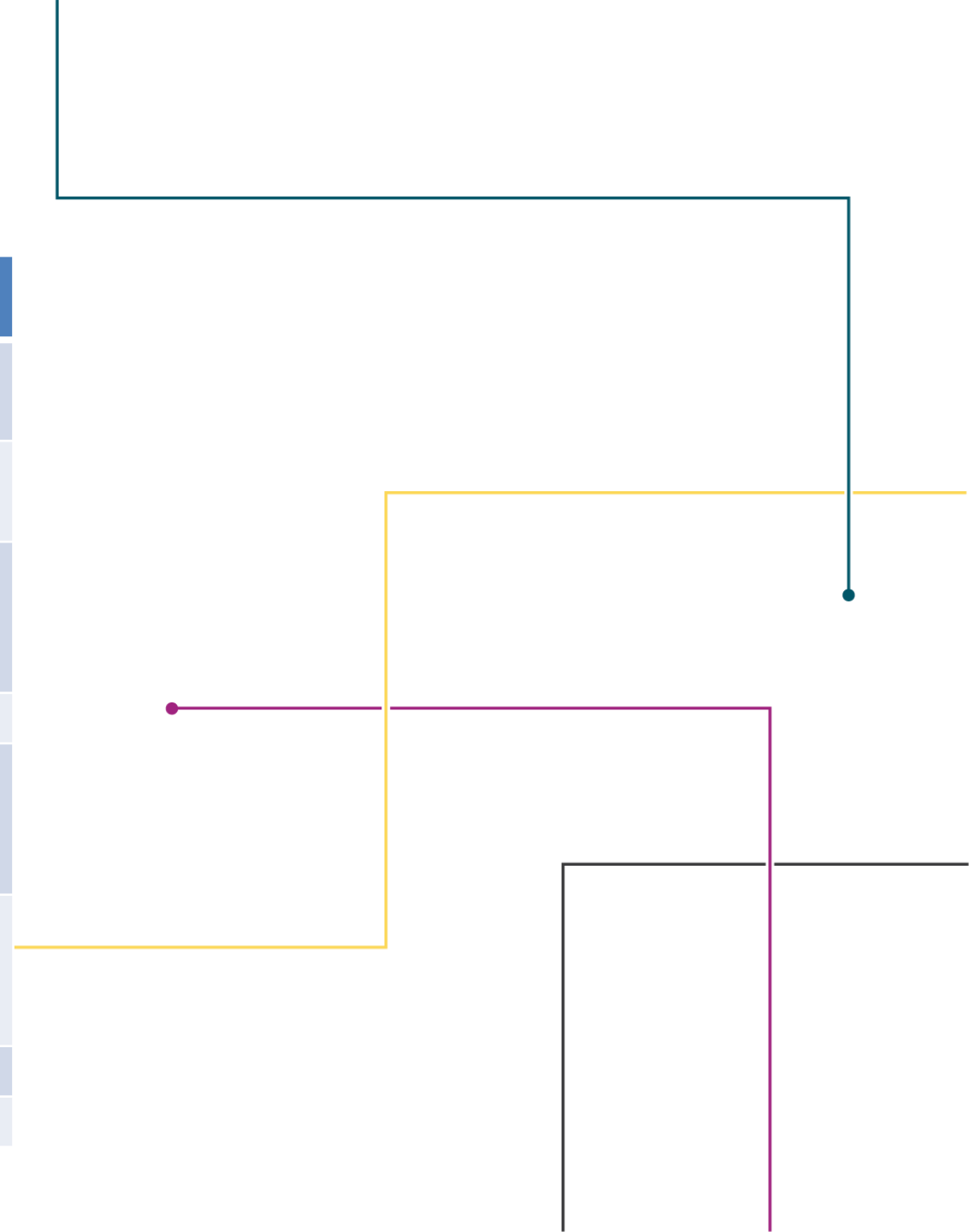




WELCOME TO THE MARCH 1, 2023 ISOAG MEETING



AGENDA	
Welcome/Opening Remarks	Tina Gaines/ VITA
Introduction to New Governance Director	Trey Stevens/VITA
Preparing for Post Quantum Cryptography	Andrew Sheedy & Dan McGinnis/Entrust
Knowbe4 Update	Tina Gaines/VITA
Knowbe4 Training Overview	Ruxandra Teodorescu/VDACS
Datapoints Review & Checklist	Erica Bland, Tina Gaines & Renea Dickerson/VITA
Upcoming Events	Tina Gaines/VITA
Adjourn	



PREPARING FOR POSTQUANTUM CRYPTOGRAPHY

Presenter: Andrew Sheedy

February 2023



ENTRUST

SECURING A WORLD IN MOTION

AGENDA

- › Introductions
- › Entrust Company Profile
- › Post Quantum Readiness
 - Post Quantum Landscape
 - Crypto Agility
 - Cryptographic Center of Excellence
 - Recommended Best Practices
- › Questions



ENTRUST

\$850M+
in revenue

2,800+
colleagues

50+
years of innovation

1,000+
partners

44
global offices



ENTRUST

1187

5B

Financial and
government cards
issued yearly with
Entrust issuance
systems

10B

ID cards activated for
students, employees,
and citizens

202

countries/nationalities
which have had their
citizen identities verified

24M+

SWIFT messages
encrypted and
secured daily

20B

payment cards
issued

690K

websites secured
globally

100M+

protected workforce
and consumer identities



ENTRUST

SAFE WITH US

25 yrs

refining methodologies to mitigate design, implementation and governance risk in cryptography

>\$100M

Annual spend on R&D

100's

Certifications and alignment to compliance standards

40+

Countries and global agencies use Passport & National ID solutions

95%

of IT professionals say Entrust is highly respected

82%

surveyed call us "best in class" for our 24/7 customer support

57%

Global Fortune 100 use our data protection



ENTRUST

PEOPLE, PROCESS, TECHNOLOGY

Digital transformation accelerated by efficiently securing identity, transactions and data



STRONG IDENTITIES

Verification, control and fraud prevention at low friction for people and machines



