VIRGINIA IT AGENCY

WELCOME TO THE APRIL 5, 2023

ISOAG MEETING

AGENDA	
Welcome/Opening Remarks	Mike Watson/VITA
KnowBe4 Phising Campaign	Chantelle Yearwood/DBHDS
KnowBe4 Update	Tina Gaines/VITA
Exceptions	Chandos Carrow/VITA
NAC Project	Darrell Raymond/ATOS
Data Points	Erica Bland, Renea Dickerson &Tina Gaines/VITA
Upcoming Events	Tina Gaines/VITA
Adjourn	

Virginia Department of Behavioral Health & Developmental Services

Phishing Campaigns in KnowBe4

Agenda

Prerequisites

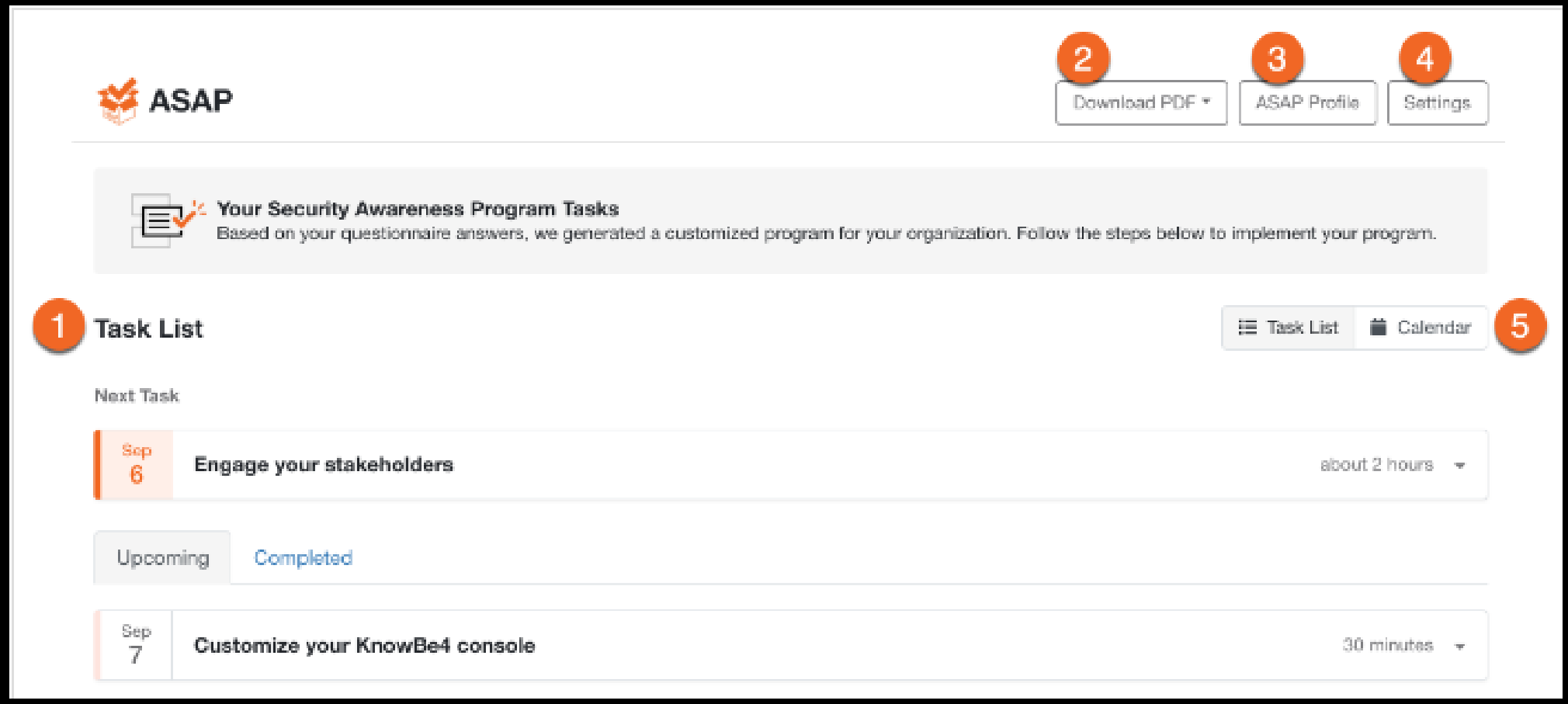
- ASAP
- Knowledge Articles
- ADI Sync / Okta
- Phish Alert Button
  - What is the PAB?
  - Training Available
  - Implementation

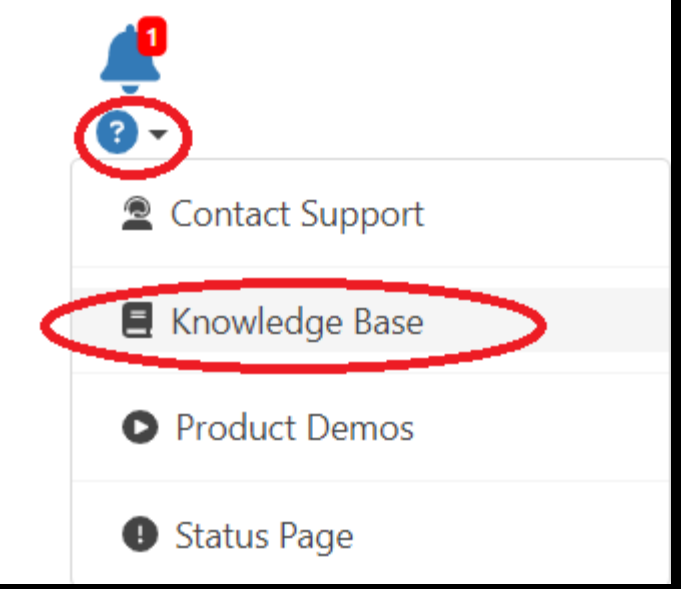
Phishing Campaigns

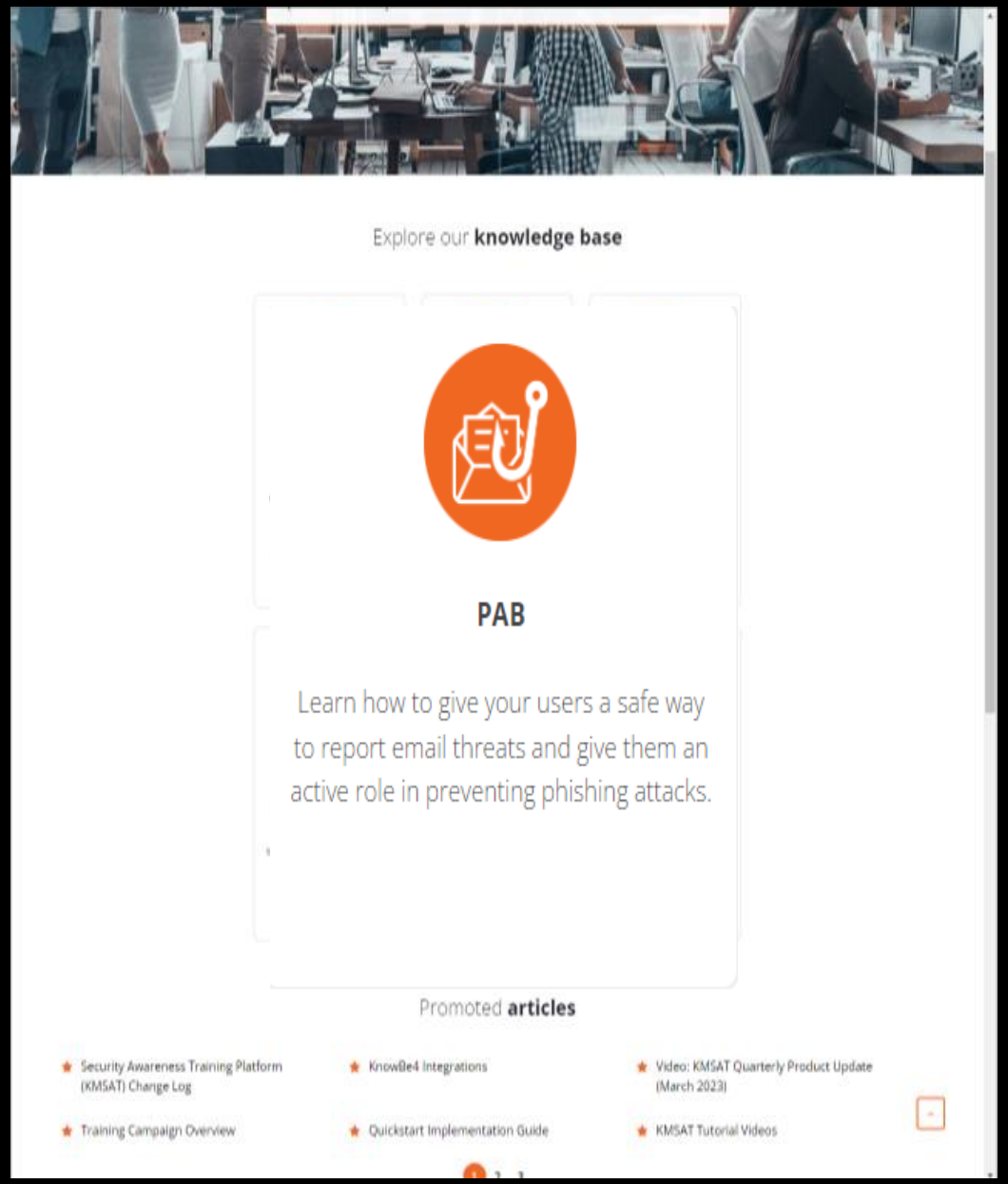
- Setting up Phishing Campaigns
- Monitoring
- Remediation

Prerequisites

ASAP Tab




1
Contact Support
Knowledge Base
Product Demos
Status Page


Explore our knowledge base
PAB
Learn how to give your users a safe way to report email threats and give them an active role in preventing phishing attacks.
Promoted articles
Security Awareness Training Platform (KMSAT) Change Log
KnowBe4 Integrations
Video: KMSAT Quarterly Product Update (March 2023)
Training Campaign Overview
Quickstart Implementation Guide
KMSAT Tutorial Videos

BE A HERO!

Use the Phish Alert Button

You receive an email asking you to take an action. Sounds suspicious, right? But don't worry. You can be a hero by taking the correct action–and giving your IT department the information they need to defend your organization against the effects of malicious email attacks. It's easy. Thanks to the **Phish Alert Button**, or **PAB** for short.

How do I know what to report?

You should only report messages you suspect are malicious, like **phishing** or **spear phishing** emails. Reporting annoying messages, like **spam**, to IT will waste their time and resources.

