Risk Management

Date: April 14, 2021

Agenda

1. Risk management overview
2. Risk model overview
3. Program health score overview
4. Current risk treatment streams
    - Out-of-Cycle reviews
    - End of Support/Open criticals
5. (p)(7) overview
6. Questions and answers

Risk Management Overview Section

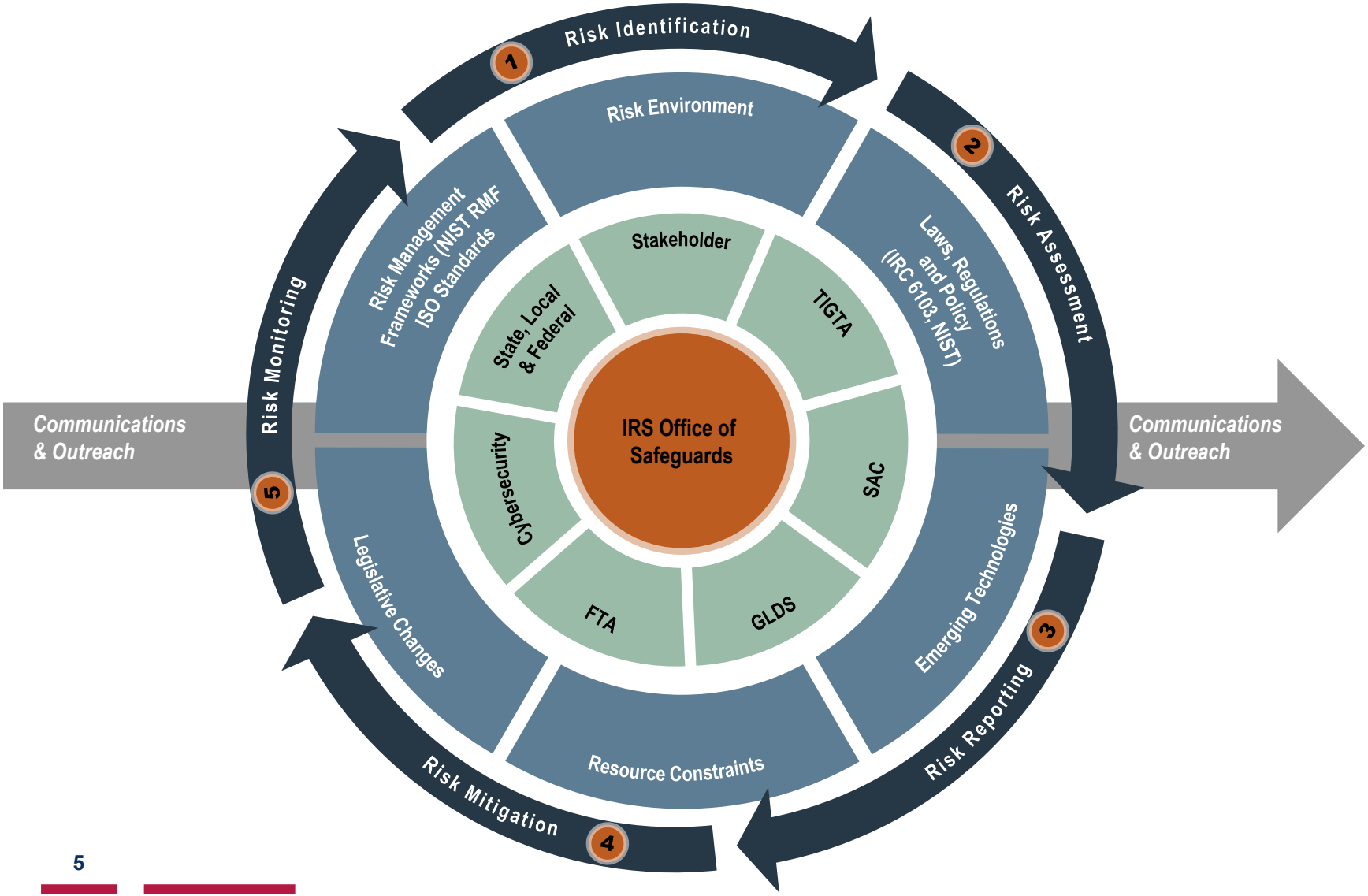
Risk Management Overview

Risk management is important due to increased cyber incidents, continually emerging cyber threats, and the need to prevent federal tax information (FTI) breaches. As such, the IRS Office of Safeguards has enhanced its risk-based capabilities.