SECURE PAYMENTS

Digitally onboard, issue and manage both physical and digital payment vehicles

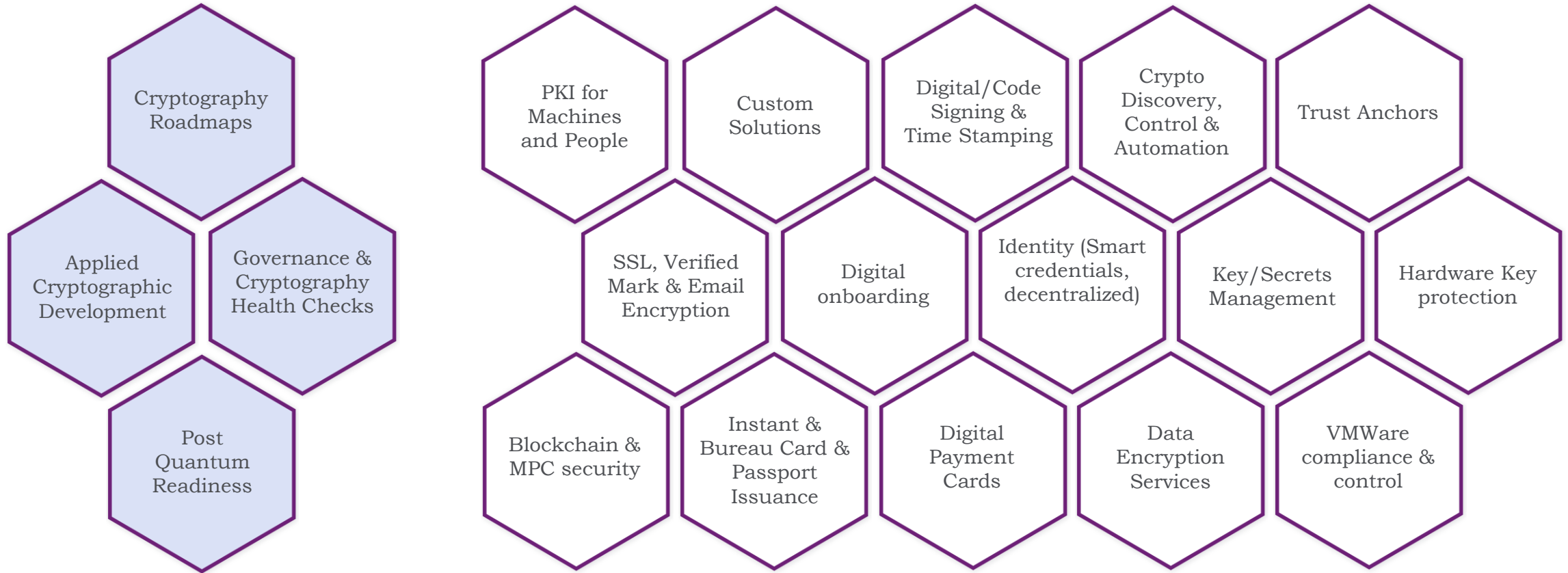


TRUSTED INFRASTRUCTURE

Assured, agile and Post Quantum ready infrastructure across enterprise and cloud



PEOPLE, PROCESS, TECHNOLOGY



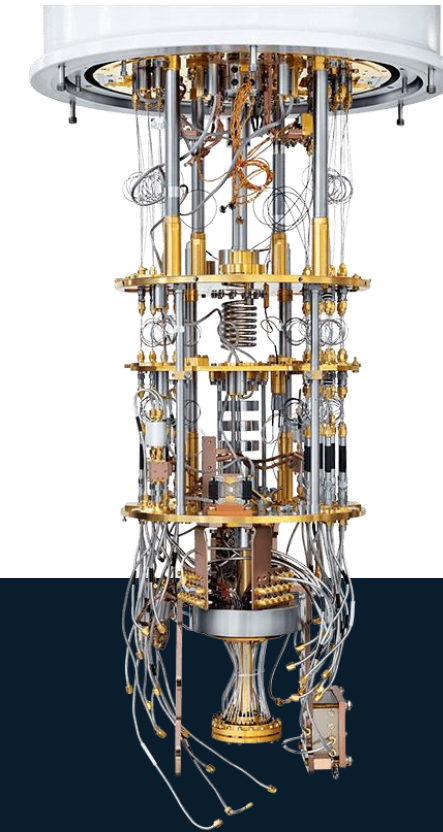
PQ PREPAREDNESS



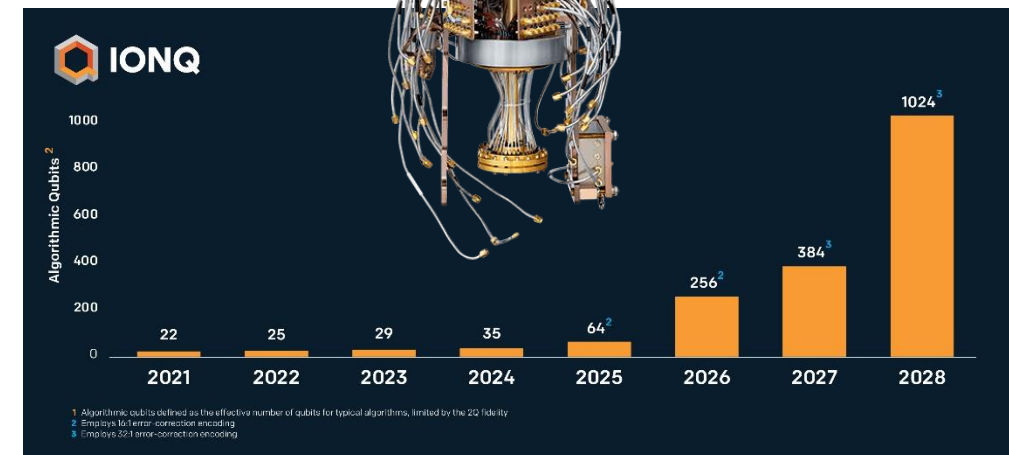
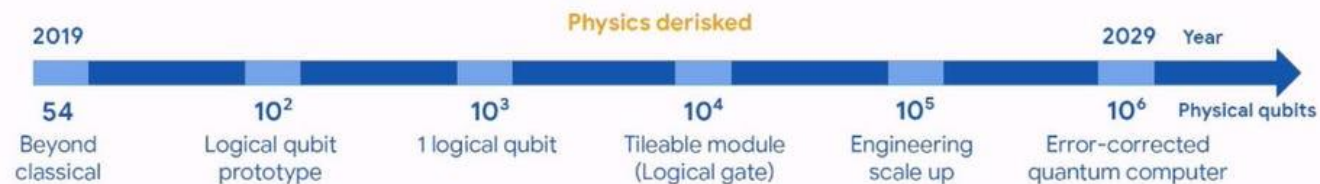
ENTRUST

SCALED QUANTUM COMPUTERS ARE ON THE HORIZON

Rigetti Aspen-11

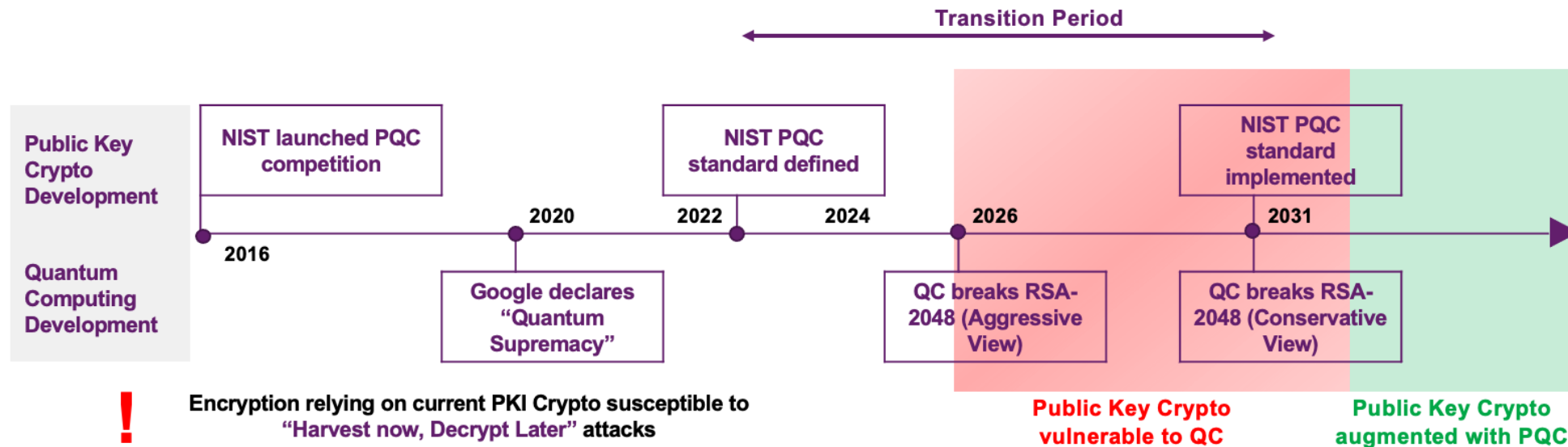


Google AI Quantum hardware roadmap

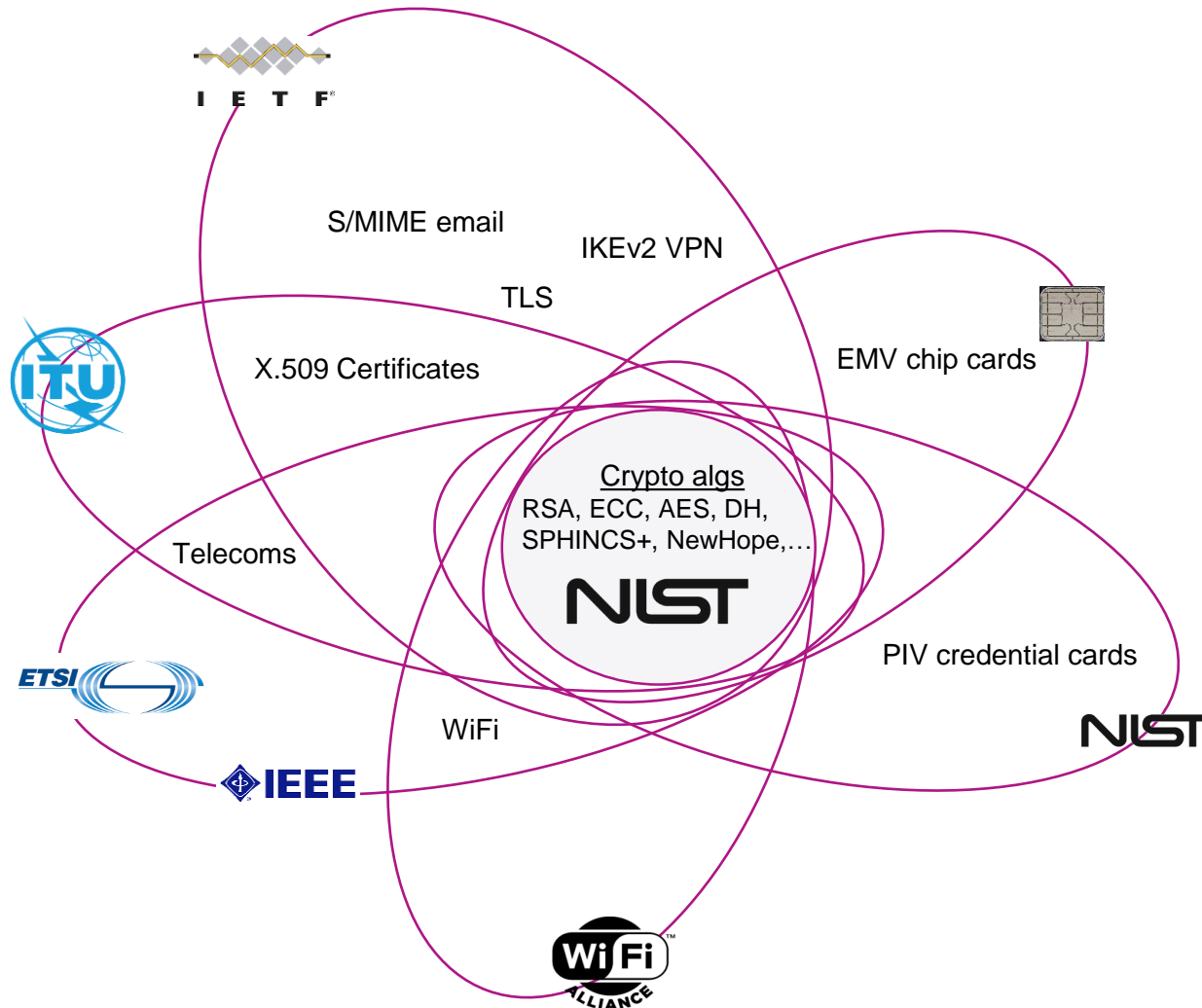


QUANTUM THREAT AND EXPECTED TIMELINE

- › Quantum computers will be able to break current public key encryption
- › Accurate crypto inventory & mitigation strategies are required
- › Long term data needs to be protected not then, but now
- › Failure to migrate leaves applications and data at risk of compromise.