Spam is unsolicited and unwanted email, typically sent to try to sell you something. While it is often annoying and misleading, it is rarely malicious.

Simply delete it!

Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious.

Spear phishing emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are extremely malicious and can lead to very damaging consequences.

Report it with the PAB!

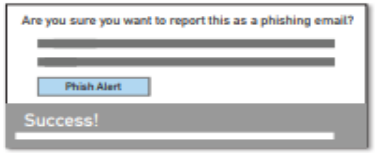
Where do I find the PAB in Office 365?

While viewing your email:

❶ You can find the Phish Alert Button by clicking the ellipses (or three dots) in the right side to open a menu. ❷ You can then click the Phish Alert Button at the bottom of the menu.

Confirm:

The pop-up box you see will prompt you to confirm your action. Once confirmed, the email in question will be immediately forwarded to your organization's IT team.



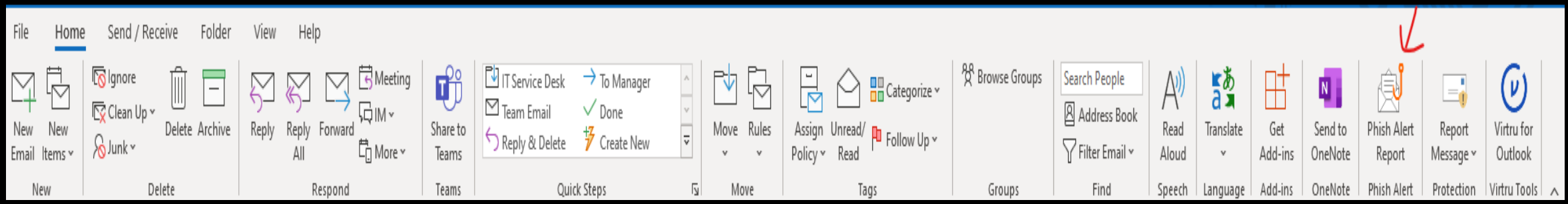
Stop. Look. Think. Report!

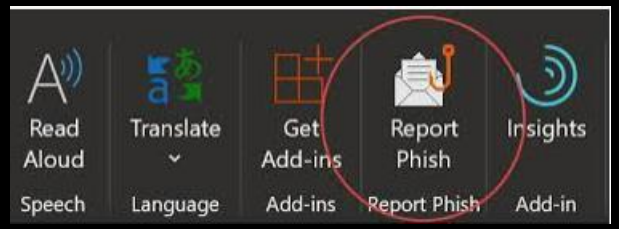
Remember, you are the last line of defense against email based criminal activity. Never click on a link or open an attachment in any unexpected or unsolicited email. If you are uncertain, follow your organization's security policy–or ask your IT team for advice.

KnowBe4
Human error. Conquered.

Locating the Phish Alert Button

The PAB can be found in the toolbar, in the reporting tab, at the top of the screen as shown below:

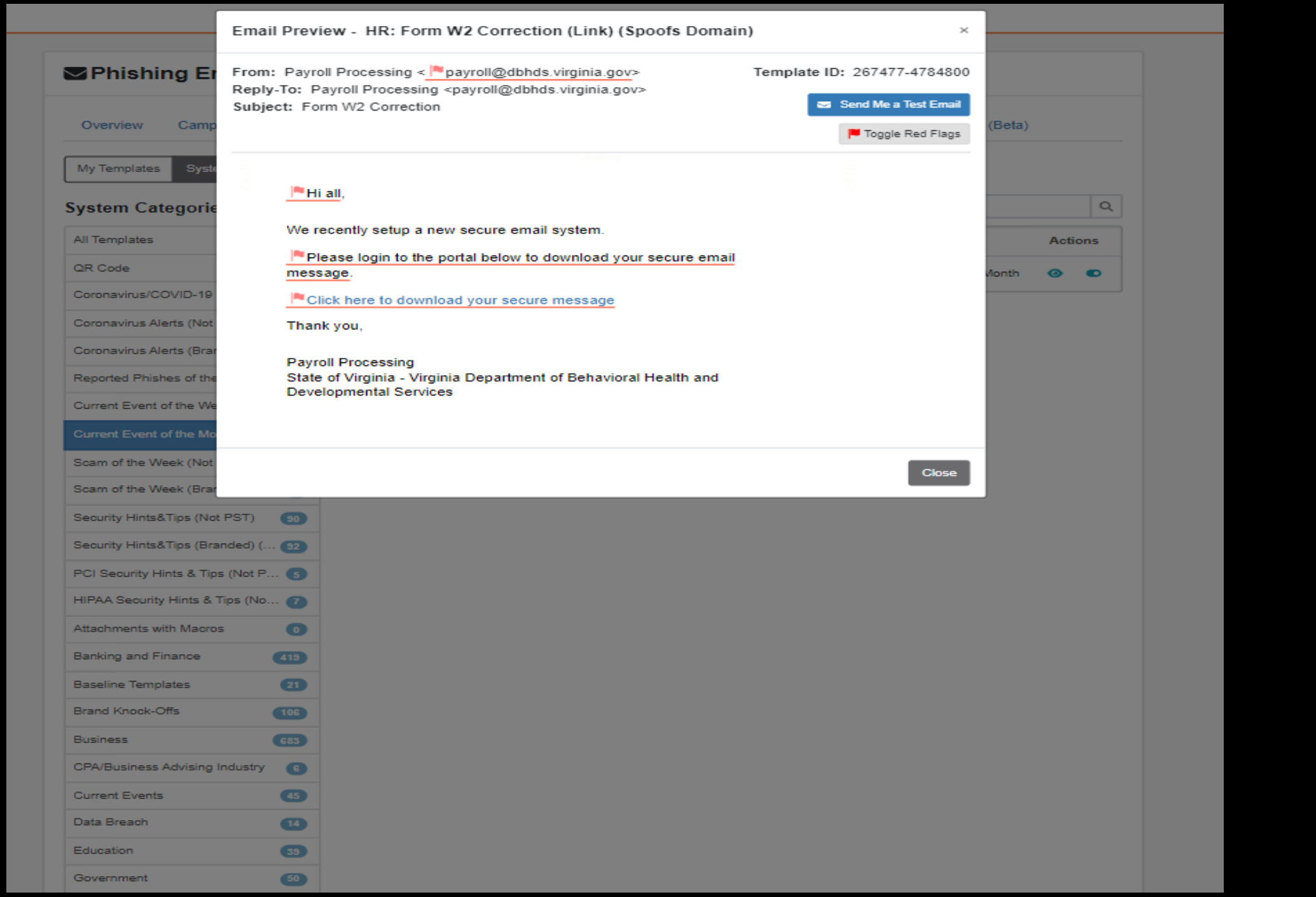




KnowBe4

KMSAT

Creating Phishing Campaigns


Email Preview - HR: Form W2 Correction (Link) (Spoofs Domain)
From: Payroll Processing < payroll@dbhds.virginia.gov>
Reply-To: Payroll Processing <payroll@dbhds.virginia.gov>
Subject: Form W2 Correction
Template ID: 267477-4784800
Send Me a Test Email
Toggle Red Flags
Hi all,
We recently setup a new secure email system.
Please login to the portal below to download your secure email message.
Click here to download your secure message
Thank you,
Payroll Processing
State of Virginia - Virginia Department of Behavioral Health and Developmental Services
Close
Phishing Er
Overview
Camp
(Beta)
My Templates
Syste
System Categorie
All Templates
QR Code
Coronavirus/COVID-19
Coronavirus Alerts (Not
Coronavirus Alerts (Bran
Reported Phishes of the
Current Event of the We
Current Event of the Mo
Scam of the Week (Not
Scam of the Week (Bran
Security Hints&Tips (Not PST) 90
Security Hints&Tips (Branded) (... 92
PCI Security Hints & Tips (Not P... 5
HIPAA Security Hints & Tips (No... 7
Attachments with Macros 0
Banking and Finance 419
Baseline Templates 21
Brand Knock-Offs 106
Business 683
CPA/Business Advising Industry 6
Current Events 45
Data Breach 14
Education 39
Government 50
Actions
Month

Email Preview - WordPress: Update Now! Severe security threat found in WooCommerce Payments (Link)

From: WordPress <noreply@account-wordpress.com>
Reply-To: WordPress <noreply@account-wordpress.com>
Subject: Update Now! Severe security threat found in WooCommerce Payments

Template ID: 267477-5016353

Send Me a Test Email

Toggle Red Flags

Show Remote Images

WordPress.com

PSA: Update Now! Critical Authentication Bypass in WooCommerce Payments Allows Site Takeover

After reviewing the latest WooCommerce Payments update we determined that it removed vulnerable code that could allow an unauthenticated attacker to impersonate an administrator and completely take over a website without any user interaction or social engineering required.

Regardless of the version you are using, we urge you to update to the latest version of the WooCommerce Payments plugin, which is 5.6.2 as of this writing, immediately. WooCommerce Payments is installed on over 500,000 sites, and this is a critical-severity vulnerability.

Click the link below to download the latest version of the plugin.

WooCommerce Payments – Fully Integrated Solution Built and Supported by Woo

Thank you,
The WordPress Team

Close

Landing Page

KnowBe4
Human error. Conquered.

English - United States

Oops!
You clicked on a simulated phishing test!

Remember these three rules to stay safe online:

01	02	03
Always stop, look, and think before you click!	Check for red flags that indicate a phishing attack is happening.	Verify suspicious emails with the sender through a different medium.

Remember: Always report suspicious emails to your supervisor or IT team. There are many ways

KnowBe4

KMSAT

Monitoring Phishing Campaigns

KnowBe4

KMSAT

Remedial
Training Campaigns


Q&A

VIRGINIA IT AGENCY

CYBERSECURITY AWARENESS TRAINING FOR THE COMMONWEALTH

Tina Gaines

CSRM

VIRGINIA IT AGENCY

PHASE TWO

- What VITA has completed:
  - Compiled the data we received from survey monkey into a spreadsheet as a centralized repository.
  - Currently working with KnowBe4 on agencies (KB4 only agencies) whose subscriptions are close to expiring so that there will not be a gap in console access for those agencies that are currently using the platform.
  - KnowBe4 console access was granted to those agencies who did not currently use the platform. Admins were sent instructions on how to access their console. There are a few agencies who do not have access and we are working with KB4 to resolve the issue. If you have not received your console access, contact CSRM.

