SECURITYSTUDIO®

Vendor Risk Management

SECURITYSTUDIO

Security Experts on a **Mission**

Introductions

- Ryan Cloutier, CISSP®
- Principal Security Consultant for SecurityStudio®
  - Over 15 years of experience in Cybersecurity
  - Chairperson of COSN Cybersecurity program
  - Cybersecurity advisor to Student Data Privacy Consortium
  - Cybersecurity advisor to Global Education Privacy Standard
  - Certified Information Security Systems Professional®

Twitter @CLOUTIERSEC

What is vendor risk management

Vendor risk management (VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance.

Facts

59%

Companies had a third party data breach

- Ponemon

16%

Effectively managing third party risk

22%

Didn’t know if they had a third party breach

$3.9M

cost of third party data breach

Where to start

- Evaluation of the security and privacy practices of all third parties
- An inventory of all third parties with whom you share information
- Frequent review of third-party management policies and programs
- Third party notification when data is shared with Nth parties
- Oversight by the board of directors

What is in the contract?

- **Understand what's in the contract:**
  - The amount of help you can expect is relative to the terms of the contract

- **Key Questions**
  - When will we be notified of a security incident or breach?
  - Who will be responsible for notification?
  - What level of support can we expect?
  - Will there be compensation?

Who is responsible

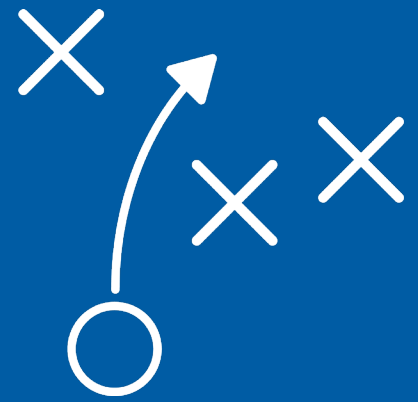
- **Appoint a vendor management lead**
- Have a vendor management team if possible
- Only one person in charge
- All vendors must be approved
- **Evaluate vendor RISK**

Questions for your vendors

- How do you manage risk?
- Will you allow a security audit?
- What insurance coverage is in place?
- Have you had a security event or breach in the last year?

Questions for your vendors

- How many logins do you have to our environment?
- How often are you connecting to our network?
- Who do you share our data with?