FRAGMENTED COMMUNITY



NEWS

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

July 05, 2022

- Standards bodies to adopt algorithms and update protocols/documentation
- PQC “ready” chips available around 2024-2025
- Certification audit/testing then follows so c.2025-2026 for release of assured products

NEW CRYPTOGRAPHIC STANDARDS RELEASED WITH TIMELINES (SEPTEMBER 2022)



Public-key

CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key

Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates

Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)



ENTRUST

NATIONAL SECURITY AGENCY – TIMELINES

- › **Software and firmware signing:** begin transitioning immediately, support and prefer CNSA 2.0 by 2025, and exclusively use CNSA 2.0 by 2030.
- › **Web browsers/servers and cloud services:** support and prefer CNSA 2.0 by 2025, and exclusively use CNSA 2.0 by 2033.
- › **Traditional networking equipment** (e.g., virtual private networks, routers): support and prefer CNSA 2.0 by 2026, and exclusively use CNSA 2.0 by 2030.
- › **Operating systems:** support and prefer CNSA 2.0 by 2027, and exclusively use CNSA 2.0 by 2033.
- › **Niche equipment** (e.g., constrained devices, large public-key infrastructure systems): support and prefer CNSA 2.0 by 2030, and exclusively use CNSA 2.0 by 2033.
- › **Custom applications and legacy equipment:** update or replace by 2033.





OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

- Is the system a high value asset based on organizational requirements?
- What is the system protecting (e.g. key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
- What other systems does the system communicate with?
- To what extent does the system share information with federal entities?
- To what extent does the system share information with other entities outside of your organization?
- Does the system support a critical infrastructure sector?
- How long does the data need to be protected?

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.



2021-2023

Inventory and prioritize systems



2024

NIST post-quantum cryptography standard published



2024-2030

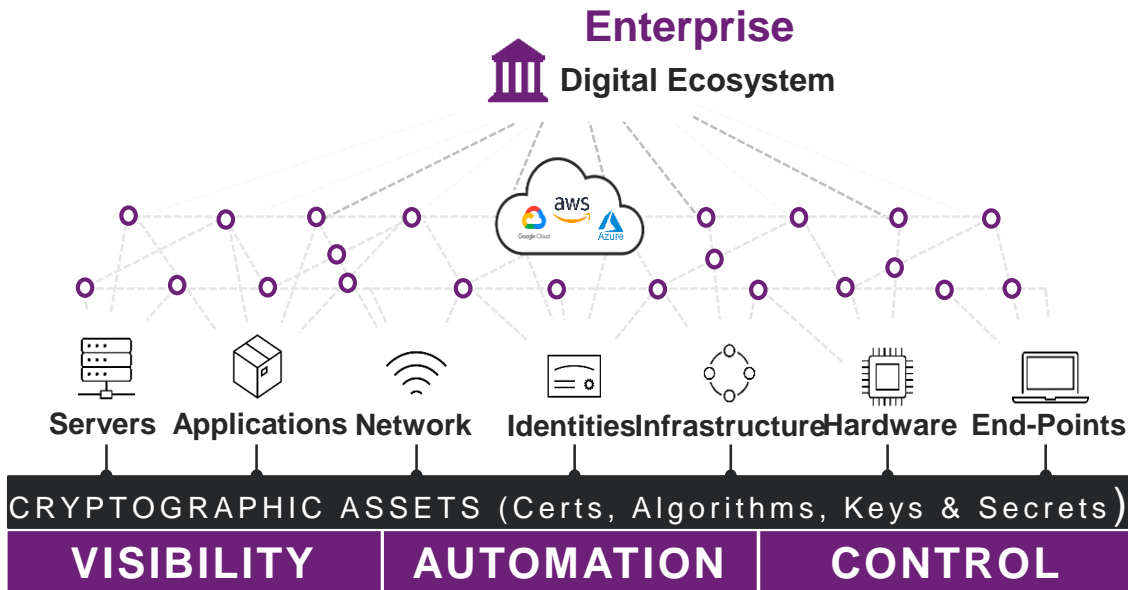
Transition of systems to NIST post-quantum cryptography standard



2030

Cryptographically relevant quantum computer potentially available

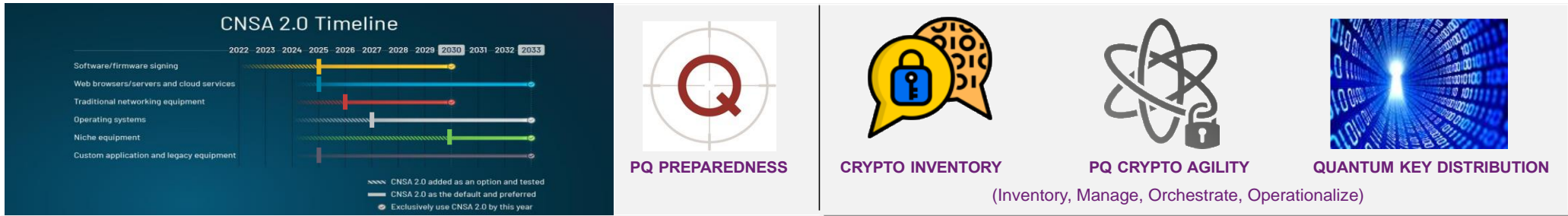
MANAGEMENT OF CRYPTOGRAPHIC ASSETS



Problem Statements:

- PKI and crypto **ARE** critical infrastructure and **expanding**
- It is a **false assumption** that systems are “forever” secured with PKI/crypto
- **Risks can be unknown** because elements are not visible/managed
- Crypto resources **are scarce and expensive**
- Best practices are **often inconvenient**
- Procedures, Policies and platforms are **not always robust or maintained**
- Many organizations **find out too late**

POST QUANTUM PREPAREDNESS



Time to set up your PQ team to build your strategy

PQ Readiness needs accurate inventories, crypto agility and new technology

Meanwhile, crypto continues to proliferate in the landscape



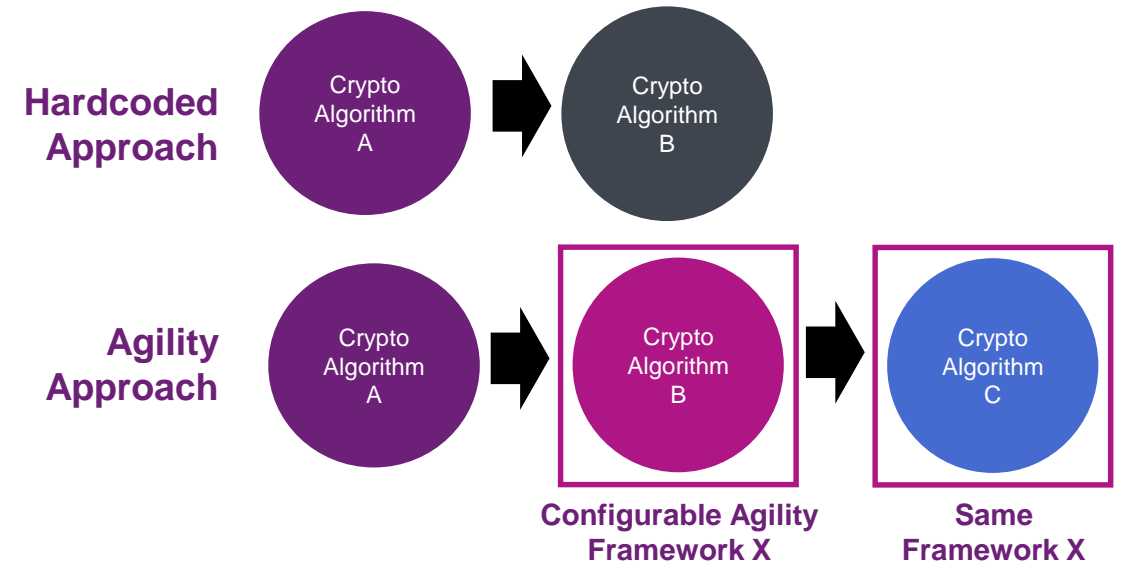
CRYPTO AGILITY AND HYBRID

The image features a large, abstract geometric composition. A large, dark purple shape occupies the upper left and center, with a sharp diagonal cutout. Below it, a magenta hexagon is partially visible, overlapping with a darker purple rectangular shape. The background is white on the right side.

WHAT IS CRYPTO AGILITY?

DEFINED:

The ability to reconfigure an application or system with a different cryptographic algorithm (or implementation).



THE CHALLENGE OF TRANSITION

Legacy Applications

- › Cryptography baked into the application
- › Multiple cryptographic dependencies
- › Requires software rewrite
- › Needs decomposition / modernization

Modern Applications

- › Cryptography baked into the platform
- › Inter-service communication often unsecured
- › New zero trust requirements
- › Complex management capabilities

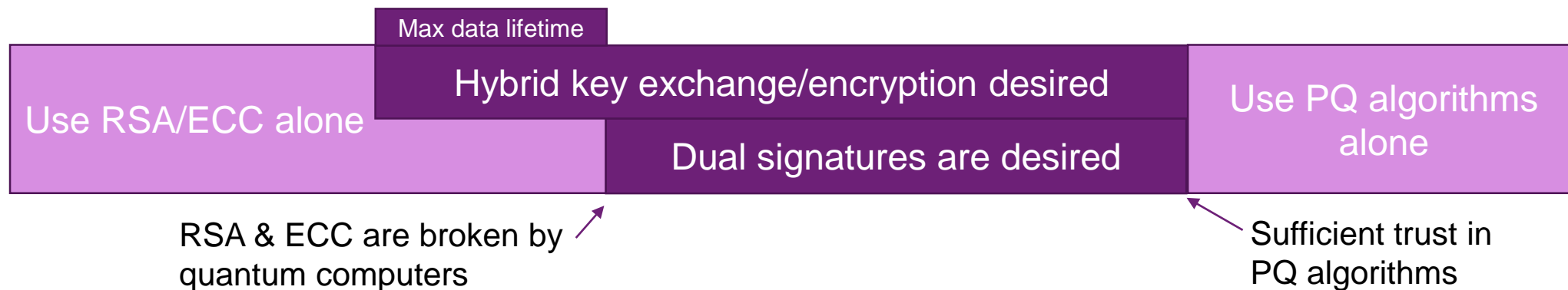
BSI CALL FOR “HYBRID”



“A dual signature consists of two (or more) signatures on a common message. It may also be known as a hybrid signature or composite signature.”