PHASE TWO (con't)

- What VITA is working on:
  - Knowbe4 Training:

    Training on KB4 started 3/29 with six agencies in attendance. There will be weekly training sessions for admins to help them become familiar with setting up their training campaigns. The goal is to schedule 10 agencies at time until all admins are trained. Admins will be notified in advance of their scheduled training date. The dates are as follows:

    Thursday, April 6
    Thursday, April 13
    Monday, April 17
    Thursday, April 27

Note: Training sessions will be from 1:15 – 1:50 p.m. Individual agency sessions will also be made available once the initial training sessions are completed. Phishing training will be offered also with the date TBD.

- The agency should:
  - Generate reports to close out their current training solution for audit purposes.
  - Start uploading your users to the KB4 platform.
  - Create a preliminary test campaign.
  - Create a test group to assign training to.

How to Get Started with KnowBe4 Console:
https://support.knowbe4.com/hc/en-us/articles/115011714508
https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/KnowBe4-527-Crosswalk.pdf

Roll Out Time Line

- 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 as their training solution

- Phase Two (Month of March)– Majority of the agencies not included in phase one. This phase is scheduled 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.

APRIL 2023

EXCEPTION PROCESS IN ARCHER

CHANDOS CARROW

VITA/CSRM Acting Security Team Lead

ISOAG

VIRGINIA IT AGENCY

AGENDA

- Purpose of the Exception Process
- COV Exception Request Process
- Agency Specific View
- How to Enter an Exception in Archer
- Approval Process
- Review Process
- Expiration Process
- Extension Approval Process
- Appendix
- Questions

PURPOSE OF THE EXCEPTION PROCESS

- Inform VITA/CSRM of non-compliance or risk

- Document a strategy to eliminate the non-compliance or risk

USE CASE FOR EXCEPTIONS

Why would you need to submit an exception?

- When the agency is not able to meet a control established in a Standard or baseline for one or more of their systems.
- When there is an audit finding that cannot be resolved in 90 days.
- When there is a risk finding that cannot be resolved in 90 days.
- When there is a need to document agency Head approval for a control that requires agency Head approval.

COV EXCEPTION REQUEST PROCESS

- The exception request process is used to document any deviation(s) from the established controls in the COV Security Policies, Standards, or Guidelines; Enterprise Architecture Policies, Standards, or Guidelines; or COV Configuration Baselines.

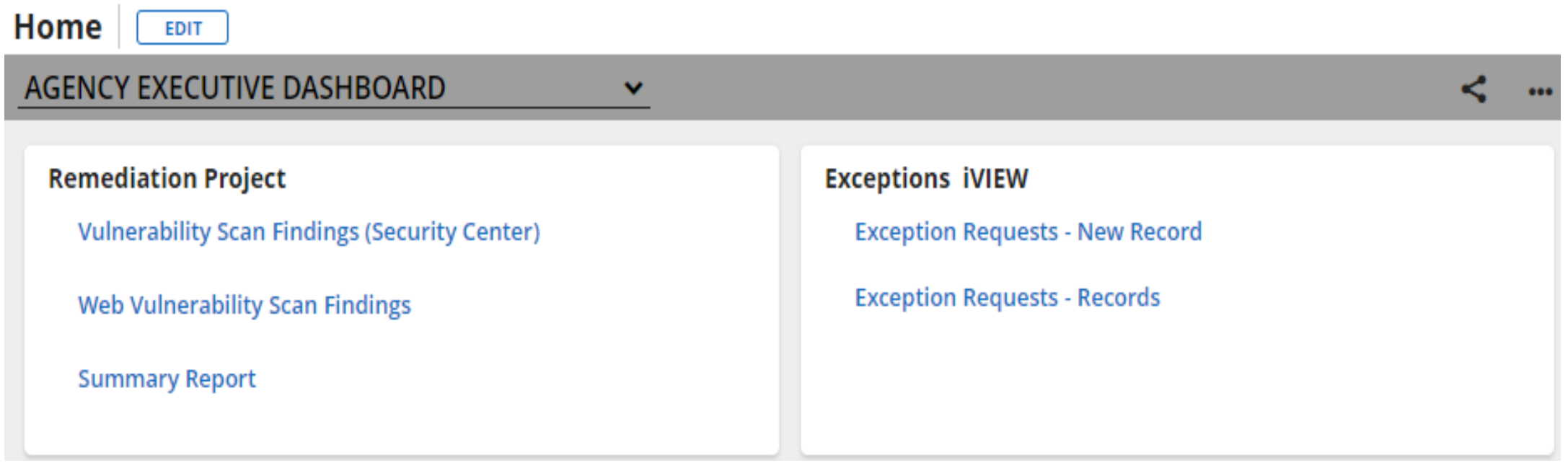
- The information provided within the exception will be used by the Agency ISO, Enterprise/Security Architect team, Agency Head, and the COV CISO/Deputy CISO to evaluate the risk as well as the controls implemented to mitigate the risk.

COV EXCEPTION REQUEST PROCESS (CONT)

- The exception request must be submitted by the COV Agency ISO or backup ISO. All SEC501, SEC525 and Enterprise Architecture exceptions must be submitted through Archer. If you need access to Archer, please contact Commonwealth Security at commonwealthsecurity@vita.virginia.gov.

- Exceptions can be granted up to one year. If the exception is still needed, the agency must file an extension.

AGENCY DASHBOARD



Click on 'Exception Requests – New Record' for starting a new exception request.

Click on 'Exception Requests – Records' for viewing your agency's exception requests.

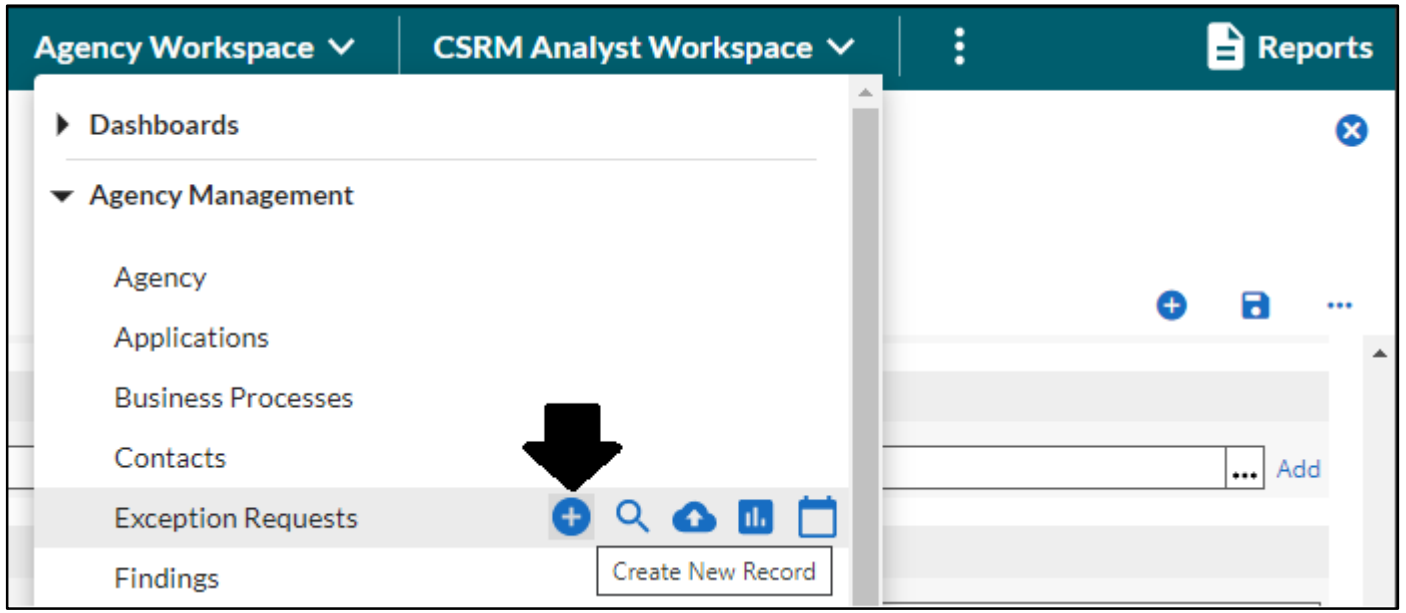
AGENCY DASHBOARD- OVERALL STATUS

Exception ID	Overall Status	Exception Type	Days to Expiration	Expiration Date
EXC-2020	In Architecture Review	SEC 525 (Hosted Environment/Cloud)		
EXC-1845	Closed	Enterprise Architecture		
EXC-1844	Extension Requested	Enterprise Architecture	0	1/12/2023
EXC-1750	Approved	SEC 525 (Hosted Environment/Cloud)	145	8/8/2023
EXC-1700	Approved	SEC 525 (Hosted Environment/Cloud)	134	7/28/2023
EXC-1688	Approved	SEC 525 (Hosted Environment/Cloud)	128	7/22/2023
EXC-1631	Closed	Enterprise Architecture		
EXC-1581	Approved	Enterprise Architecture	16	4/1/2023
EXC-1559	Closed	SEC 501	2	3/18/2023
EXC-1432	Expired	SEC 525 (Hosted Environment/Cloud)	0	11/18/2022
EXC-1374	Expired	SEC 525 (Hosted Environment/Cloud)	0	10/4/2022

CREATING AN EXCEPTION

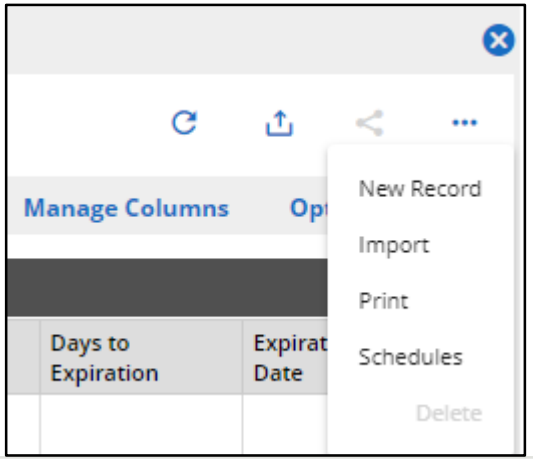
- Login to Archer:
- Navigate to:

Agency Workspace → Agency Management → Exception Requests → Circle with Plus Symbol.



- Alternately navigate to:

Agency Workspace → Agency Management → Exception Requests → 3 Dots → New Record.



NEW RECORD

Exception Requests: Add New Record

SAVE | SAVE AND CLOSE

Exception Declaration | Review and Approvals | Extension Request

▶ ABOUT

▼ GENERAL INFORMATION

Exception ID:

* Agency:

Submission Status: Draft

Overall Status: Draft

Expiration Date:

Submit Date:

Days to Expiration:

Requested Expiration Date:

Initial Creation Date:

The requested duration of the exception should not exceed twelve months.