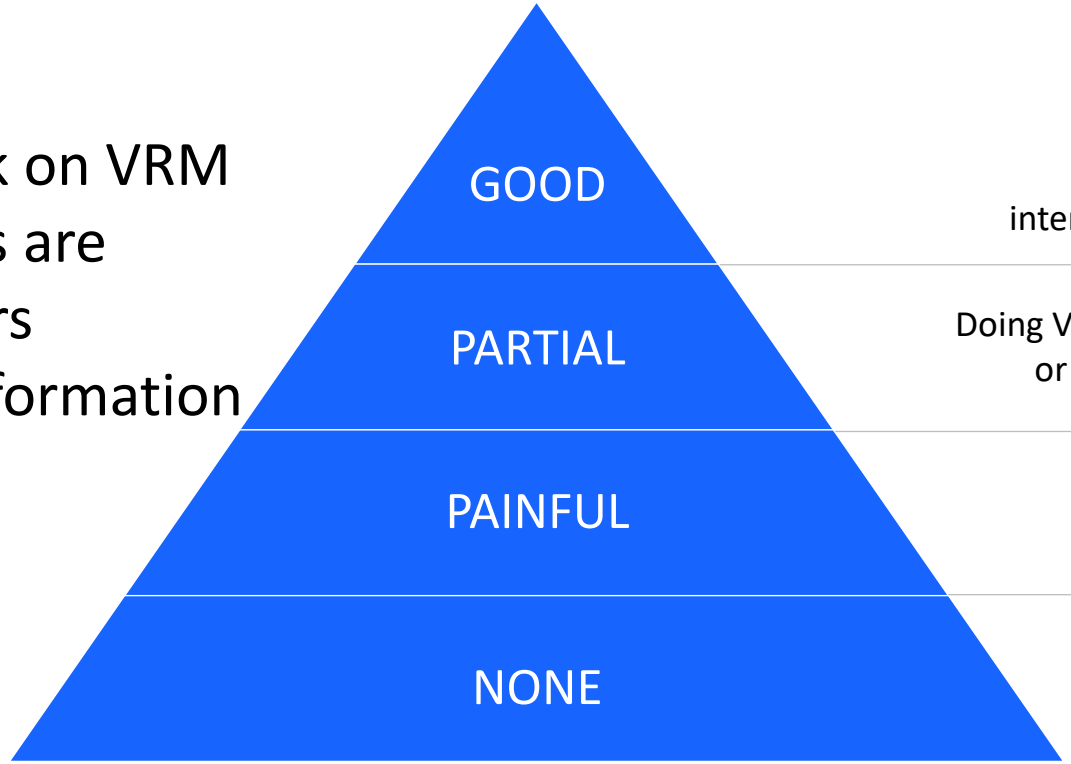
Four Approaches to VRM

Where Do You Fall?

Four Categories of Organizations

Common issues:

- Several people having to work on VRM
- Knowing who all your vendors are
- Categorizing 'high risk' vendors
- Gathering accurate vendor information
- Tracking and acting on results
- Keeping up with scheduling

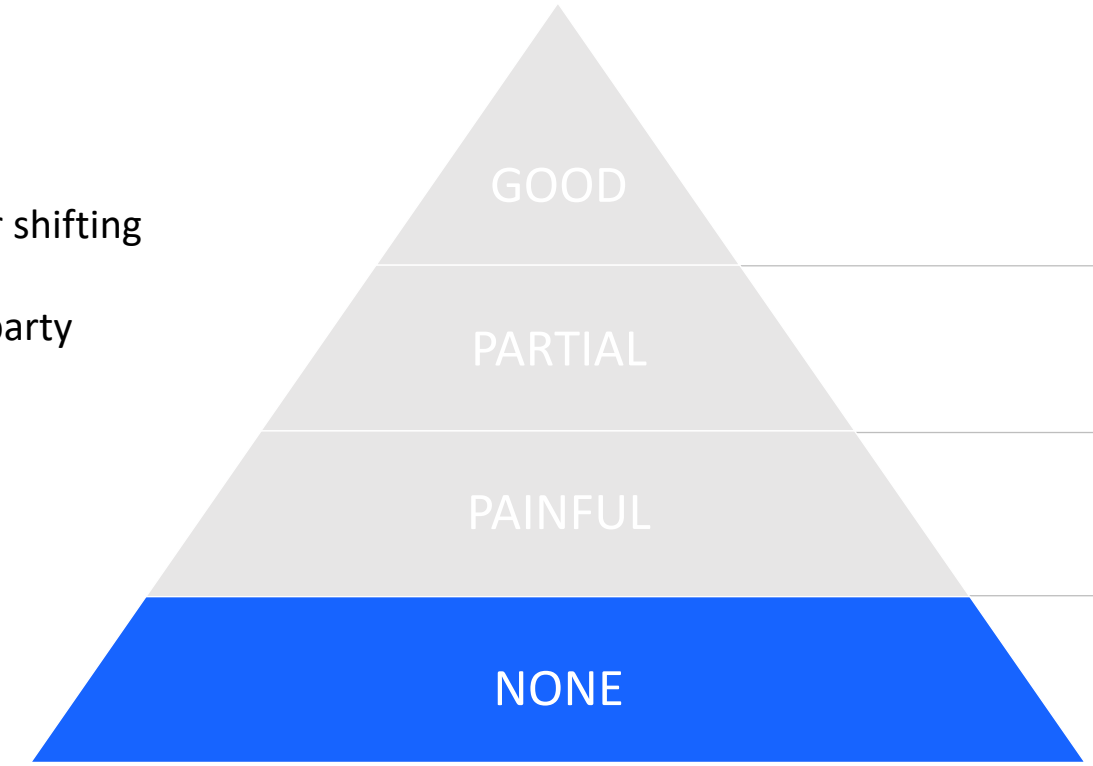


Where Do You Fall?