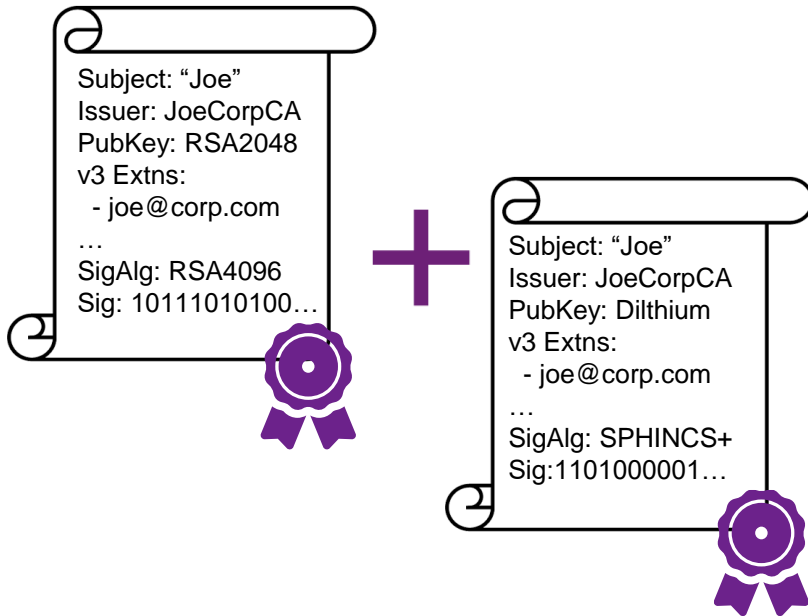
Solutions are FIPS-compliant as long as one component is FIPS-compliant;
Ex {RSA + Dilithium}

- Hybrid modes provide protection until we have confidence in PQC:
 - Time between publication of NIST standards and full confidence.
 - Time between publication of new attack and patching.



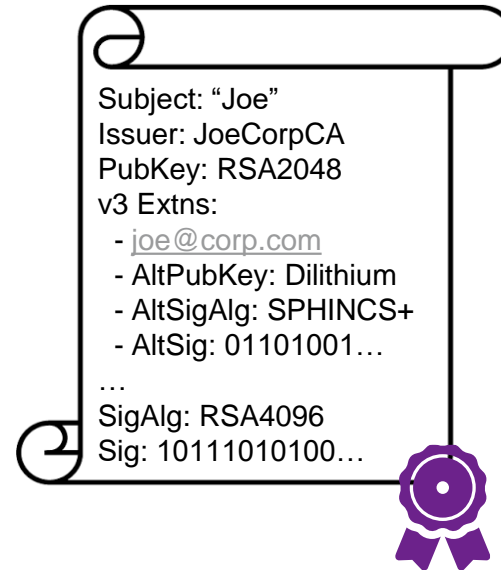
PRE-QUANTUM APPROACHES FOR POST QUANTUM

MULTI-CERT



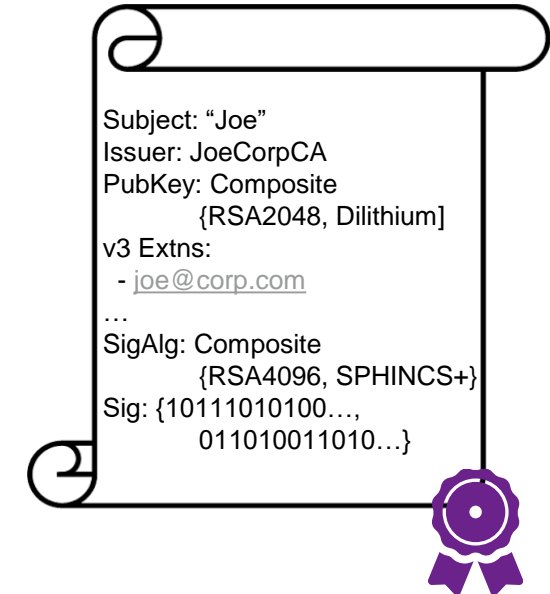
"HYBRID" CATALYST™ 1

IETF: draft-truskovsky-lamps-pq-hybrid-x509



COMPOSITE 2

IETF: draft-ounsworth-pq-composite-sigs



Entrust is working on standardizing this!