Closure Status: Open

Number of Extensions:

Agency Contact: Add

Architect Type:

Exception Type:

COV Inherited Permissions:

NEW RECORD (CONT)

Exception Requests: Add New Record

SAVE | SAVE AND CLOSE

▼ ASSOCIATED POLICIES

Associated Policies: [...]

▼ EXCEPTION DECLARATION

* Exception Description:

Business and Technical Justification:

NEW RECORD (CONT)

Business Impact and Risks:	
Residual Risk:	

NEW RECORD (CONT)

▼ AFFECTED APPLICATIONS

Affected Applications: [...] Add

▼ ASSOCIATED FINDINGS

Associated Findings: [...] Add

▼ COMPENSATING CONTROLS

Compensating Controls: [...]

Additional Compensating Controls:

NEW RECORD (CONT)

▼ AFFECTED DEVICES

Affected Devices: ... Add

▼ EXCEPTION REQUEST ATTACHMENTS Add New

Name	Size	Type	Upload Date
No Records Found			

▼ AGENCY HEAD APPROVAL Add New

Name	Size	Type	Upload Date
No Records Found			

▶ HISTORY

COMPLETING AN EXCEPTION (CONT)

Please enter the following required information:

- Agency
- Submit Date
- Requested Expiration Date (**CANNOT** exceed 12 months)
- Agency Contact
- Exception Type (Enterprise Architecture, SEC501, or SEC525)
- Associated Policies
- Exception Description
- Business and Technical Justification (please be as detailed as possible)

COMPLETING AN EXCEPTION (CONT)

Please enter the following required information:

- Business Impact and Risk (please be as detailed as possible)
- Residual Risk (the risk still associated after the additional compensating controls have been implemented associated with the control identified)
- Affected Applications
- Additional Compensating Control (needs to identify the actions taken by the agency to mitigate the risk of not meeting that control)
- Affected Devices

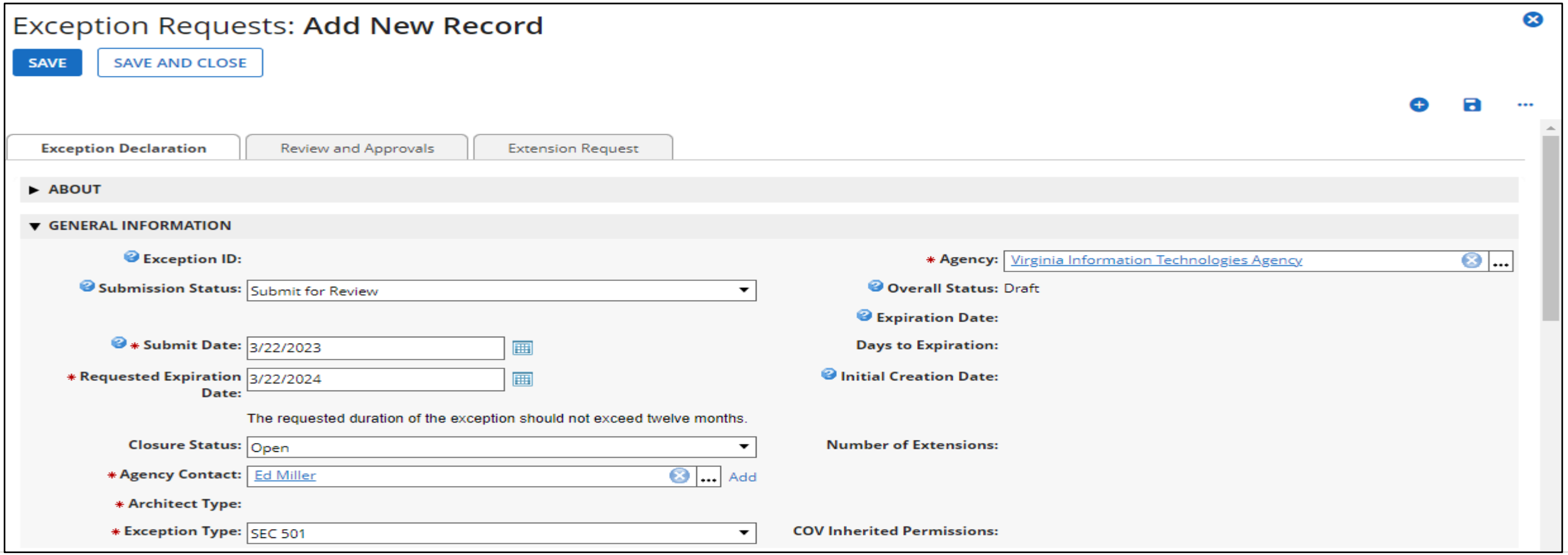
COMPLETING AN EXCEPTION (CONT)

Optional Fields:

- Any attachments which will aid in the review process:
  - Project plans – tasks, scheduled dates, person(s) responsible
  - RITMs, PRJs, REQs, DMNDs, INCs, PGRs
  - Email communications with suppliers
  - Proof of designation of authority (if necessary)
  - Any Associated Findings (if applicable)
  - Etc.
- DO NOT attach the agency head approval at this point.

SUBMITTING AN EXCEPTION (CONT)

Once the information has been entered, please change the 'Submission Status' to 'Submit for Review' and click 'SAVE' (located at the top of the form). The Architecture team will get an email once it has been submitted and the overall status will update to 'In Architecture Review'.



REVIEW PROCESS

You have submitted your exception. Now what happens?

1. If the Architect needs additional information from the agency, they will change the status to 'Awaiting Submitter Feedback'.

1. The Architect will type questions in the 'Comments and Conditions' text box, and send an email to the Agency Contacts.

1. If an agency gets an email asking for feedback on an exception ('Awaiting Submitter Feedback'), please remember to place the exception in Draft mode before entering and/or attaching any information.

1. Once you have entered, all requested information, please change the Submission Status back to 'Submit For Review' and this will send an email to the Architecture team.

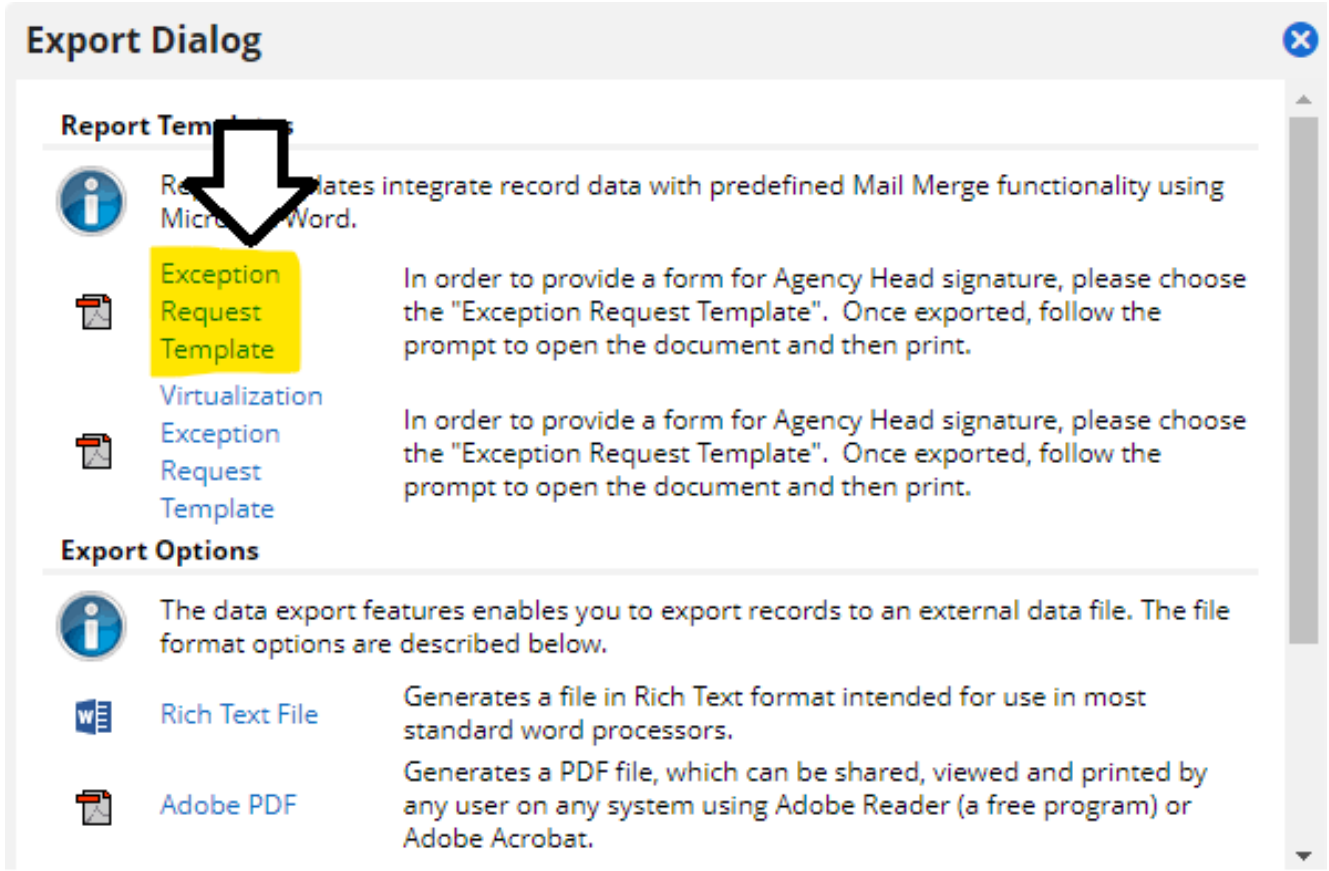
1. Once the review is complete, the Architect will change the exception status to 'Ready for Agency Head Approval' and the agency ISO will receive a notification email to obtain Agency Head approval.

APPROVAL PROCESS (CONT)

ISOs can print the 'Exception Request Template' for Agency Head Signature from the 'EXPORT' option within the exception record. Open the exception and at the top right, click on the Export button.

