# A Modern Day Look at Auditing Cybersecurity Risks

DEBBIE LEW
SVP, CHIEF AUDIT EXECUTIVE
KAISER PERMANENTE



## Agenda/Objectives

- Discuss audit committee expectations and communications on cybersecurity audit results.
- Discuss challenges and opportunities to audit cybersecurity risks
  - Share internal audit limitations, traditional and non-traditional cybersecurity audit approaches
- Understand the benefits and challenges of leveraging NIST Cybersecurity Framework (CSF)
- Leveraging the NIST Cybersecurity Framework (CSF) to audit cybersecurity

Members
**12.7M**

Hospitals
**39**

Medical offices[1]
**622**

Physicians[2]
**23,982**

Nurses[3]
**68,218**

Employees+
**212,974**

# KP at a glance

Kaiser Permanente exists to provide high-quality, affordable health care services and to improve the health of our members and the communities we serve.

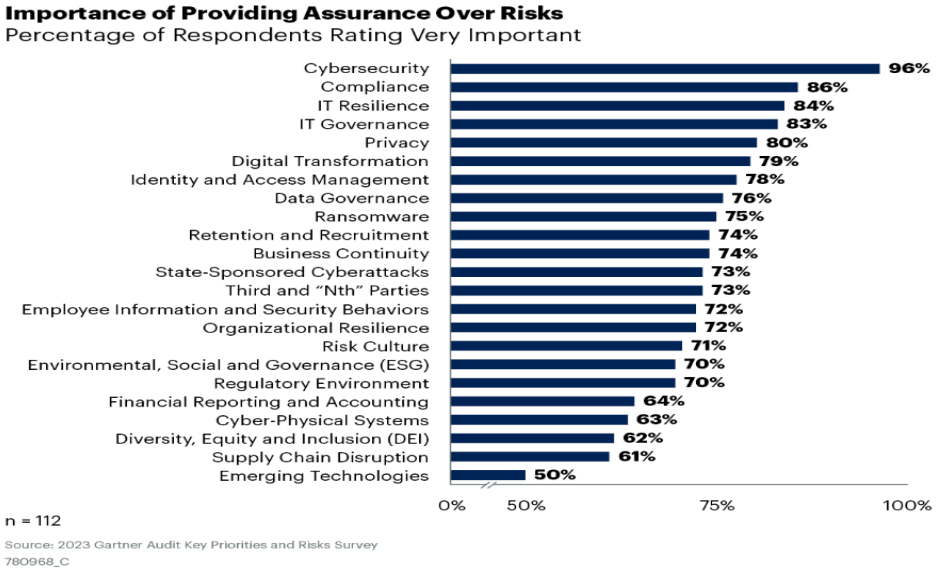


# Audit Committee Priorities

## Polling Question #1

**Go to menti.com, Enter Code provided**

# 2023 Top CAE-Identified Risks






# Audit Committee Communications

Discussion:

How do you communicate cybersecurity audit results to your Audit Committee?

# Challenges for auditing Cybersecurity

## Thoughts?

**Go to menti.com, Enter Code provided**



# Audit Approaches for Cybersecurity Audits

Discussion:

What is your approach to auditing cybersecurity?

- Risk assessment
- How many?
- Frequency
- Resources
- Framework
- Use of techniques and technology
- Other

# NIST Cybersecurity Framework?

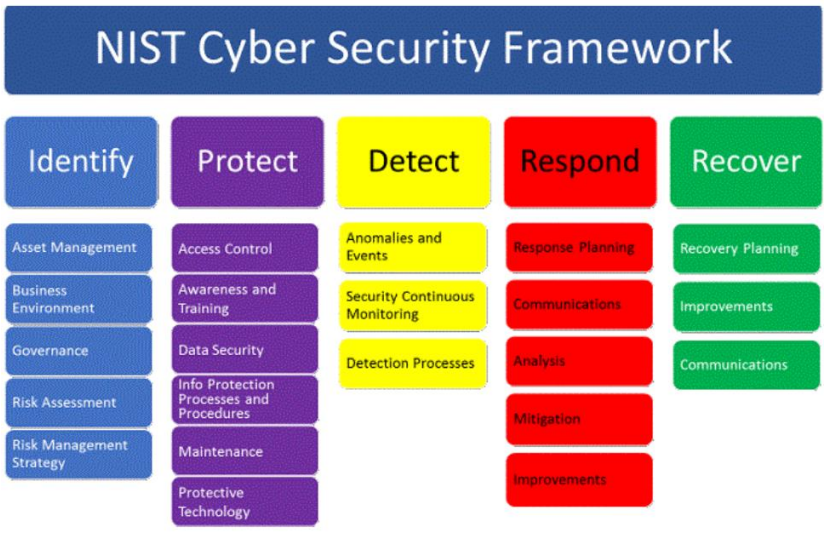
## What framework do you leverage to audit Cybersecurity?