Safeguards follows a multiphase, risk-based initiative to provide more attention to higher-risk agencies. The initiative:

- Uses a risk-driven methodology that reduces the likelihood of significant FTI data breaches and incidents
- Enhances the Safeguards Risk Model with a risk profiling capability to expand compliance focus with data-driven risk management focus
- Increases confidence in the integrity of the tax system

Risk Management Overview



Risk Management Overview

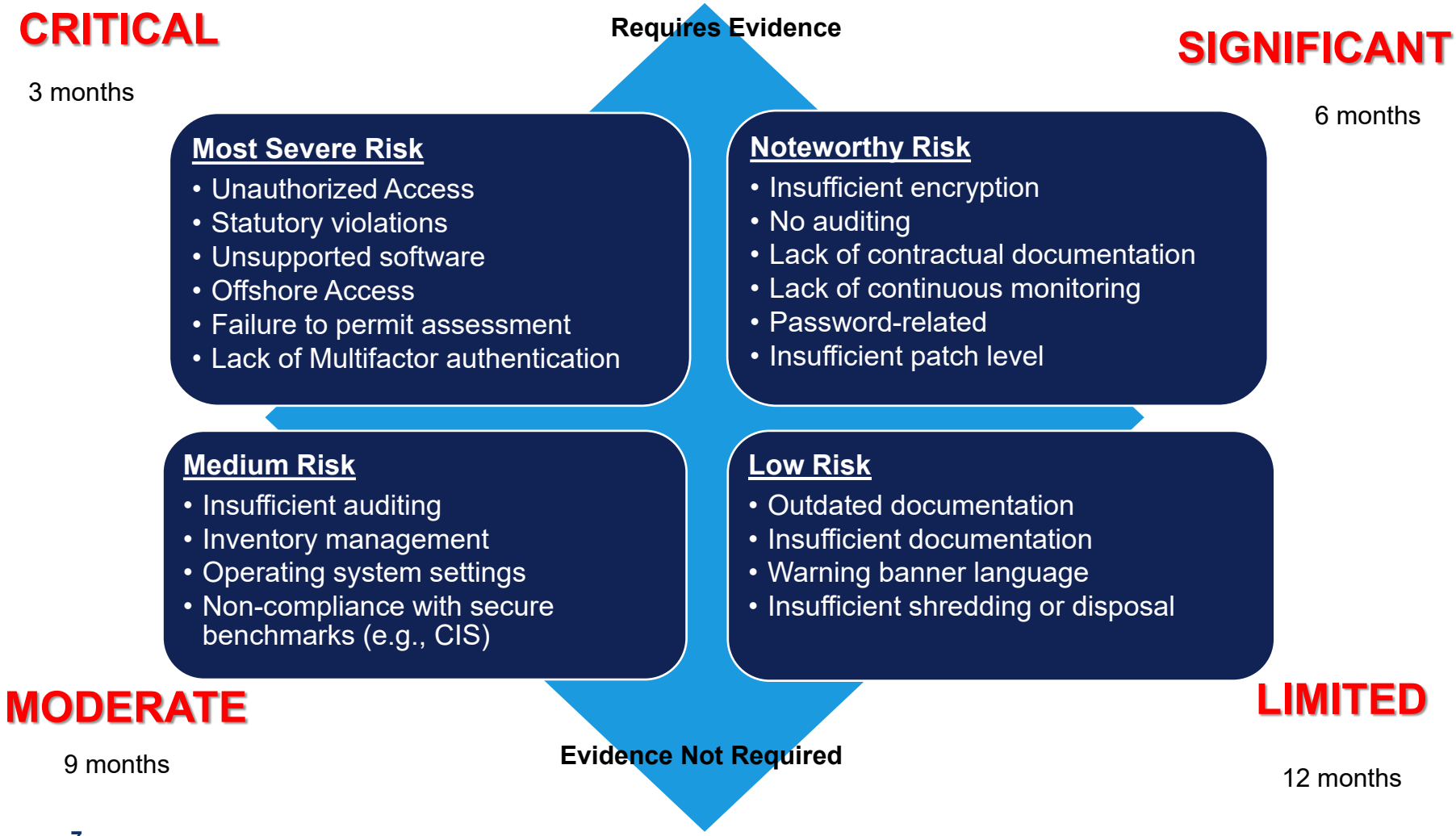
Safeguards collects most of the data used for risk management during on-site reviews, remote assessments, out-of-cycle reviews and agency reports (CAPs and SSRs).

Safeguards assigns each review finding a criticality and corresponding issue code based on potential impact and likelihood of risk:

- “Criticality” identifies the risk level: limited, moderate, significant and critical.
- Issue codes used to categorize findings.
  - They group similar findings to identify trends or common vulnerabilities

Risk Management Overview

Findings are categorized into four different **criticality ratings** used to define risk and the IRS targeted implementation date.