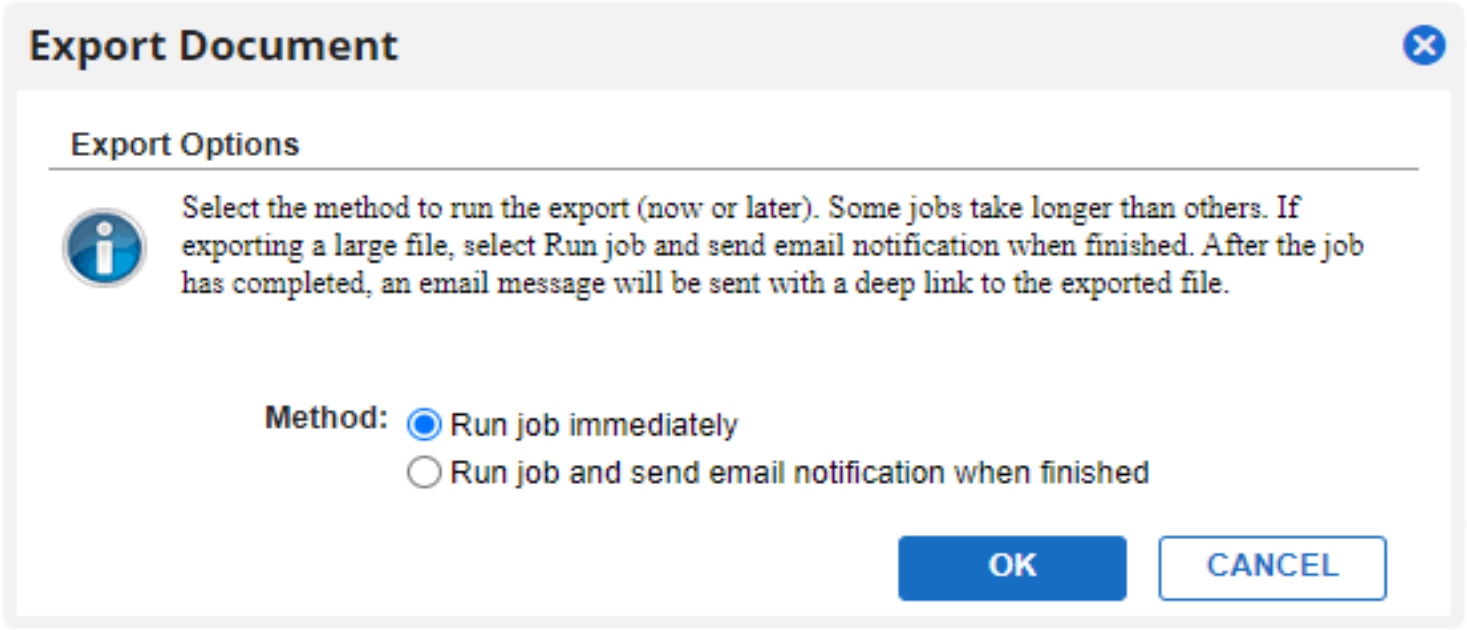
APPROVAL PROCESS (CONT)

At the "Exception Request: Export Options" window, select "*EXCEPTION REQUEST TEMPLATE*"



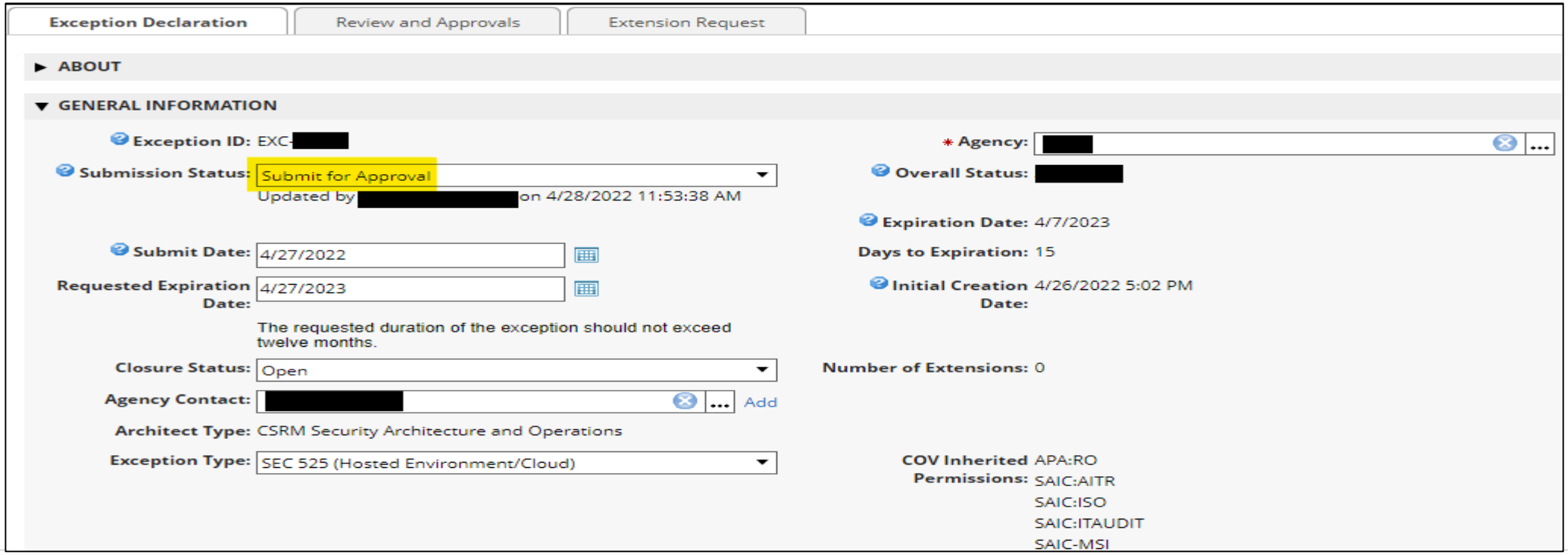
APPROVAL PROCESS (CONT)

At the 'Export Document' window, select Method: 'Run job immediately' and then click 'OK'.



APPROVAL PROCESS (CONT)

Once the agency head approval is ready, scan the signed document, make sure the Submission Status is set to 'DRAFT' and upload it to the exception record as a PDF file under the 'Agency Head Approval' section. Then Change the Submission Status to 'Submit for Approval' and 'SAVE'.



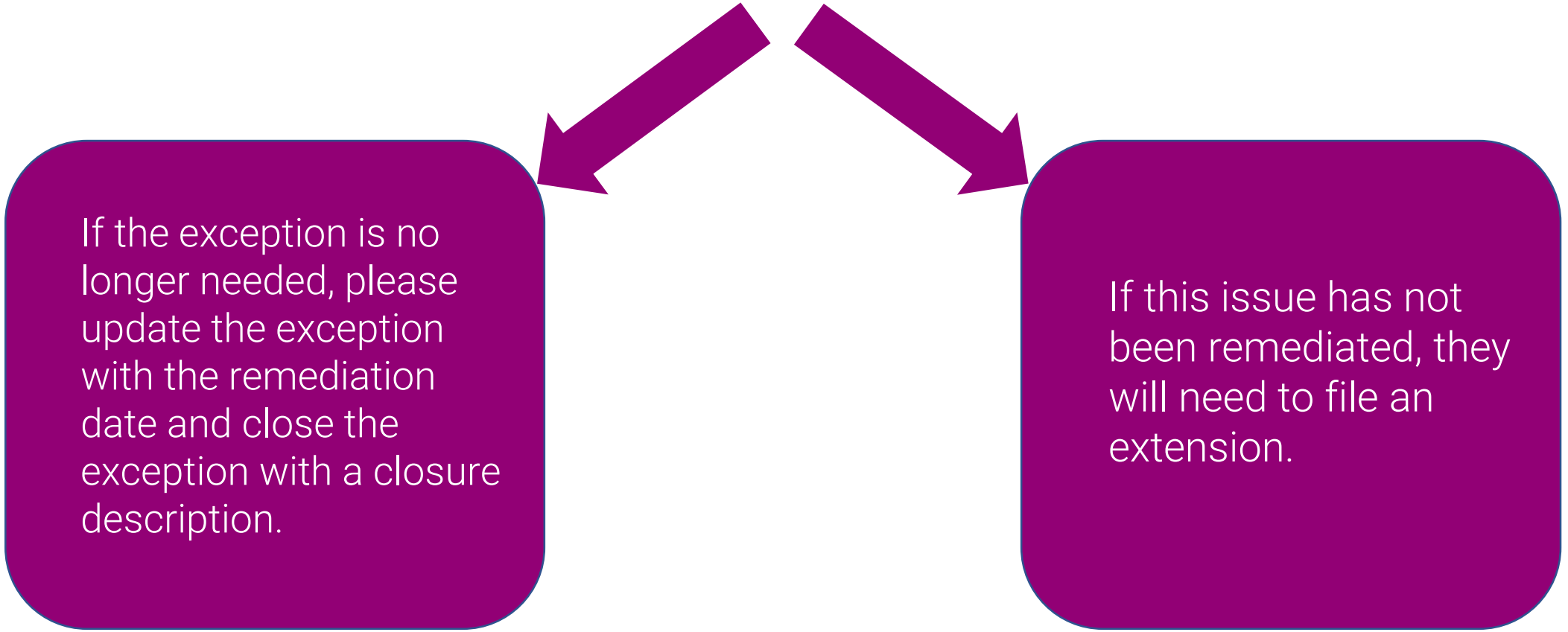
REVIEW PROCESS

Once the Agency Head approval has been attached and the exception Submission Status changed to 'Submit for Approval', the Architect will receive an email and perform their final review to ensure everything is documented correctly.

After review, the Architect will add their comments stating that the Architect review is complete and input their recommendation for approval. The exception is then reviewed by CSRM, where it is either approved or denied. An email is then automatically sent to the agency's ISO of the update and they can then send it to their appropriate agency personnel.