**Go to menti.com, Enter Code provided**



# Why NIST Cybersecurity Framework (NIST CSF)

- NIST developed the Cybersecurity Framework (CSF) for Protecting Critical Infrastructure Cybersecurity in response to an executive order from President Obama.
- Health and Human Service's recommended cybersecurity framework, and it's the framework that DHHS Office of Civil Rights utilizes to conduct their own assessments of covered entities.
- Gartner says NIST will be used by over 55% of US organizations by 2021
- Developed by thousands of contributors and organizations, making it an independent, agnostic framework that is flexible
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction
- Guided by many perspectives – private sector, academia, public sector



# NIST CSF – Mapping to other frameworks

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions | **CIS CSC**, 16<br>**COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03<br>**ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4<br>**ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1<br>**ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1<br>**NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 |
| | | **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | **CIS CSC** 1, 12, 15, 16<br>**COBIT 5** DSS05.04, DSS05.10, DSS06.10<br>**ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9<br>**ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10<br>**ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4<br>**NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 |



# Enterprise cybersecurity audit journey

- Develop an enterprise cybersecurity audit strategy over 2 years
- Have a dedicated cybersecurity audit team (hire for the right skills)
- Develop a Communication Plan including what reporting would look like
- Send communication announcement of the audit to the enterprise
- Clear roles and responsibilities (RACI)
- Selected the National Institute Standards Technology Cybersecurity framework (NIST CSF) to audit against
- Consolidate and map NIST 800-53 key controls against the NIST CSF
- Budget and plan controls testing each quarter (timeline)
- The audit will be based on objective, pass/fail testing rather than interviews as requested.

For example:

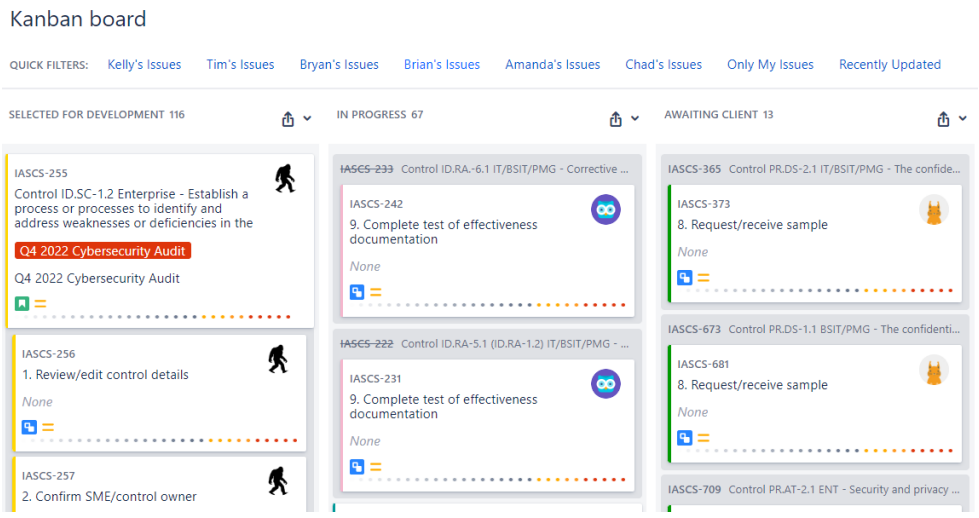
| | |
|---|---|
| Control: | Microsoft Window Patches are in place |
| Pass Criteria: | 100% of devices connected to the network are updated within XX days of patch availability |
| Sample: | 100% of connected devices for a set period (xx/xx/xxxx to xx/xx/xxxx) |
| Test result: | 92% updated |
| Grade: | Fail |