NONE

Several reasons, including:

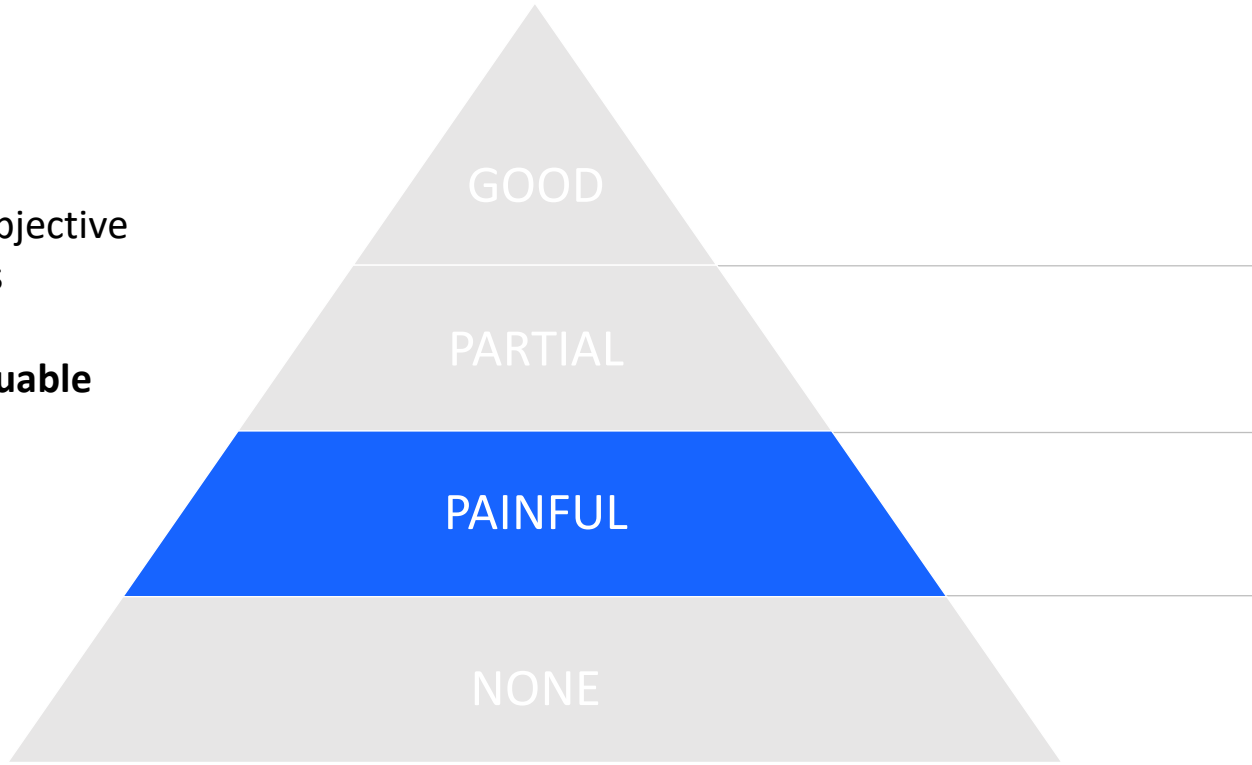
- You just didn’t/don’t know any better.
- You don’t know where to start.
- You’ve tried before and gave up due to complexity or shifting priorities.
- You don’t see the value in establishing a good third-party information security risk management program.
- You don’t have the time or money
- Executive Leadership do not feel it is a priority
- Other?



Where Do You Fall?

PAINFUL

- Trying to do VRM, but it's painful
- Want to do the right thing.
- Forced to do it.
- Usually manual, difficult to manage, disruptive and subjective
- Overall ineffective at managing risk and defensibility is variable.
- **The painful approach is expensive and a waste of valuable resources.**