EXCEPTION EXPIRATION

Approximately 30 days and two weeks prior to the exception expiration date, the ISO will receive an email notifying them of the expiration:

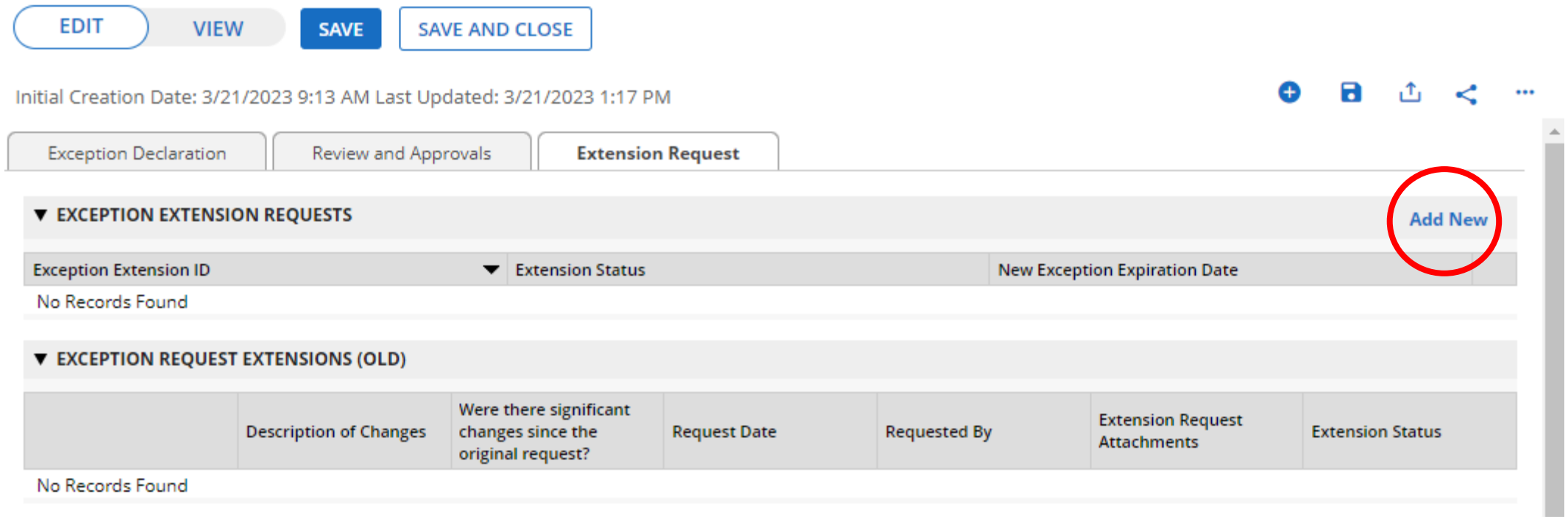


CLOSING PROCEDURE

EXCEPTION EXTENSION

Filing an extension:

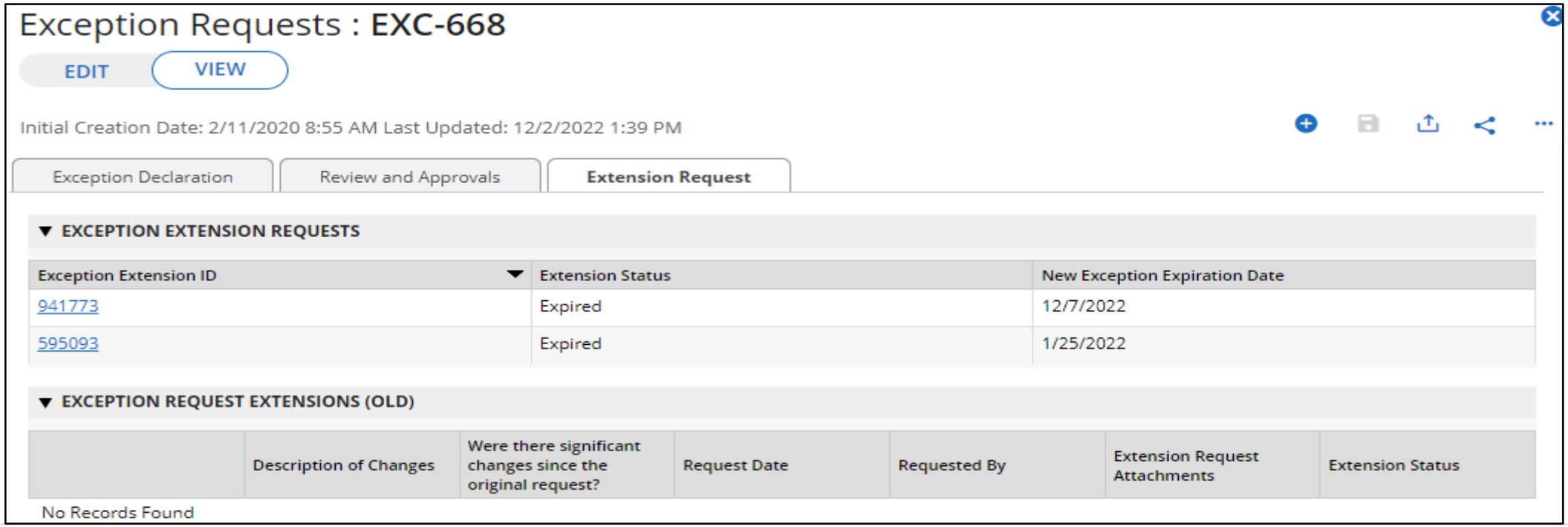
In the exception request, click on 'Extension Request' tab, click on 'Edit', and then click on 'Add New'.



EXCEPTION EXTENSION

After creating an exception extension it will then show under section ‘Exception Extension ID’

Click on the Exception Extension ID that was created to view it’s ‘General Information’.



EXCEPTION EXTENSION (CONT)

On the 'General Information' tab of the exception, complete the following fields:

a. Agency
b. Agency Submission date
c. Submitted by
d. Requested extension expiration date (which is to not exceed 12 months)
e. Exception Type
f. Extension Justification and Change (please be as detailed as possible)
    i. Reason for extension
    ii. Updated project plan with tasks, dates, and person(s) responsible
    iii. Updated remediation plan.

EXCEPTION EXTENSION (CONT)

General Information | Review and Approvals

▼ GENERAL INFORMATION

Exception Extension ID:

Exception: EXC-1762 ... Add

Agency Submission Status: Draft

* Agency:

Agency Submission date:

Extension Status:

Submitted By:

Extension Expiration Date:

Requested extension expiration date:

Architect Type:

Exception Type:

* Extension Justification and Changes: Please describe the changes that have occured here.

EXCEPTION EXTENSION (CONT)

DO NOT attach the Agency Head Approval at this point.

1. Attach any necessary documentation in the Extension attachment on the General Information tab that provides evidence for the need for the extension

2. Once the information has been entered, please change the 'Agency Submission Status' to 'Submit for Review' and click 'SAVE' (located at the top of the form). The Architecture team will get an email once it has been submitted and the overall status will update to 'In Architecture Review'.

EXCEPTION EXTENSION (CONT)

Please note:

If an agency gets an email from CSRM entitled 'Awaiting Submitter Feedback', please remember to place the extension in Draft mode before entering any information. Once you have entered, all appropriate information, please change the status back to 'Submit For Review' and this will send an email to the Architecture team.

EXTENSION REVIEW PROCESS

You have submitted your extension. Now what happens?

1. If the Architect needs additional information from the agency, they will change the status to 'Awaiting Submitter Feedback'.

1. The Architect will type questions in the 'Comments and Conditions' text box, and send an email to the Agency Contacts.

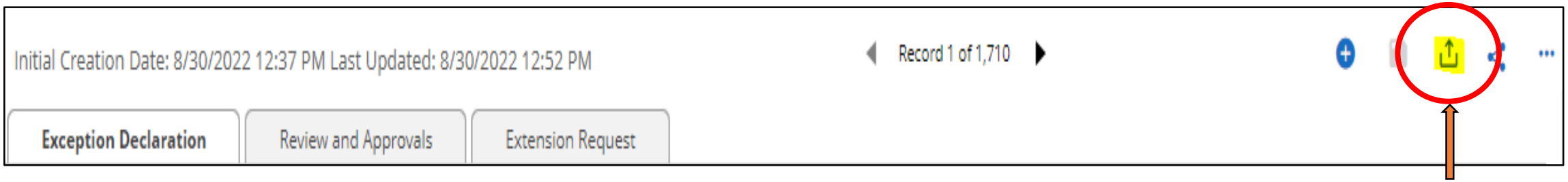
1. If an agency gets an email asking for feedback on an exception ('Awaiting Submitter Feedback'), please remember to place the exception in Draft mode before entering and/or attaching any information.

1. Once you have entered, all requested information, please change the Submission Status back to 'Submit For Review' and this will send an email to the Architecture team.

1. Once the review is complete, the Architect will change the exception status to 'Ready for Agency Head Approval' and the agency ISO will receive a notification email to obtain Agency Head approval.

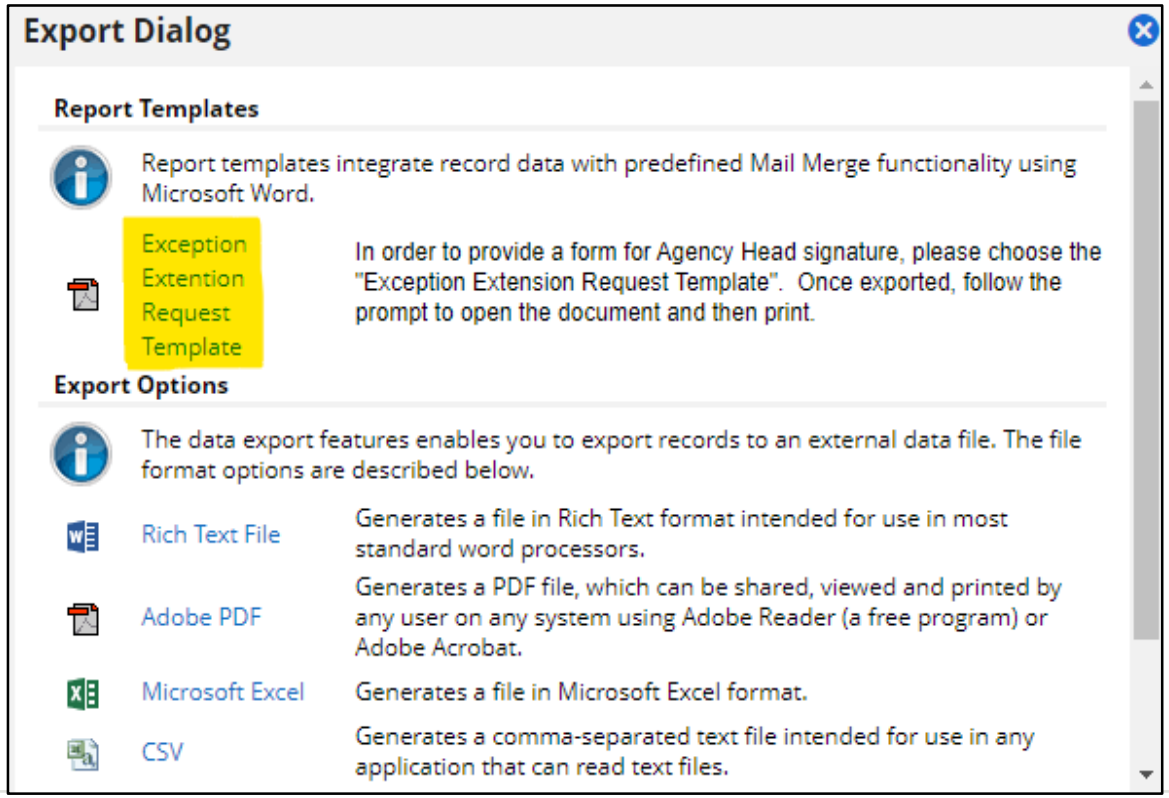
APPROVAL PROCESS (CONT)