# Pass/Fail of Cyber controls testing

| Control Count | IT/Clinical | Control ID | Pass/Fail Criteria | Sample Size | Sample Results | Test Results | Issue Reference |
|---|---|---|---|---|---|---|---|
| # | Type | ID.BE-1.1 | Supply chain risks have been identified and documented. Of the sampled supply chain risks, 99% or more have appropriate safeguards implemented to limit adverse effects. | XX vendor risk registers | XX/XX met criteria | Pass | N/A |
| # | Type | ID.AM-5.1 | Assets are prioritized based on criticality and business value. Of the sample selected, 100% must include a classification in alignment with the business priority in the Business Impact Assessment (BIA). | XX business impact assessments | XX/XX met criteria | Pass | N/A |
| # | Type | ID.RA-1.1 | Server vulnerabilities are resolved timely as defined by policy/standard on 100% or more of systems examined. | XX,XXX servers | XX,XXX out of XX,XXX met criteria | Fail | # 2 |
| # | Type | PR.IP-12.1 | Server vulnerability scans (Qualys) are performed on systems, system components and systems services. Of the systems selected, 99% or more must have vulnerability scans performed on systems, system components and systems services. | XX,XXX scanned servers by Qualys | XX,XXX met criteria | Pass | N/A |
| # | Type | DE.AE-4.1 | System audit records are reviewed and analyzed for indications of inappropriate or unusual activity including impact of detected events. Of the sample selected, 99% or more must include risk/impact rating for the event. | XX event logs | XX/XX met criteria | Pass | N/A |
| # | Type | RS.CO-3.1 | Of the sample selected, 95% or more shows evidence of communication of assessment findings to the appropriate risk owner. | XX applications | XX/XX met criteria | Pass | N/A |

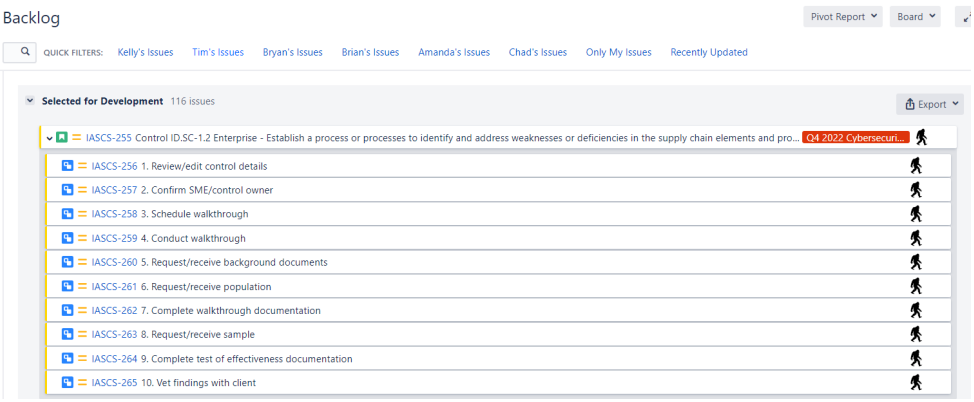


# Use of Agile & Jira




**Kanban board showing the controls started ("Selected for Development") and "In Progress" by the auditors as well as items in the client's queue ("Awaiting Client").**

# Use of Agile & Jira




**The Jira backlog shows the controls that are in scope for the quarter and awaiting start.**

**Once the auditor is ready to start them, they will be pulled into the "Selected for Development" status.**



# Next Steps

- Develop cybersecurity audit strategy
- Include follow-up audits of Corrective Action Plans from the enterprise cybersecurity audit.
- Risk-based and cadence coverage map.
- Continuous Auditing (use of AI?) – collaborate with CISO to identify risk indicators to include.

# Thank you for Sharing Your journey

Questions?

Thank you!



# Resources

- CSWP 29, The NIST Cybersecurity Framework 2.0 | CSRC – NIST Cybersecurity Framework
- Cybersecurity Framework | CSRC (nist.gov) – implementation/audit testing recommendations
- CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov) – crosswalks to other frameworks