¹ ISARA - Entrust - Cisco collaboration; IETF and ISO drafts

² Entrust – CableLabs – Cisco collaboration; IETF draft

CRYPTOGRAPHIC CENTER OF EXCELLENCE



CRYPTOGRAPHIC CENTER OF EXCELLENCE

Cryptographic Center of Excellence

EXPERT-BY-YOUR-SIDE

VISIBILITY

BEST PRACTICES

PKI GOVERNANCE
CONSULTING

DESIGN &
IMPLEMENTATION

PKI HEALTH CHECK
& PKI DISCOVERY



CRYPTO GOVERNANCE
CONSULTING

CRYPTO HEALTH CHECK

PQ MATURITY
ASSESSMENT

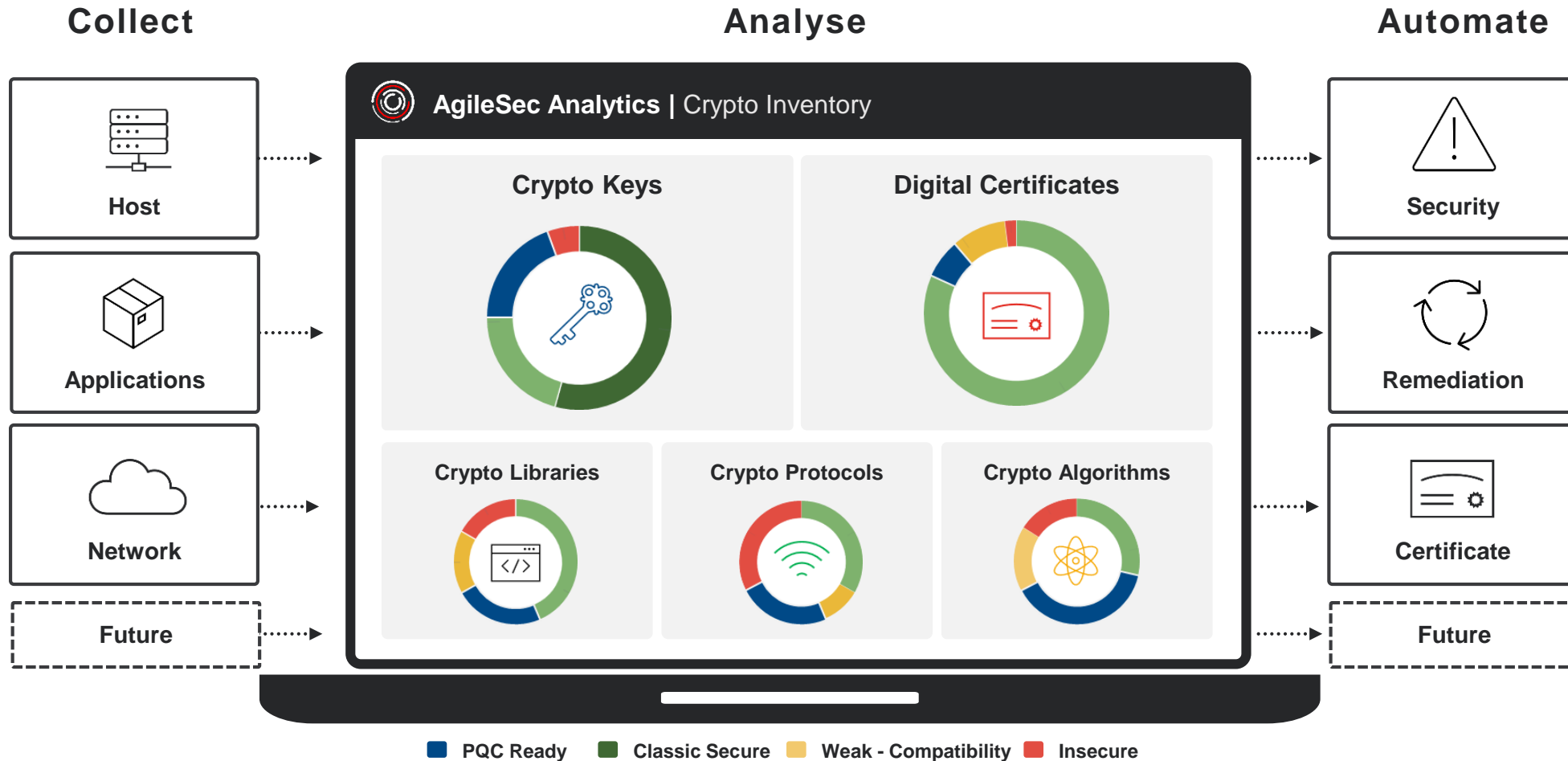
PKI

CRYPTO



ENTRUST

CRYPTO INVENTORY | AUTOMATION

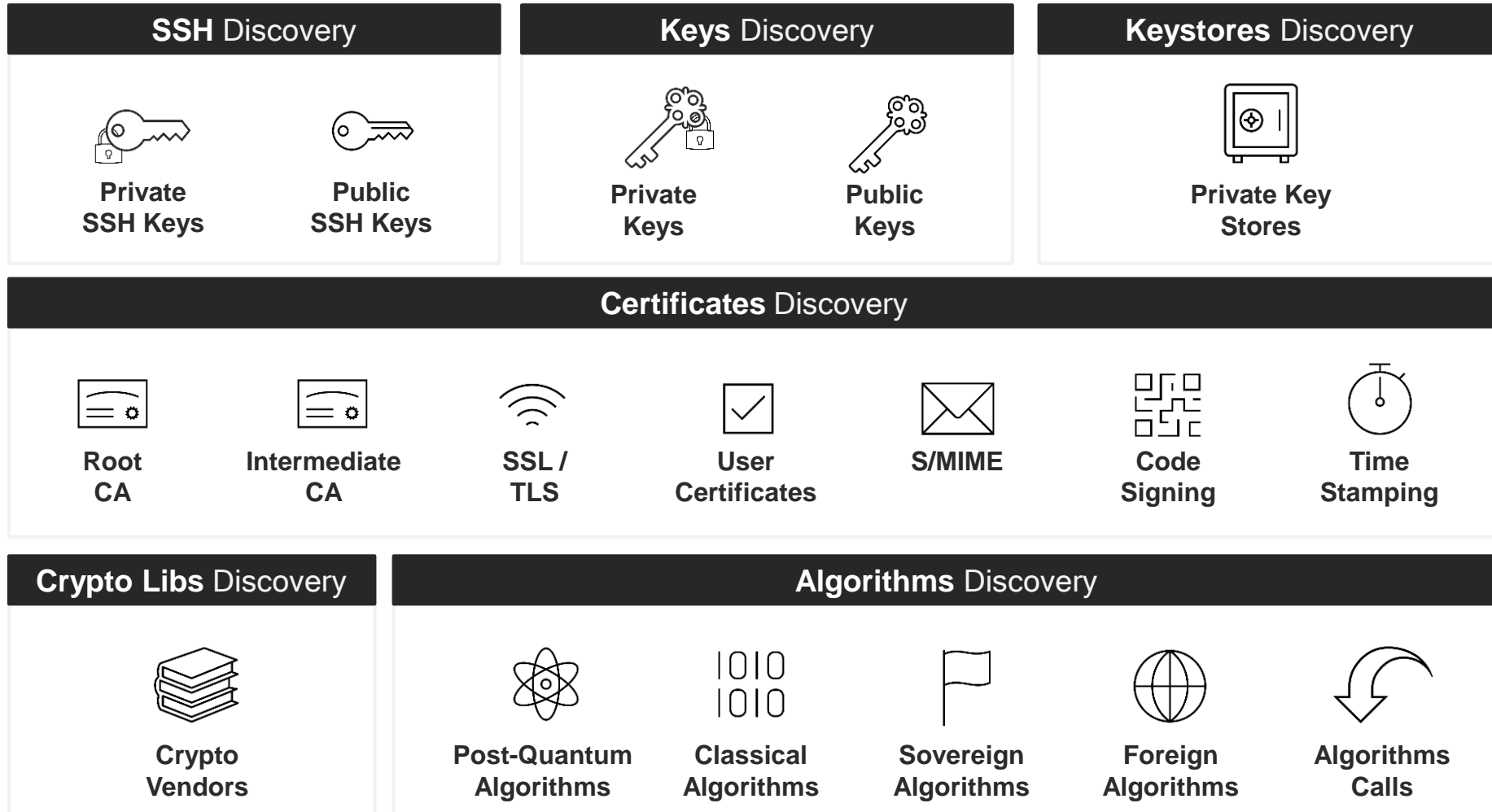


Integrations

Windows	RedHat
Linux	Ansible
Artifactory	ServiceNow*
CrowdStrike*	Tanium
Venafi	CertHub*
Sentinel	Others

* In process

CRYPTO INVENTORY | COLLECTED OBJECTS



Custom Cryptographic Objects

CRYPTO INVENTORY | USE-CASES



Prevent
Secret Key Leakage

KEY & SECRETS

Detect secrets keys leaked into systems or applications before they are exploited.



Prevent
System Downtime

X509 CERTIFICATES

Detect certificates hidden into systems or applications before they expire.



Detect
Shadow Certificates

X509 CERTIFICATES

Detect Machine Identities generated outside of corporate process as soon as they appear.



Automate Crypto
Compliance

CRYPTO INVENTORY

Verify compliance with Cryptographic standards, including NIST or internals.



Find Crypto
Critical Vulnerabilities

CRYPTO INVENTORY

Detect exploitable cryptographic vulnerabilities within infrastructure and systems.

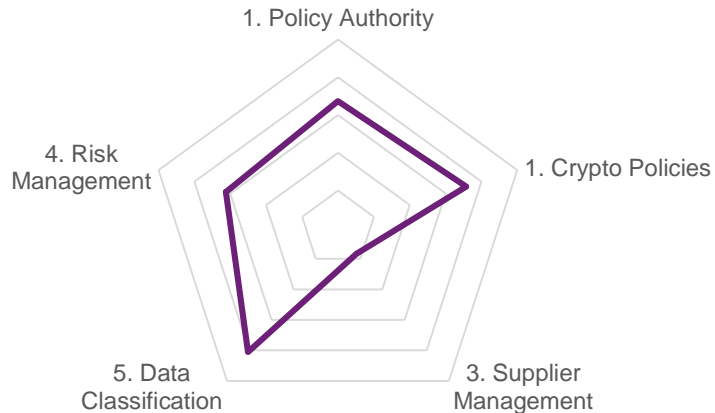


Prepare for
Quantum Threat

CRYPTO INVENTORY

Plan transition to post-quantum cryptography by inventorying cryptographic objects.

POST QUANTUM MATURITY ASSESSMENT



- › Maturity level assessed across:
 - Process, People & Technology
- › Recommendations documented
- › Roadmap mutually agreed and tracked

Unknown

- **Highly reactive**
- Lack of ownership
- No centralized policy
- No inventory of assets
- Silo and segmented organization
- **No roadmap**

Awareness

- **Reactive**
- Decentralized crypto; ad hoc tools
- Evaluates regulations and understands **crypto landscape**
- Risk mitigation plan in place, but **lacks planning** and visibility of critical issues

Management

- **Moderately proactive**
- Policy established
- Crypto policy and staffing in place
- Exposed to vulnerabilities
- **InfoSec oversight**
- Backlog of issues and improvements
- **Short-term vision**

Optimization

- **Proactive**
- Central policy widely enforced
- Crypto management and discovery tools
- Cross functional team
- Modern, cloud-based technologies
- Lacks dedicated resources; competing priorities
- **3-year crypto roadmap**

Excellence

- **Highly proactive**
- Centralized crypto centre established
- Full set of tools and best practices in place
- Board support
- Fast response to fix vulnerabilities and comply with new standards with **Crypto Agility**
- Manage investments in timely matter
- Monitors emerging threats
- **5-year crypto roadmap**

POST-QUANTUM READINESS

Timing Guidance to be prepared	Inventory 2022-2024 Build cryptographic inventory, policies, transition (BSI Hybrid?) plan, and start crypto-agile development strategy	Governance 2024-2027 Implement transition plan, crypto policies, and crypto-agile application development, and purge weak crypto	Operationalize 2027-2028 End of life non-Agile applications, enforce strong crypto policies for data, test and vet new PQ algorithms, transition to COE
PQ Readiness Solutions	Inventory & Control – Infosec Global AgileSec & Entrust Cert Hub		
	PQ Maturity Assessment, Health Checks & Discovery		
	Early Adopter: PKI and Cryptographic solutions	PQC Hybrid enabled Entrust solutions	

THE STEPS TO QUANTUM SAFETY

Step 1:

Become excellent at
Crypto Agility

Step 2:

Inventory your
crypto assets &
map to the data

Step 3:

Figure out your
timeline to transition

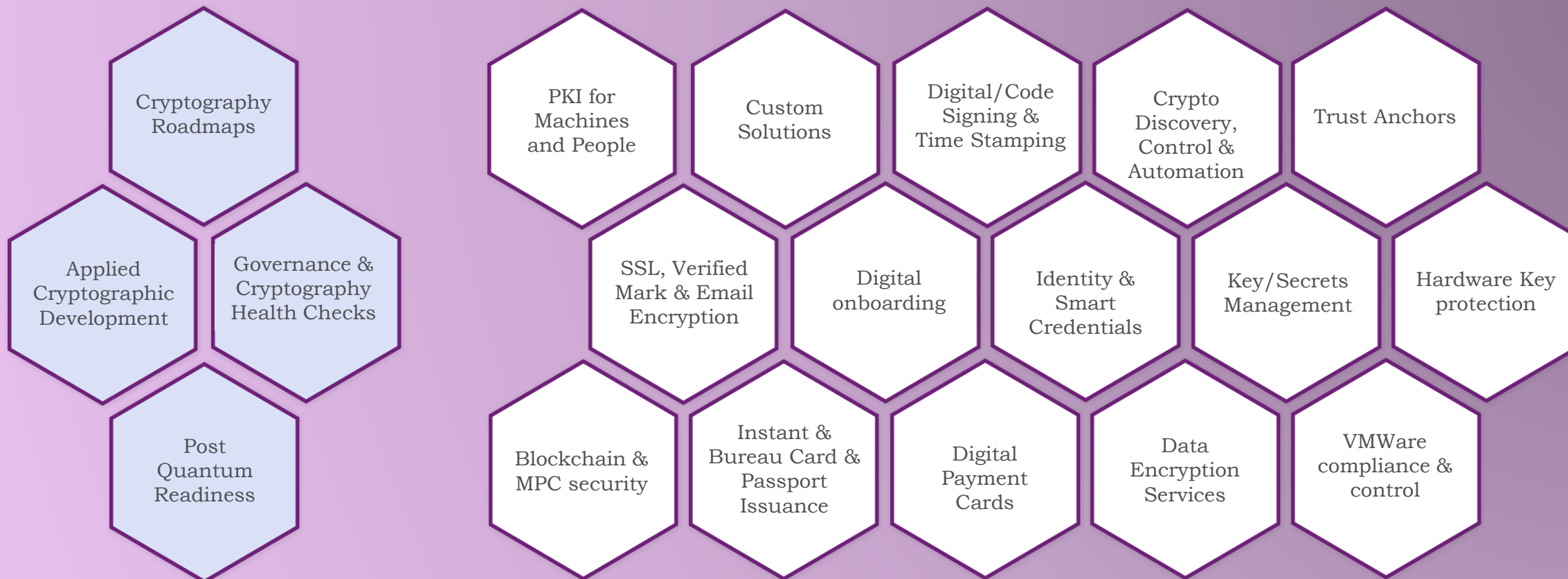
Step 4:

Plan the migration



ENTRUST

PEOPLE, PROCESS, TECHNOLOGY



THANK YOU

Visit [entrust.com](https://www.entrust.com)



ENTRUST

SECURING A WORLD IN MOTION

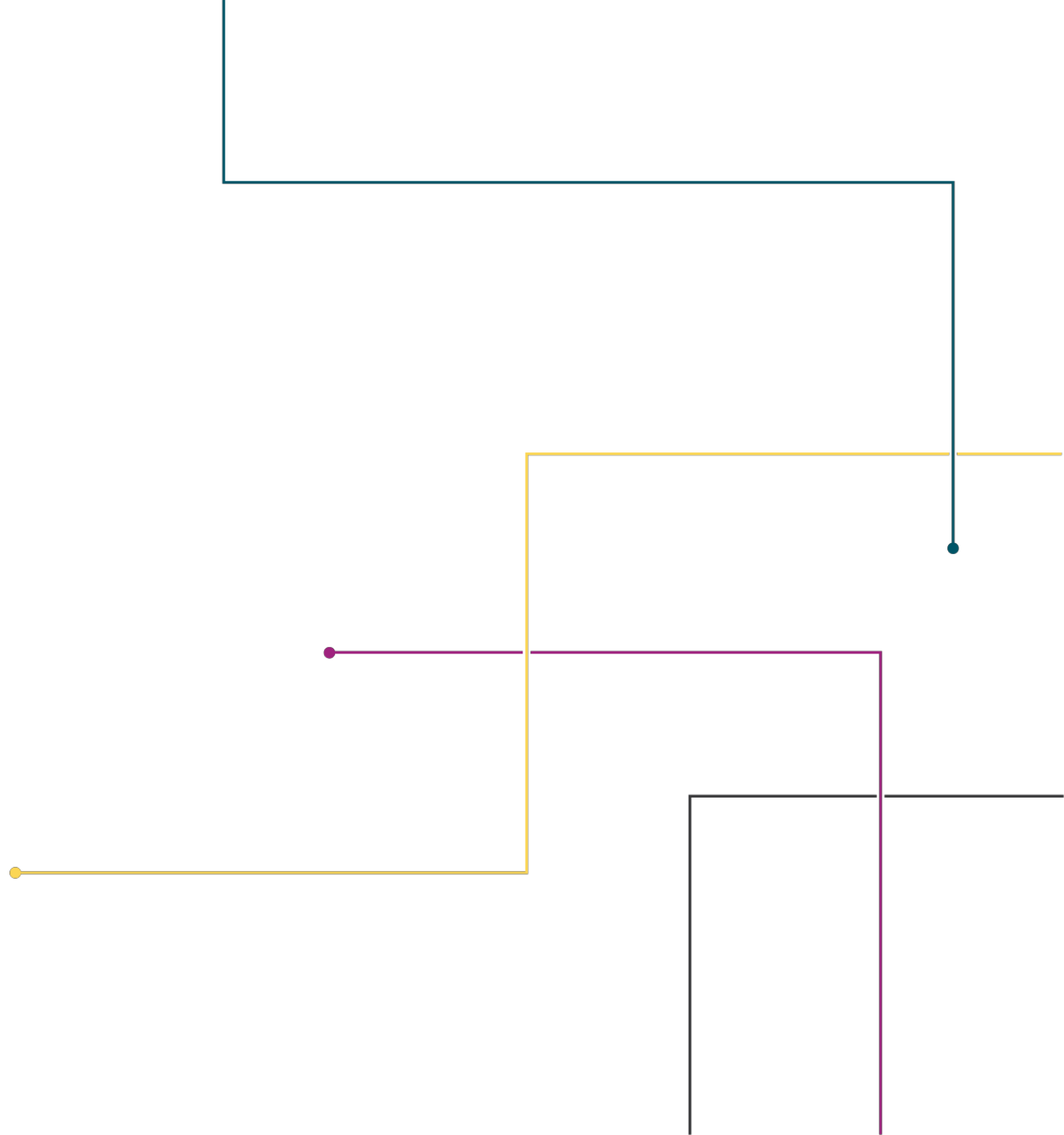


KNOWBE4 UPDATE

Tina Gaines

Security Awareness Training
Manager

CSRM





What's the





- Twenty three agencies that use KnowBe4 were moved under the VITA tenant with minimum issues the week of Jan. 30. In addition, three agencies that used other security awareness training solutions were moved and given access to their KnowBe4 console.
- What was requested from agencies during phase one:
 - Current training solution and contract expiration date.
 - Number of employees to include FTEs, wage and contractors.
 - Name and email address of agency designated administrator(s).



- What VITA received the week of Feb. 20:
 - Current training solution and contract expiration date.
 - Number of employees to include FTEs, wage and contractors.
 - Name and email address of agency designated administrator(s).

- What VITA is working on:
 - Compiling the data we received from survey monkey into a spreadsheet as a centralized repository.
 - Working with KnowBe4 on agencies whose subscriptions are close to expiration so that there will not be a gap in console access for those agencies that are currently using the platform.
 - Preparing to grant KnowBe4 console access to those agencies who subscriptions are close to expiration and are using another training solution other than KnowBe4 starting the week of **March 6**. Agencies involved will be notified in advance.

 - Knowbe4 Training: VITA will begin scheduling training sessions with console admins in **April**.

- Phase One – Those agencies who are currently subscribed to Knowbe4. This phase will take place the week of **Jan. 30, 2023**. Phase one included over 20 state and independent agencies, two higher ed agencies, the Governor’s Office, and two agencies who did not use Knowbe4.
- Phase Two (**Start Date week of March 6**)– Majority of the agencies not included in phase one. This phase is schedule to be completed by **July 2023**.
- Phase Three – This phase will include agencies that might be a little more complex, challenging, or their subscription renewals expire later in the year or next year. This phase is scheduled for completion by **December 2023**.

Custom Content:

<https://support.knowbe4.com/hc/en-us/articles/360047284433>

KnowBe4 527 Crosswalk: <https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines>

What type of reporting is available?

<https://support.knowbe4.com/hc/en-us/articles/360007952894>

Will it be OKTA enabled? OKTA configurations:

<https://support.knowbe4.com/hc/en-us/articles/115013176407>

Training Notifications:

<https://support.knowbe4.com/hc/en-us/articles/115010848868>

<https://www.knowbe4.com/en/security-awareness-training-features/>

Here is a link to a recorded version of the webinar so you can get a feel for it.

<https://attendee.gotowebinar.com/recording/6413257131567872515>



QUESTIONS





SECURITY AWARENESS TRAINING



KNOWBE4 AND THE AGENCY SECURITY AWARENESS TRAINING PROGRAM

Ruxandra Teodorescu

ISOAG 3/1/2023

Agenda

- Account Settings
- Campaign Planning
- User Groups
- Campaign Settings
- Campaign Custom Notifications
- Policies Settings
- Training Status and Reports
- Challenges



+



Account Settings

- **Configure Single Sign On**

- Phased rollout

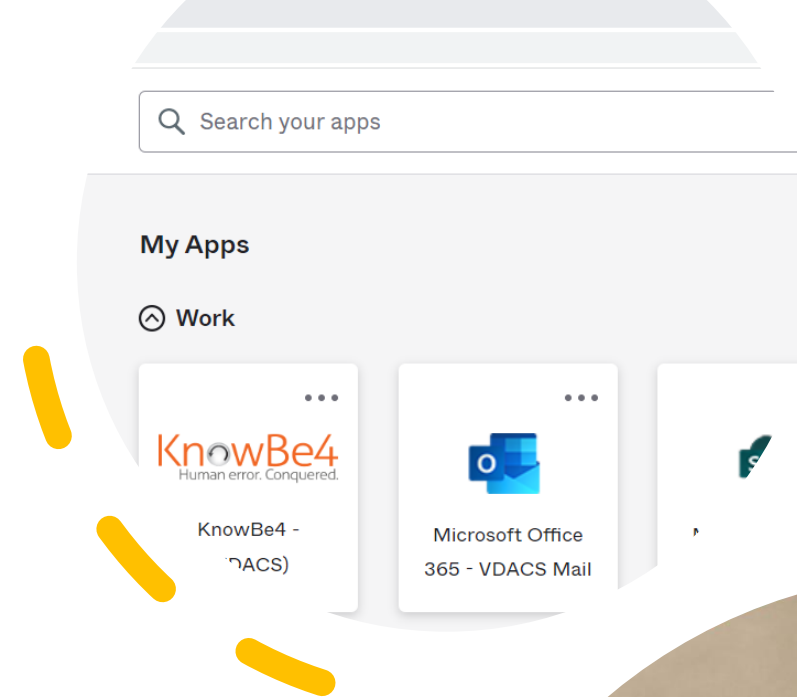
[COV-AUTH Okta Application Integration](#)

- **Branding**

- Add a link to your agency logo – size and format restrictions apply
- Set up a brand color (Hex value)
- Upload your branded certificate - see the KnowBe4 knowledge base [article](#) for image specifications and templates.

