From:	Laska, Erin (SAO)
To:	Fox, Stevens (WaTech)
Cc:	Wilson, Karen (SAO)
Subject:	RE: Legislative risk and compliance report assistance request
Date:	Thursday, January 18, 2024 12:55:00 PM
Attachments:	image001.png image002.png

Good afternoon, Stevens, if this is what you needed may I delete from the SAOShare? Just checking in

---

From: Laska, Erin (SAO)
Sent: Tuesday, December 12, 2023 8:31 AM
To: Fox, Stevens (WaTech) <stevens.fox@watech.wa.gov>
Cc: Wilson, Karen (SAO) <wilsonk@sao.wa.gov>
Subject: RE: Legislative risk and compliance report assistance request

Good morning, Steve

Is this what you are looking for?

Grant Information Request

~ Erin

From: Fox, Stevens (WaTech) <stevens.fox@watech.wa.gov>
Sent: Monday, December 11, 2023 6:54 AM
To: Laska, Erin (SAO) <laskae@sao.wa.gov>
Cc: Wilson, Karen (SAO) <wilsonk@sao.wa.gov>
Subject: RE: Legislative risk and compliance report assistance request

Erin,

I recall you shared a summary of audit findings earlier this year in connection with the SLCGP grant. The email retention process has since deleted that email. Can you resend it?

What I seek is a list of either finding associated with either weak controls or non-compliance with OCIO 141.10. I can then map those findings to CIS Control deficiencies. I can use this information to identify potential threat scenarios that target those deficiencies.

Thanks,

Stevens

From: Wilson, Karen (SAO) <wilsonk@sao.wa.gov>
Sent: Tuesday, December 5, 2023 8:43 AM

To: Fox, Stevens (WaTech) <stevens.fox@watech.wa.gov>; Laska, Erin (SAO) <laskae@sao.wa.gov>
Cc: Zee, Samantha (WaTech) <samantha.zee@watech.wa.gov>
Subject: RE: Legislative risk and compliance report assistance request

Hi Stevens and Samantha,
We do not do any statewide comparison of attestation audits as each is an individual contract and results are between the agency and WaTech for consideration and resolution.

For our audits where we issue our opinions we find that most agencies don't have formalized or current risk assessments to identify risks and potential mitigations so we don't get to review those for risks identified.

I'm not completely sure I answered your question but will be on the call Friday if you need to redirect me to what you are looking for.

Karen Wilson, CPA, CISA
IT Systems Program Manager

From: Fox, Stevens (WaTech) <stevens.fox@watech.wa.gov>
Sent: Monday, December 4, 2023 5:40 AM
To: Laska, Erin (SAO) <laskae@sao.wa.gov>; Wilson, Karen (SAO) <wilsonk@sao.wa.gov>
Cc: Zee, Samantha (WaTech) <samantha.zee@watech.wa.gov>
Subject: Legislative risk and compliance report assistance request

Erin and Karen,

I am working on a legislative report associated with RCW 43.105.450(7)(c),

"On an annual basis, the office of cybersecurity must provide a confidential report to the governor and appropriate committees of the legislature identifying and describing the cybersecurity risk or failure to comply with the office of cybersecurity's security policy or implementing cybersecurity standards and policies, as well as the agency's plan to resolve such failure or risk. Risks that are not mitigated are to be tracked by the office of cybersecurity and reviewed with the governor and the chair and ranking member of the appropriate committees of the legislature on a quarterly basis."

My assumption is the SAO may be able to provide 2022-2023 audit-based insights on compliance gaps and any related risks. Samantha Zee may be able to provide insights from audit-related waiver requests.

I will engage with CISA to get some vulnerability and threat intelligence to enhance my data set. Let me know if you know of some information sources I should consider.

Thanks,

Stevens F. Fox, MBA, CISSP, CISA, CISM, GDPR Practitioner
Washington Technology Solutions

Deputy CISO, Policy and Program Management
360-480-6771 | Mobile
Mailstop 41501
1500 Jefferson Street SE | Olympia, WA 98504-1501

Need help? Contact us through our **Customer Portal** or 360-586-1000 | 1-855-WaTech1.
Legal Notice: Under Washington's Public Records Act, all emails sent by or to me on this state-owned email account may be subject to public disclosure.