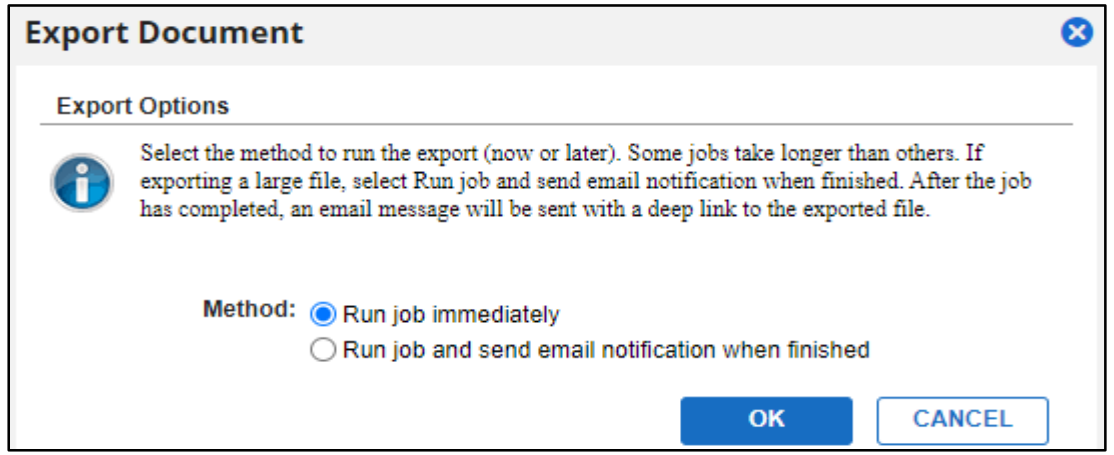
ISOs can print the 'Exception Request Template' for Agency Head Signature from the 'EXPORT' option within the exception record. Open the exception and at the top right, click on the Export icon.

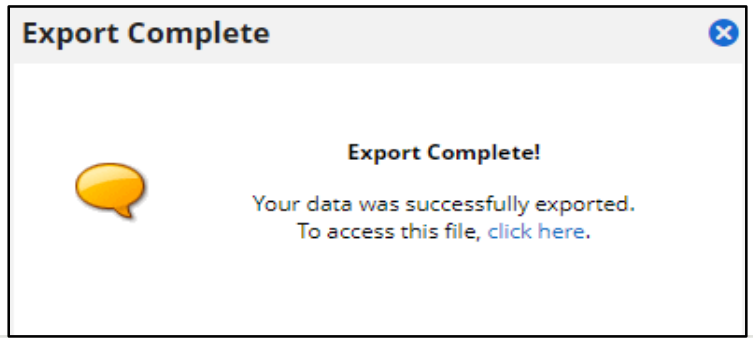


APPROVAL PROCESS (CONT)

After clicking on the export icon, you can select 'Exception Extension Request Template,' then an Export Document pop-up will display. Select the 'Run job immediately' and select 'OK'. Then an Export Complete pop-up will display, select 'click here' to download the PDF.

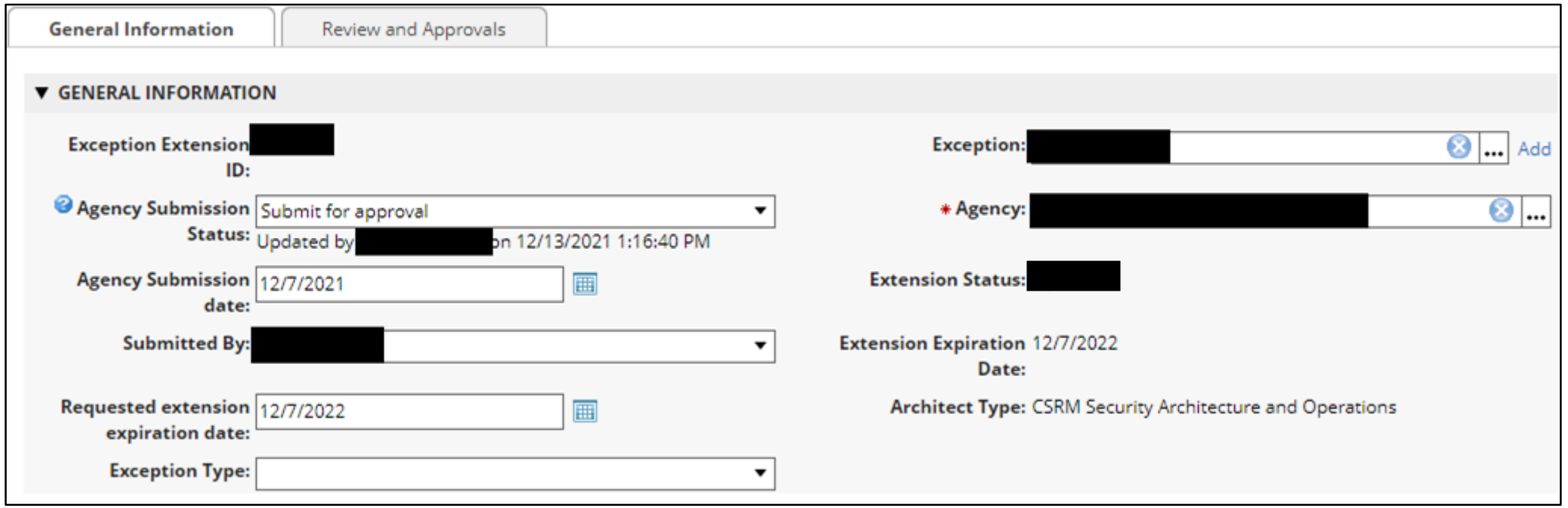






APPROVAL PROCESS (CONT)

Once the Agency Head approval is ready, scan the signed document, make sure the Submission Status is set to 'DRAFT', and upload it to the exception record as a PDF file under the 'Agency Head Approval' section. Then change the Submission Status to 'Submit for Approval' and 'SAVE'.



REVIEW PROCESS

Once the Agency Head approval has been attached and the exception Submission Status changed to 'Submit for Approval', the Architect will receive an email and perform their final review to ensure everything is documented correctly.

After review, the Architect will add their comments stating that the Architect review is complete and input their recommendation for approval. The exception is then reviewed by CSRM, where it is either approved or denied. An email is then automatically sent to the agency's ISO of the update and they can then send it to their appropriate agency personnel.

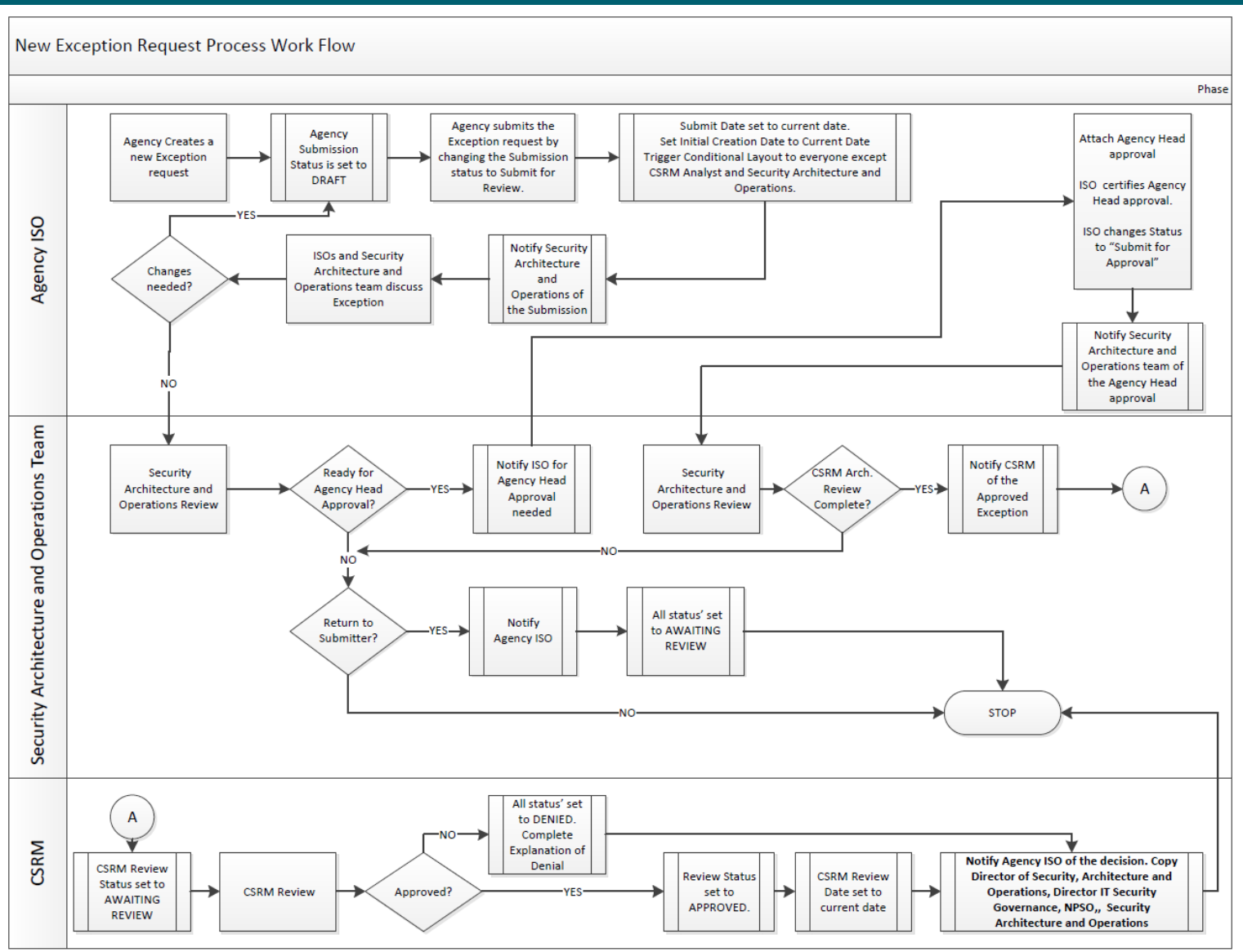
APPENDIX

NEW EXCEPTION PROCESS WORK FLOW

For EA exceptions - POC is Stephen Smith

For SEC 501 exceptions - POC is Preston Talbott or Chandos Carrow

For SEC 525 exceptions - POC is Debi Smith or Wilbert Jones



QUESTIONS?

THANK YOU

And a big thank you to the Security Architect

Team who put this presentation together!

Thank you very much Jackie and Preston!!

VIRGINIA IT AGENCY

COMPLIANCE TESTING NETWORK (CTN)

CMDB Policy Notification/VITA Rollout/April 2023

Jeff Barker
CTN Project Manager

APRIL 5, 2023

- The Compliance Testing Network (CTN) is a network access control tool that verifies compliance with COV security standards prior to providing access to COV network resources.
- The CTN comprises discovery and enforcement technologies commonly known as network access control (NAC).
- CTN provides an infrastructure to ensure network compliance of endpoints connected to the Commonwealth of Virginia (COV) network. ForeScout is the primary NAC software for CTN.