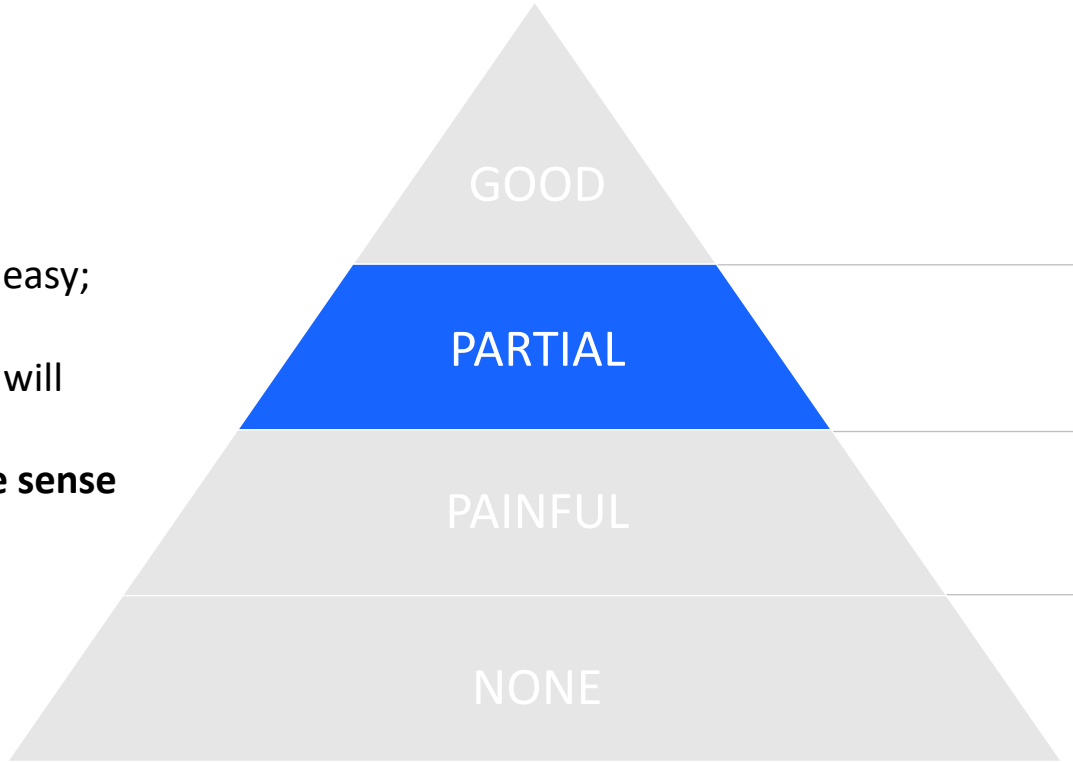


Where Do You Fall?

PARTIAL

- Only covers part of “information security”
- Information security is managing risk to information confidentiality, integrity, and availability considering administrative, physical, and technical controls.
- Typically focused on technical controls because they’re easy; however, aren’t people the greatest risk?
- Good at partial, but not likely to address how breaches will occur; partially defensible.
- **The partial approach is incomplete and leads to a false sense of security (sometime worse than no security at all).**

SecurityScorecard BITSIGHT riskrecon



Where Do You Fall?

GOOD

- Rare, but effective and streamlined.
- Doesn’t compromise on our definition of “information security”.
- **Simplified** – no unnecessary steps; easy-to-follow.
- **Standardized** – objective, same processes for all third-parties.
- **Defensible** – logical, organized, objective, auditable and completely effective.

Simplify: The Four-Phase Approach

The four Phases

Step 1

- Initial inventories can be a task, but the first time is the hardest.
- Import them into S2 Vendor®
- You are now managing vendor risk!

Step 2

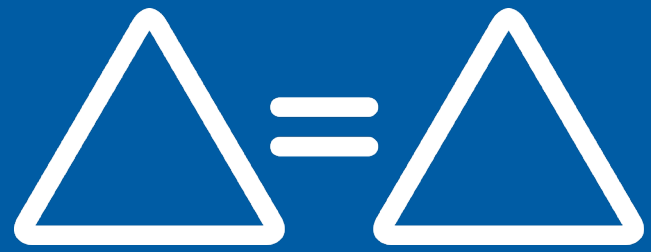
- Determine the impact the vendor/third-party can have on us (inherent risk)
- Simple and quick rules; 10 questions or less (configurable)
- Splits vendors/third-parties into Low/Medium/High buckets (configurable)

Step 3

- Determine the residual risk for vendors/third-parties who can impact our organization.
- Specific questions that represent risk, based on open standards like NIST and ISO
- Objective yes/no questions

Step 4

- Decide what you want to do: accept, remediate or reject.
- S2 Vendor® scores assessments, so we can set specific (and objective) thresholds.
- Build remediation plans with one click!