- **Learner Experience**

- Enable Learner Dashboard
- Enable Team Dashboard



Certificate of Achievement

Employee Name

Has successfully completed

Example Course Name

February 27, 2023

User Dashboard View

- Learner Experience
 - **Enable Learner Dashboard**
 - Training Progress Bar
 - Assignment Name
 - View Messages
 - **Enable Team Dashboard**
 - Limit User Information Shown: Disabled
 - Select a Team
 - Training Progress Bar
 - Team Details (training overdue, due soon)

VIRGINIA DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Dashboard Training Messages

My Dashboard Team Dashboard

Training Progress

Select a Team
Select a team to view information about their training progress, phishing results, and combined Team Risk Score.

Select a team...

View ↻

Training Progress

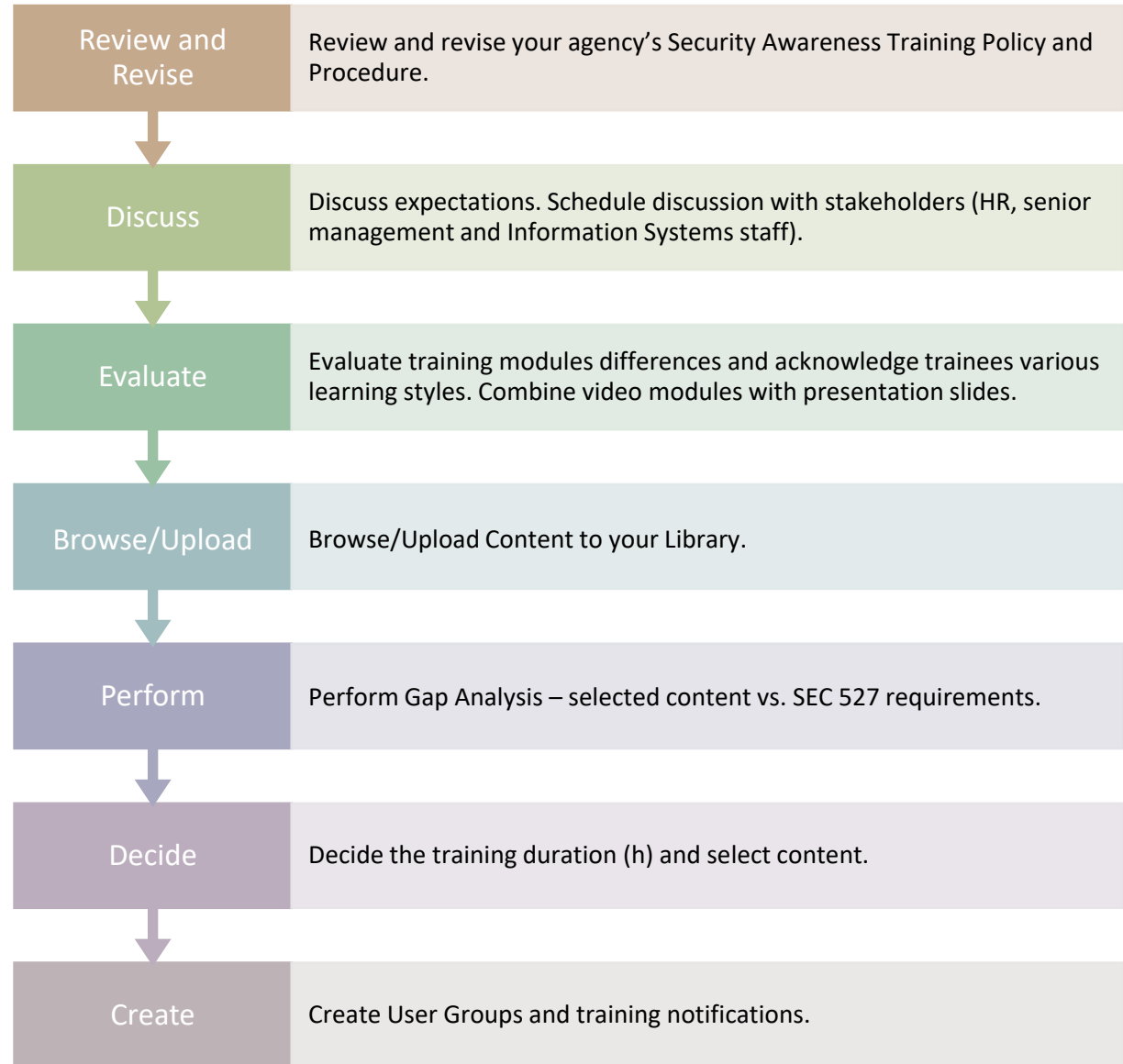
100% The percent of training assignments completed by your team members within the last year

20 / 20

Team Details for the Last Year [Hide All \(3\)](#)

0	0	1
Training Overdue	Training Due Soon	Completed Training
Name	Email	Training Progress
VDACS Test200	vdacs.test200@vdacs.virginia.gov	0% <div style="width: 0%;"></div>
VDACS Test100	vdacs.test100@vdacs.virginia.gov	0% <div style="width: 0%;"></div>
Thomas Mad...	thomas.mad...	100% <div style="width: 100%;"></div>

Training Campaign Planning



Training Content

Option 1: browse Knowbe4 content and add it to Library

- MODSTORE → Browse → Library

Option 2: add personalized content

- MODSTORE → Uploaded Content (SCORM 2004 2nd, 3rd or 4th edition, video files)

Option 3: add documents and presentation slides as PDF files under the Policies section.

- TRAINING → Policies (PDF, URL)

- ✓ Non-Disclosure Agreements (NDAs)
- ✓ Separation of Duties
- ✓ Principle of Least Privilege Training

ModStore

Edit SCORM Language File

Title: VITA Training for System Owners (2022-2023) ?

Description: VITA Training for System Owners (2022-2023) ?

Language: English (United States) ?
The language cannot be changed while
Select the SCORM package to upload for this language. Must be SCORM 2004 2nd, 3rd, or 4th Edition.

SCORM File: Choose File No file chosen ?
Your file must be smaller than 1 GB

Save Cancel

Important: Uploading a new file will reset the progress of all users who are incomplete with this training. This affects all uploaded language files for this content.

Title and description changes will be visible to your users immediately.

User Groups

1. Manage Existent Users

2. CSV Import – predefined groups

- ✓ [Agency] Active Employee List
- ✓ [Agency] New-Hire List
- ✓ [Agency] System Administrators

3. SmartGroups – predefined criteria

- ✓ [Agency] New Employees
- ✓ [Agency] Terminations

The screenshot displays the 'Manage Users' interface. At the top, there is a header with a user icon, the title 'Manage Users', and an 'Add Users' button. Below the header, there are tabs for 'Users', 'Groups', 'Import Users', 'Merge Users', 'Messages', and 'Security Roles'. A 'Selected Users' box shows 3 users, with an 'Archive' button and a 'Select Option' dropdown. An 'Add to Groups' button is also present. Below this, there are filters for 'Status: Active', 'Type: All', and 'Groups: All'. There are also buttons for 'Bulk Archive' and 'Generate CSV', and a search bar labeled 'Search by email or name...'. A table header is visible with columns: 'User', 'PPP', 'Risk', 'Groups', 'Joined on', 'Last Login', and 'Actions'. Below the table, there is a 'Smart Group Criteria' section with a dropdown menu. Two criteria are listed: 'User Date' (User must have been created from 01/01/2023 through 01/31/2024) and 'User Field' (The group name must be equal to VDACS New-Hire List). Both criteria show '17 users' and have edit and delete icons. At the bottom, there are 'Cancel' and 'Save' buttons.

Campaign Settings

- **End Date:**

- Specific Date – used for the annual SAT campaign, needed for email notifications.
- Relative Duration – new hire, other ongoing campaigns, if employees need to access their training certificates.
- No End Date – optional content

- **Allow** assignments to be completed after due date. Use Past Due Notifications.

- **Enable** Content Survey

- **Enable** Track Scores

Create New Training Campaign

Campaign Name

Start Date
(GMT-05:00) Eastern Time (US & Canada)

End Date

Relative Enrollment Duration

Allow assignments to be completed after due date

Content

Content Order

1. 📖 New Hire's Guide to Security Awareness Retired
2. 📺 Keep an Eye on PII
3. 📖 2023 Kevin Mitnick Security Awareness Training - 45 minutes
4. 📖 Taking Security Home: Working Remotely
5. 📖 VDACS 10.1 Ethical Use of Agency Information and Computing Resources
6. 📖 VDACS IS Code of Ethics and Information Security Access Agreement

Enable Content Survey
 Allow users to leave comments

Track Scores

Enroll Groups

Enroll Groups All Users Specific Groups View All Groups

VDACS New-Hire List ✕ ↻

Enable automatic enrollment for new users ?

Enable progress reset for remedial training ?

Add Completed Users To VDACS Active Employee List ✕ ?