Current Project

Project 1: CMDB compliance verification and notification

Future Projects

Project 2: Security agents' compliance and notification

Project 3: Enforcement

- All workstations on the network should be in CMDB. CTN is doing a CMDB compliance check on all workstations. Any workstation not in CMDB will generate an email to the agency ISO and AITR notifying them that there is a workstation that is out of compliance and needs to be added to CMDB.

- The agency will need to submit a CMDB update request.

- Project 1a CMDB compliance and notification will start on April 10th with VITA only. If there is a non-compliant workstation, the VITA ISO and AITR will receive an email notification. They will need to take action to add the workstation into CMDB.
- Project 1b CMDB compliance and notification for all other agencies will start April 17.
- We recommend that each ISO check the VITA Security Dashboard to validate current compliance of the CMDB policy.
- Agencies can be proactive by submitting CMDB update requests as needed.

For questions about the project please contact

Jeff Barker (jeffrey.barker@Atos.net)

Kevin McLees (kevin.mclees@Atos.net)

VIRGINIA IT AGENCY

SECURITY MINUTE: DATA POINTS

ERICA BLAND

IT Security Governance Analyst

ISOAG MEETING

APRIL. 5, 2023

We're now in the second quarter of the calendar year!

- The compliance metrics we know as **data points** revolve around each agency's **audit** and **risk** programs for the calendar year. These metrics help to demonstrate how an agency is managing its IT security program.

- VITA is required to annually report to the Governor and General Assembly on the state of the Commonwealth's IT security per ***§ 2.2-2009. Additional duties of the CIO relating to security of government information.***

- The report is a public record and it's **VERY IMPORTANT** that each agency does well.

- Based on the data point metrics, we use Archer to calculate a report card grade for each agency.

- The data point metrics are fairly straightforward. We convert each metric to a numeric score, add them up and then average it. Then the numeric score is reported as a letter grade: A B C D F

AUDIT DATA POINTS

- The **audit score** is probably the simplest to calculate but may be one of the hardest to receive a high score on. Each sensitive system is required to be audited at least once every three years.

- Auditing has very specific requirements and can only be performed by qualified and independent auditors.

- Audits can also be very involved, time-consuming, and costly (especially if they need to be out-sourced). It is incumbent on the agency head to allocate sufficient resources in order to have its sensitive systems audited in a timely and efficient manner.

AUDIT DATA POINTS

- The ***audit score*** is essentially the average of three data points:

  1) Audit plans. Each agency must submit an **audit plan** *annually*. The only requirement is that it lists all the agency's sensitive systems and includes a scheduled audit date within three years of the date of the last audit. The metric will be either pass or fail (numerically that means 100% or 0%). It can be re-submitted anytime your plan changes.

  2) Audits. Each sensitive system should be audited at least *once every three years*. The metric is a percentage of sensitive systems audited. If the agency is reporting 10 sensitive systems and eight were audited over the last three years period, it's a score of 80%.

  3) Quarterly updates. Remediation steps need to be reported for *all open audit findings on a quarterly basis*. If a finding is open all year long, we are expecting at least four updates for the finding. The metric is a % of quarterly updates received for each finding. If an agency cannot remediate a finding in 90 days, please submit an exception request.

- The final audit metric is **[(Audit plan) + (% of audits completed) + (% of quarterly updates)] / 3**

RISK DATA POINTS

The **risk score** is probably more directly controlled by the agency ISO since it doesn't have to involve auditors.

- It consists of eight different metrics:
  1. **Risk assessment plan** (must be submitted annually/PASS or FAIL)
  2. **Risks assessments performed** (% of RAs submitted over the last three years)
  3. **Quarterly updates of risk assessment findings** (works the same way as audit findings, reported as a %)
  4. **BIA** (All reported business processes must be updated annually. Archer calculates a %)
  5. **Applications certified** (all applications must be "certified", i.e., associated with at least one business process, one dataset and at least one device (or product/service). IT strategic plan approval requires app certification.
  6. **IDS reporting** each quarter (for enterprise managed agencies, this is always a PASS. For independent agencies, we expect quarterly updates to be sent to Commonwealth security)
  7. **ISO certification** (agency primary ISO must meet the certification requirement, this is reported as (PASS/FAIL)
  8. **ISO must report to the agency head** (required by OSIG audit of security in the Commonwealth in 2019)

The final risk metric is **[(risk assessment plan) + (% of risk assessments completed) + (% of quarterly updates) + (% business processes updated) + (% of applications certified) + (% of IDS reports submitted) + (ISO certification) + (ISO reports to agency head)] / 8**

RISK DATA POINTS

The **risk score** is then just a simple calculation:

+ RA plan (must be submitted annually. Its either Pass/Fail or 100%/0%)

+ % RAs over the last three years

+ % of QUs received for the current year

+ BIA % (must be updated annually)

+ Applications certified (must be certified annually)

+ IDS reports (must be submitted quarterly)

+ ISO certified (an annual requirement)

+ ISO reporting to agency head

SUBTOTAL and divide by 8

That's it.

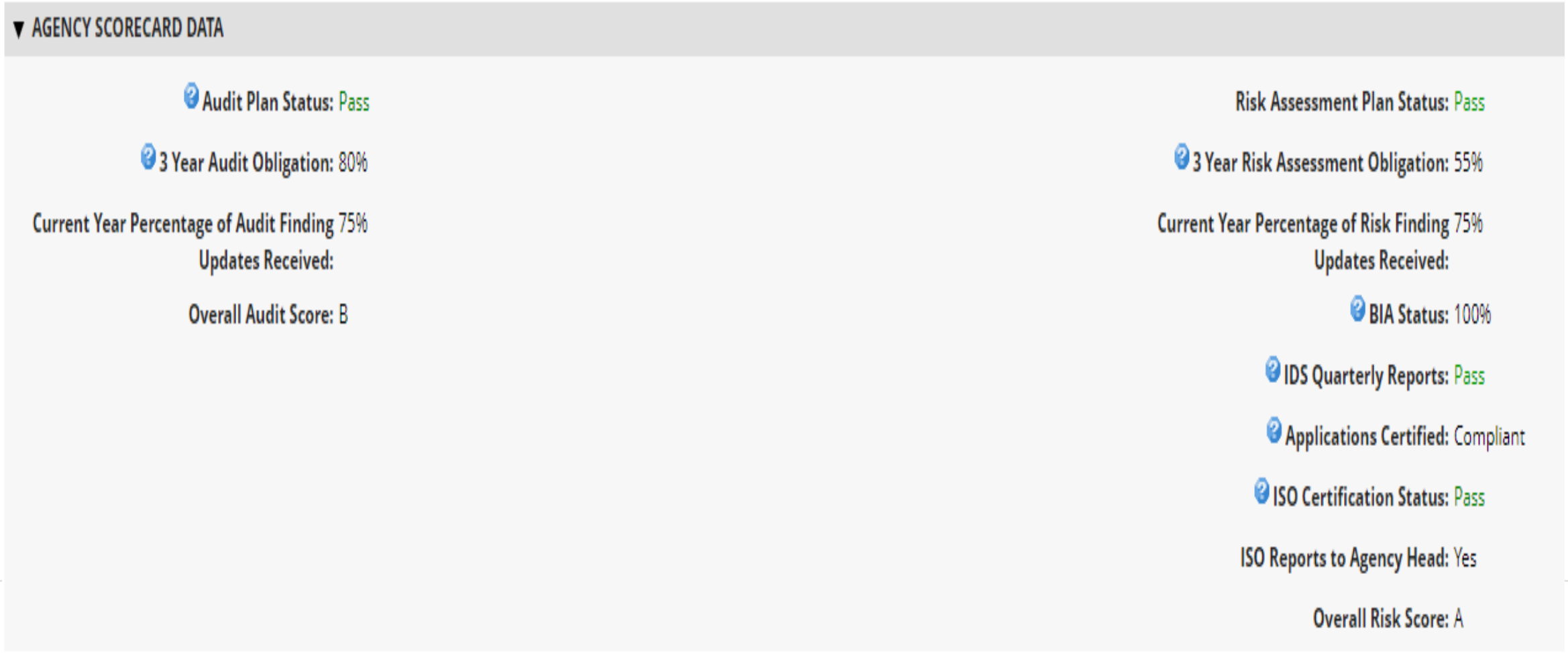
The way the metrics are setup and the way Archer works for some of the metrics, most scores don't start to accurately reflect what the agency will receive as a grade until some time in the fourth quarter, and usually not until the first quarter of the next year.

Your agency's CSRM analyst can help you stay current and on track.

In addition, Archer automatically sends out a reminder for some of the metrics when they are due or about to expire.

ARCHER DATA POINTS

- You can keep track of your agency's data point status by looking in Archer.
- When in Archer, click on your agency's name in any place where you see it hyperlinked.
- Scroll about halfway down and you'll see your agency's current scorecard.



AGENCY DATA POINTS REMINDER

- Submit quarterly updates, audit reports, and risk assessments timely. We encourage you to not wait until the fourth quarter to submit artifacts for the calendar year.
- Routinely check Archer to ensure your audit and risk scores are accurate.
- If you have any questions, please contact your CSRM analyst and/or the Commonwealth Security mailbox.

QUESTIONS?

UPCOMING EVENTS

IS ORIENTATION

IS Orientation

Remote – WebEx

Date: June 28, 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/rbc9d847b4c8579e4428f406f6275aeb9

The next scheduled meeting for the IS Council:

May 17, 2023

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 – 8:00 a.m.
Richmond Marriott
500 East Broad Street – Richmond, VA
VA Network Drink Reception at 5 p.m.

Register at:
PSIS_2023_USA_Government-Innovation-VA.pdf (publicsectornetwork.com)

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

2023 COV SECURITY CONFERENCE - SAVE THE DATE

Save the date for the most innovative Commonwealth of Virginia Information Security conference, yet!

This year's conference will be on **Thursday, Aug. 17**, at the Hilton Richmond Hotel and Spa/Short Pump at 12042 West Broad Street, Richmond, VA 23233.

Join us for a day of thought - provoking discussions and networking opportunities with industry experts.

Stay tuned for more details on our can't-miss IN PERSON event!

ISO REMINDERS
COMPLIANCE AND VERIFICATION SAT FORMS

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

MAY ISOAG MEETING

MAY 3, 2023

TIME 1 – 3 P.M.

SPEAKERS: TBA

VIRGINIA
IT AGENCY

MEETING ADJOURNED