Standardize: One-Offs Hurt

Standardize

One-Offs Hurt

- Once we've established the standard process, don't deviate unless it's **absolutely** necessary.
- If deviations from the standard process must be done, make sure they're documented and signed off on.
- Each deviation from the standard process erodes defensibility.

Standardize

One-Offs Hurt

- Big vendors (Microsoft, Google, Amazon, etc.) may not participate in our VRM process; these are common deviations and are exceptions that can easily be explained away should something bad happen.
- Standardization comes through documentation, training, and automation. Every step in the process
  that **can** be automated **should** be automated.

Defensible: The True Motivation

Defensible

The True Motivation

- Defensibility in your VRM is arguably the most significant "**why**" for doing it in the first place.
- If/when something bad happens, **attackers** become customers, regulators, opposing counsel, etc.

Defensible

The True Motivation

- Ask yourself about defensibility constantly during VRM activities. Examples:
  - How many vendors do we have? Defensible?
  - How many high-risk vendors do we have? Defensible?
  - Have you vetted all high-risk vendors? Defensible?
- Non-definitive answers (assumptions, guesses, etc.) are more likely to be indefensible.

DIY, Or Get Help

DIY, Or Get Help

There's nothing wrong with doing VRM yourself

- The primary motivations for using tools or consultants are:
  - **Automation** of processes.
  - **Enforcement** of business rules on a consistent basis.
  - **Defensibility** is improved because you're using a tool developed by experts and one that is used by multiple organizations (herd mentality).
  - **Expertise** is doing this before, hopefully the right way.
  - Others…
- Try it yourself though, if you want. Here's our process in S2 Vendor®