Risk Model Overview Section

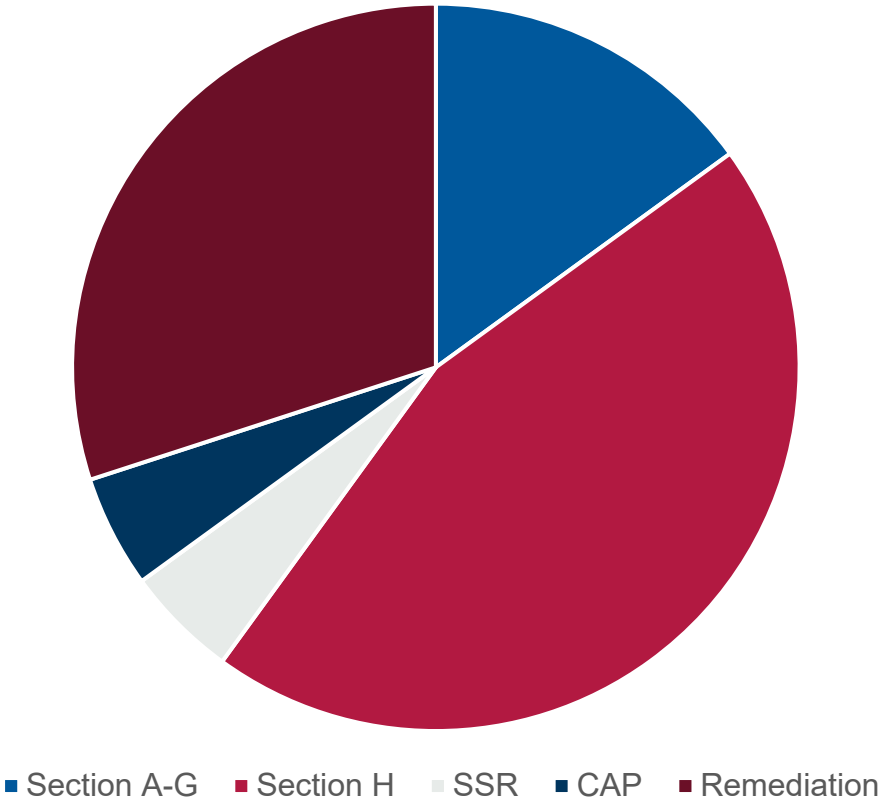
Risk Model Overview

The Risk model establishes a scoring technique that ranks and scores all agencies against one another based on their current risk posture.

Open Findings	Number of open findings weighted by issue code rating (e.g., 8 to 1). Integrated with device-level standardization which maps technologies back to SCSEM to identify a risk-based score of the existing open findings.
Reporting Compliance	Timeliness of last SSR and CAP submittals regarding due dates and extensions
Remediation	Criticality-weighted number of findings closed on time divided by the criticality-weighted total number of findings (accounts for CAP submissions/due dates)
End of Support Flag	Adjustment to overall score indicating that soon-to-be unsupported technologies are within the scope
Overall Score	Overall score is weighted sum of components and any adjustment (e.g., end-of-support Flag)

Risk Model Overview

Data scoring for the risk model



Section A-G – 15%

Section H - 45%

SSR Compliance – 5%

CAP Compliance – 5%

Remediation Closure – 30%

Risk Model Overview

Current risk treatment streams, including OOC reviews and (p)(7), put a heavy focus on open critical findings. This stands to reason because they're the most severe risk category and they should be closed within 3 months from being identified.

However, recent analysis is also starting to focus on open significant findings, which are the second most severe risk category and should be closed within 6 months from being identified.

Analysis on significant findings is underway and may lead to another treatment stream. A couple of initial observations include:

1. There are many agencies that have hundreds of open significant findings.

2. There are many significant findings that remain open more than 3 years.

Current Risk Treatment Streams Section

Current Risk Treatment Streams

Safeguards conducts quarterly out-of-cycle (OOC) reviews on high-risk agencies.

- Current review cycle is 3-years between reviews.
- Out-of-cycle reviews were implemented in FY2016.
- OOC reviews can be done remotely, onsite or part of a CAP review. OOC CAP reviews are not in lieu of the normal CAP, but in addition to it.
- Reviews enable regular communication and outreach with targeted high-risk agencies to make sure they follow detailed action plans.
- During OOC reviews, Safeguards helps agencies by addressing open findings, answering questions, providing guidance and ultimately lowering their overall risk with safeguarding federal tax information (FTI).

