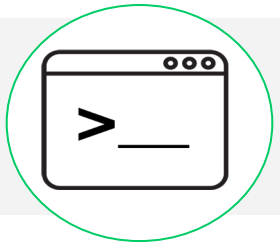
Tools & Technologies



Vendor Tools

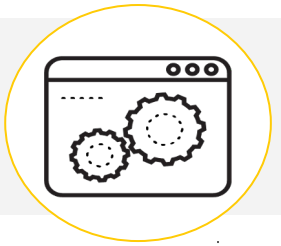
- Investigated six (6) “automation” compliance products.
- **Negligible time savings & benefits relative to cost and implementation time**
- **Inability of tools to scale across multiple compliance frameworks**

External Tech



Scripts & APIs

- Investigating options for leveraging scripts and APIs to automate evidence gathering from systems
- Access issues limit ability of Cert Team to cut the middleman - Product Team and/or IT teams would still be needed



Internal Tools

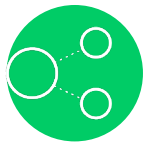
- Prisma Cloud and XSOAR
- Tools not yet used in a manner that would allow for audit automations (detective but not preventive controls)
- Incompatibility issues: ability to streamline, direct access, and/or support from teams to build out data pull, logic, & reports

Internal Tech

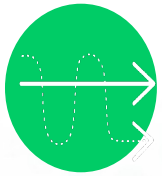
PCI Security Standards Council

Process Optimizations

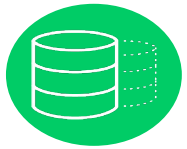
Consolidated Audit Engagement
Combining multiple certifications into a singular audit engagement results in a ***savings of 5,262 Cert Team audit hrs in 2024, resulting in efficiencies of 55%*** *across SOC 2, C5, & IRAP.*



Common Control Testing
Exponential time savings has been realized via Common Control (CC) testing.



Streamlined & Systematic Operations
The start-to-finish operations of the SOC 2 audit have been systematically streamlined to allow for ***completion in 2-3 months, ⅓ the average length of a SOC 2 audit****.*



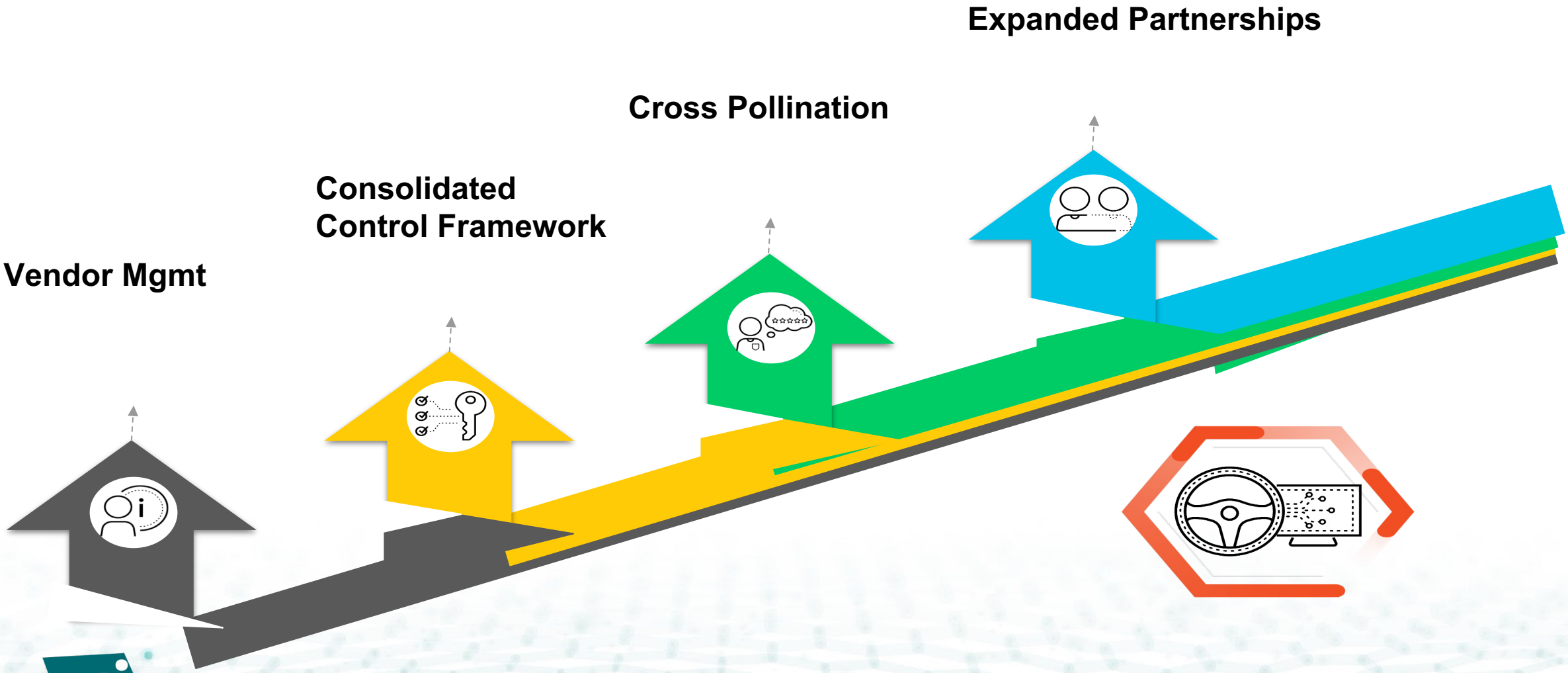
Evidence Optimizations
Audit evidence has been optimized through an audit- and vendor-agnostic internal repository, historical data dumps, and automations through on-demand access to evidence.

Compliance Checklist
"Compliance Checklist" for Product Teams, ***consolidating the readiness assessment for recertifications portion of an audit into a 1 hour workshop.***

Proactive Program Management
Essential assets such as *resource and planning materials* and audit communications have been automated to allow for efficient and repeatable execution, **eliminating guesswork and reducing errors and inconsistencies**.

PCI Security Standards Council®

Program Optimizations



PCI Security Standards Council

2024 Certification Result

- **6,326 cert team hours saved** through combining SOC 2, C5 & IRAP
- **23% decrease** in individual or “unique” engagements
- **29% increased savings** of testing hours via CC optimization
  (3,235 hrs saved)
- **18% increase** in number of certifications pursued
- **40% increase** in three audit programs: *ISMAP, IRAP, C5*

PCI Security Standards Council


PCi
Security
Standards Council
®