Remove Completed Users From Select one or more groups from the list... ?

Notifications + Add Notification

Past Due | Notify: User, Manager, Admin | Send Reminder: 1 day after Resend Reminder: Every 3 days ✎ ✖

Campaign Completion | Notify: User, Manager, Admin Email ✎ ✖

Remind Before Due Date | Notify: User, Manager, Admin | Send Reminder: 12 days before Email ✎ ✖

Remind After Enrollment | Notify: User | Send Reminder: 10 days after Resend Reminder: Every 5 days Email ✎ ✖

Edit Training Notification

Notification Type Welcome

Select Recipients and Templates

User ? VDACS New-Hire Security Awareness Training Notification ✎

Manager ? VDACS Employees Enrolled (Manager) (From Company Domain) ✎

Admin ? VDACS Users Enrolled (Admin) (From Company Domain) ✎

[Manage Training Notification Templates](#)

Save Cancel

Remind Before Due Date | Notify: User, Manager, Admin | Send Reminder: 2 days before Email ✎ ✖

Update Campaign

Campaign Notifications

- Select Specific Groups
- Enable** automatic enrollment for new users (if needed)
- Add Completed Users To a selected group (if needed)
- Schedule Email Notifications**
 - ✓ Welcome Emails
 - ✓ Remind after enrollment on-time
 - ✓ Remind after enrollment sent regularly at a specified interval
 - ✓ Remind before due date – approx. 10-12 days
 - ✓ Remind before due date – 2 days
 - ✓ Campaign Completion
 - ✓ Past Due

User Custom Notification Example

2022 Role-based Training Notification - Enrollment

[← Back To Training Notification Templates](#)

Template Name

2022 Role-based Training Notification - Enrollment

Leave this field blank to use the Subject field as the Template Name.

Sender's Email Address

itsecurity@vdacs.virginia.gov

Sender's Name

VDACS IT Security

Subject

Important: Mandatory VDACS Role-Based Training



VDACS Role-Based Training Enrollment

Hello [[display_name]].

The [[company_name]] (VDACS) uses the KnowBe4 platform to provide role-based security awareness training for employees that hold certain roles within the organization. You have been identified as being in one of the following roles: System Owner, Data Owner, or System Administrator. You have been enrolled in the [[TRAINING_CAMPAIGN]] which must be completed by [[training_campaign_end_at]].

If you do not currently hold any of the above roles and believe this was sent in error, please reach out to the VDACS IT Security team at itsecurity@vdacs.virginia.gov to let us know.

You can access the KnowBe4 platform by clicking on the icon posted on the new [VDACS Insite Information Systems page](#) and using your employee email address to log in, or you can use the unique link below to begin your training. The training content can also be accessed from a mobile device. Please use Google Chrome when accessing the training from a computer. [\[\[LOGIN_LINK\]\]](#)

We need to defend our organization against cyber crime, and security is a team effort. In order to meet the Commonwealth's IT security compliance requirements, it is important that you complete this training before the deadline. Please email VDACS IT Security if you have questions or need to report a suspicious activity.

Thank you!

VDACS IT Security
itsecurity@vdacs.virginia.gov

Manager Custom Notification Example

TRAINING USERS ASAP PHYSICAL TESTS - SECOND CHANCE MODSTORE REPORTS

VDACS Employees Incomplete (Manager) (From Company Domain) - 2 days left [← Back To Training Notification Templates](#)

Template Name

Leave this field blank to use the Subject field as the Template Name.

Sender's Email Address Sender's Name

Subject


Source | Styles | Format | Font | Size | Placeholder

This is a friendly reminder to ensure that employees complete the annual mandatory security awareness training. As of [[current_date_0]], [[user_list_count]] of your employees have not completed their assignment(s) as part of training campaign: [[training_campaign]] due in two days.

User List:

User Names	Emails
[[user_fullname_list]]	[[user_email_list]]

VDACS IT Security
itsecurity@vdacs.virginia.gov



body

Save

Policies Settings

PDF Test2021_Ethical Use of Agency Information and Computing Resources

[← Back to Policies](#)

Policy Title ?

Status ?

Minimum Time Required ?

Allow download ?

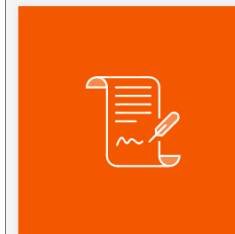
Description ?

Add Language

[+ Add Language](#) ?

Preview

×



27 days left

TEST2021_DHRM Policy 1.75 - Use of Electronic Communications and Social Media

Start

English (United States)

Received

Example Training Campaign

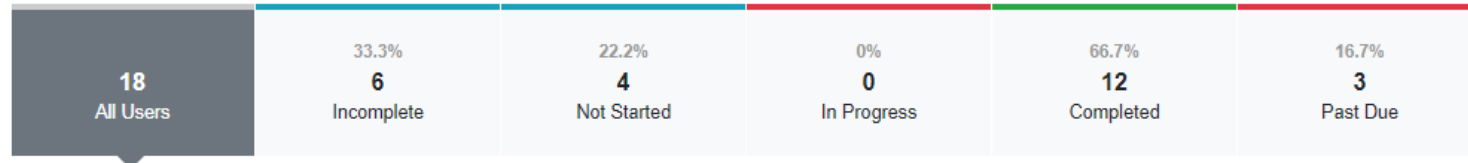
2023 VDACS New-Hire Security Awareness Training

[← Back to Training](#)

Groups: VDACS New Employees

Overview **Users** Survey Results

Note: Users are allowed to complete training after the due date. This setting can be changed by editing the campaign.



Search for users by name or email

Include Archived Users

[Bulk Update](#)

[Generate CSV](#)

[Enroll Users](#)

[Actions](#)

Send Notification

Training
Status
and
Reports

Survey Results

- You can use the results of your survey to keep informed on the type of content your users find the most engaging. Using training assignments that your users are more engaged with makes them more likely to finish their training on time.
- As an example, if you receive negative survey feedback regarding the length of the content you are assigning to users, you can adapt your training content selections based on this feedback for your next training campaign.

2023 VDACS New-Hire Security Awareness Training [← Back to Training](#)
Groups: VDACS New Employees

[Overview](#) [Users](#) [Survey Results](#)

Survey Results [Generate CSV](#)

Content Title	Responses	Helpfulness of Content	Length of Content	Presentation of Content
Business Conduct Series: Acceptable Use Policy <i>Duration: 5 minutes</i> <i>Style: Training Module</i>	2	5.0	5.0	5.0
Conflict of Interest <i>Duration: 2 minutes</i> <i>Style: Video Module</i>	3	4.7	5.0	5.0
Ethics: Gifts and Entertainment <i>Duration: 4 minutes</i> <i>Style: Training Module</i>	3	5.0	5.0	5.0
Fake Meeting Request Demonstration <i>Duration: 5 minutes</i> <i>Style: Video Module</i>	1	5.0	5.0	5.0
Insider Threats for End Users <i>Duration: 10 minutes</i> <i>Style: Training Module</i>	1	5.0	5.0	5.0

Challenges



**ACCOUNT FOR NETWORK PERFORMANCE
ISSUES FOR EMPLOYEES IN REMOTE
LOCATIONS.**



**HARD TO DIFFERENTIATE BETWEEN TRAINING MODULES COMPLETED
FROM ONE YEAR TO ANOTHER. CLOSE TRAINING CAMPAIGNS AS
NEEDED**



THANK YOU!



Ruxandra Teodorescu, CDPSE, CISA
VDACS Information Security Officer
ruxandra.teodorescu@vdacs.virginia.gov

ARCHER SCORECARD

Agency score card metrics captured from Jan. 1 to Dec. 31 of each calendar year. The metrics listed below reset at the beginning of each calendar year in Archer:

- Current year percentage of risk finding updates received;
- Current year percentage of audit finding updates received;
- ISO certification.

Agency head approved audit and risk plans covering a three-year period are due annually.

Expiring audit or risk plans should be updated as soon as possible and submitted to the CSRM mailbox, commonwealthsecurity@vita.virginia.gov.

Scheduled audits and risk assessments should be submitted upon completion and agency head approval.

March 31 is the end of the first quarter. Please submit all quarterly updates due to the CSRM mailbox.



UPCOMING EVENTS



IS Orientation

[06993b2934c3270491](#)

Remote – WebEx

Date: March 29, 2023

Start time: 1:00 p.m.

End time: 3:00 p.m.

Instructors: Erica Bland, Renea Dickerson and Tina

Gaines

<https://covaconf.webex.com/weblink/register/r97c7834e1e02a6>

The next scheduled meeting for the IS Council:

March 22, 2023 (revised date)

12 p.m. – 1 p.m. (virtual)

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

Government Innovation Virginia
How Technology is Making Citizens Lives Better
Wednesday, April 12, 2023
Richmond, VA | 8:00 a.m.
Network Drink Reception at 5 p.m.
Location: TBA

Register at:

[PSIS_2023_USA_Government-Innovation-VA.pdf \(publicsectornetwork.com\)](#)

Speakers:

Bob Osmond (VITA), Zacc Allen (DOC), Ravi Padma (DVS),
Mike Riggs (SCV), Peter Aiken (VCU) and more.....

The Compliance and Verification forms were due on Jan. 31, 2023.

The form maybe completed manually or in Archer by clicking on the “Verification and Compliance Tab under the Security Awareness Training Questionnaire for year 2022. If you do not see the tab, click on recalculate and it should appear.

If you have questions, contact
Tina.Gaines@vita.virginia.gov



APRIL ISOAG MEETING

APRIL 5, 2023

TIME 1 P.M. – 3 P.M.

SPEAKERS: TBA

MEETING ADJOURNED