Current Risk Treatment Streams

Some criteria that helps determine if an agency is suited for an OOC review (remote, on-site, CAP) are:

1. Agencies normally ranked within the top of the output of the quarterly risk model

2. Instances of missed scheduled CAP and/or SSR submissions or a history of submissions being rejected

3. Agencies that haven't had a full review for more than one year and are not scheduled to have a review within six months

4. Agencies that have many open findings, especially critical and significant

5. Agencies that have a low rate of remediation, indicating a long period to close findings

Current Risk Treatment Streams

Open critical findings and end of support (EOS) technologies are emerging treatment streams to help lower the risk to FTI.

- Safeguards conducts quarterly reviews on a high-risk agency.
- The scope of these reviews is very limited and focuses on technologies that are out of support by vendors, have open critical findings and possibly some open significant findings.
- Due to the limited scope, Safeguards normally only needs a few meetings to work with the agency on the targeted discussion topics. The goal is to close as many findings as possible.
- Safeguards analyzes data from the quarterly risk model to identify potential high risk candidate agencies.
- Safeguards is conducting pilots for this treatment stream prior to full implementation.

Program Health Score Overview Section

Program Health Score

The current program health score analyzes data contained in e-Case on Safeguards partner agencies. Data input includes:

1. Open findings (critical, significant, moderate and limited)
2. Remediation scores (based on analysis of open CAP findings)
3. Reporting scores (based on analysis of timely SSR and CAP reports)
4. End-of-support technologies (based on the number of end-of-support flags)
5. Out-of-cycle flag, which indicates higher risk exposure in overall health score
6. Data incident flag, which indicates higher risk exposure in overall health score

The Program Health Score is based on known information that is continuously collected and reported. Future state would provide a more predictive and trend supportive model that gives insights into increased exposure and areas to allocate resources to help minimize risks to FTI.

Program Health Score

Knowing what contributes to the program health score is important. Agencies should understand what they can do to help promote and maintain a healthy program. Below are proactive steps:

1. Preparation: Utilize SCSEMS and perform continuous monitoring of physical controls; preventing findings is easier than mitigating them.

2. Reporting: Providing complete, accurate and timely reports (SSRs and CAPs) to Safeguards.

3. Remediation: When findings are identified during a Safeguards review (regardless if its an on-site, remote or OOC CAP review), the agency should mitigate them according to the Safeguards recommended remediation timelines.

4. Technologies: Do not let system and/or software technologies reach their end of support from the vendor; prepare and follow a timely product upgrade plan.

Program Health Score

Since the initial application of the risk model and program health score in FY16 Q1, there has been several positive outcomes that have helped in the overall protection of FTI throughout all agencies:

1. The risk model and program health scores have been used to identify high risk agencies for OOC reviews.

2. OOC reviews generate increased awareness and identification of potential (p)(7) issues, which if not fixed, could lead to a suspension of receiving FTI.

3. With assistance from Safeguard's personnel, improvements with agency reporting has helped with compliance efforts and overall improvement of health scores over the past two years.

4. A comparison of agencies eligible for an OOC review in FY20 Q3 and those eligible in FY21 Q3 demonstrate significant improvement in relative health at the individual agency levels.

(p)(7) Overview Section

(p)(7) overview

Internal Revenue Code (IRC) Section 6103

(p)(4) Requires external agencies and other authorized recipients of federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive.

(p)(7) Authorizes the IRS to take actions, including suspending or terminating FTI disclosures to any external agencies and other authorized recipients, if there is misuse, or if the safeguards in place are inadequate to protect the confidentiality of the information, or both.

(p)(7) overview

Criteria for agencies to fall under (p)(7)

1. Unauthorized Access or disclosure of FTI data
   A. Statute violations

2. Noncompliance with Safeguard requirements
   A. Constraint of on-site assessment
   B. Failure to correct findings categorized as critical risk
   C. Failure to submit required reports

(p)(7) overview

Below are common ways that (p)(7) criteria can be identified.

1. Regular on-site reviews
2. Remote assessment reviews
3. Out of Cycle (OOC) reviews

4. Through internal reviews of an agency's Safeguard Security Report (SSR) and/or CAP report

(p)(7) overview

Steps that occur after placing an agency under (p)(7)

1. Critical findings should be closed within 30 days of the (p)(7) Warning Letter from the Office of Safeguards.

2. Agency develops a remediation plan and shares it with Safeguards.

3. Safeguards conducts monthly status meetings with the agency to check progress in the remediation plan, answer questions, discuss issues etc.

4. The agency may request an extension if they can not mitigate and close all the findings within the original 30-day timeframe.

5. When findings are closed, the agency sends in the proper evidence (such as screen shots), Safeguards then validates them, and the (p)(7) can be closed.

Questions

Safeguard mailbox: SafeguardReports@irs.gov