DIY, Or Get Help

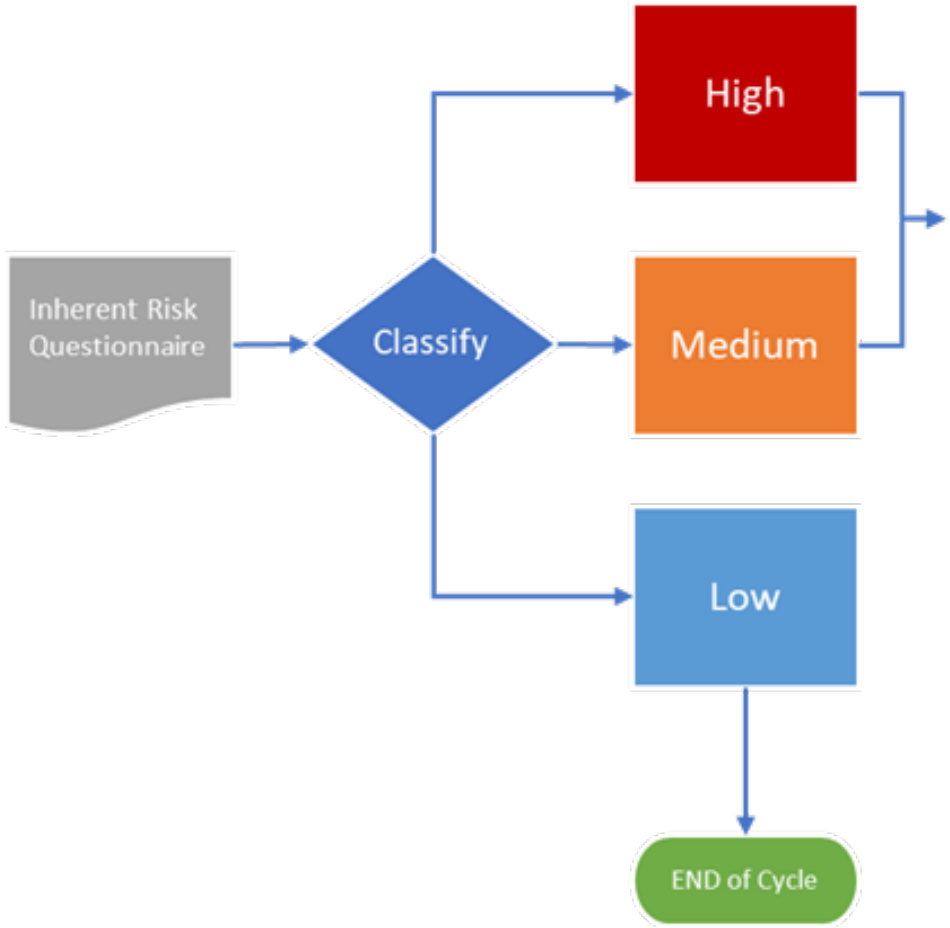
Phase 1

Inventory

Onboarding

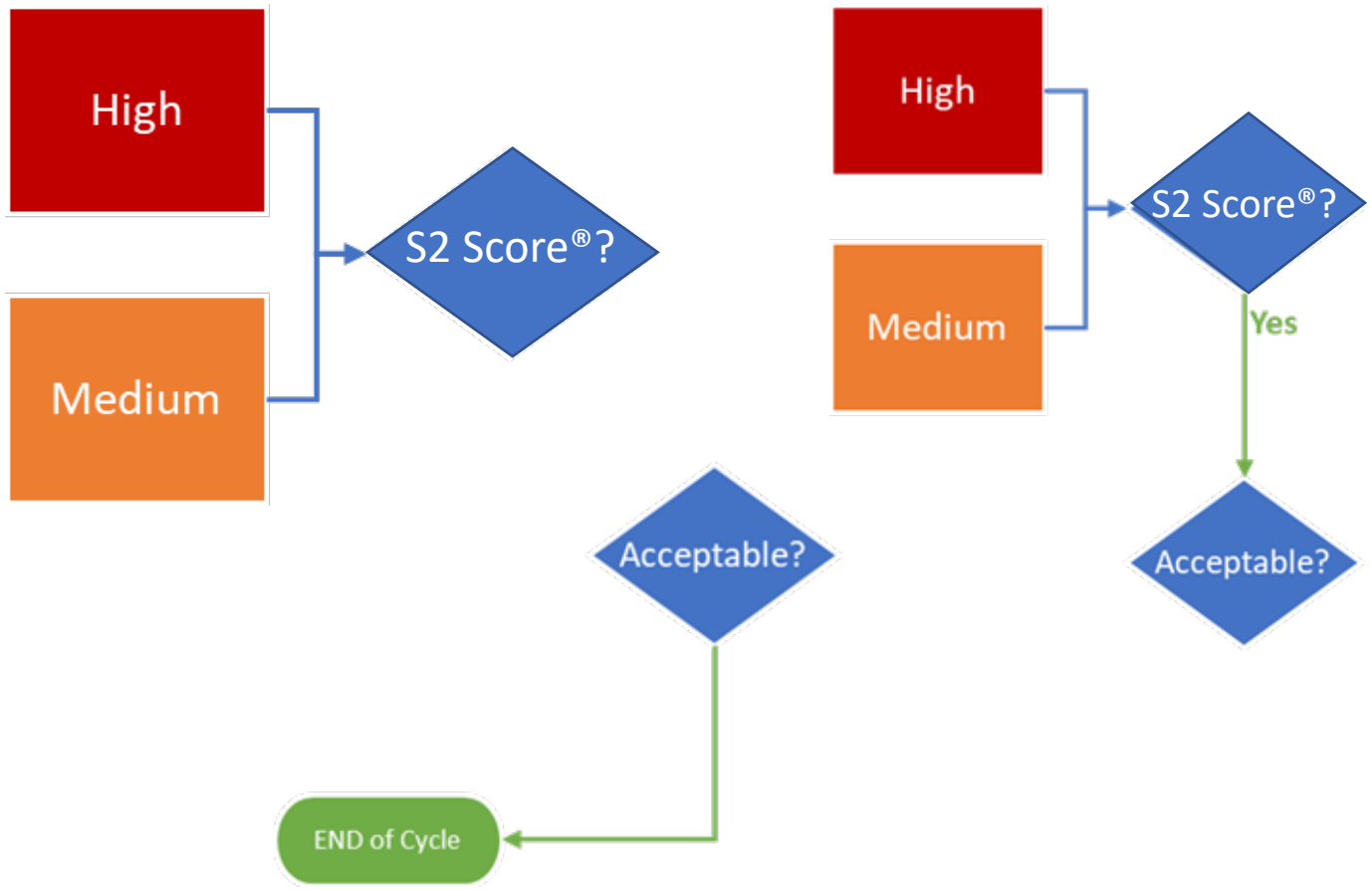
DIY, Or Get Help

Phase 2



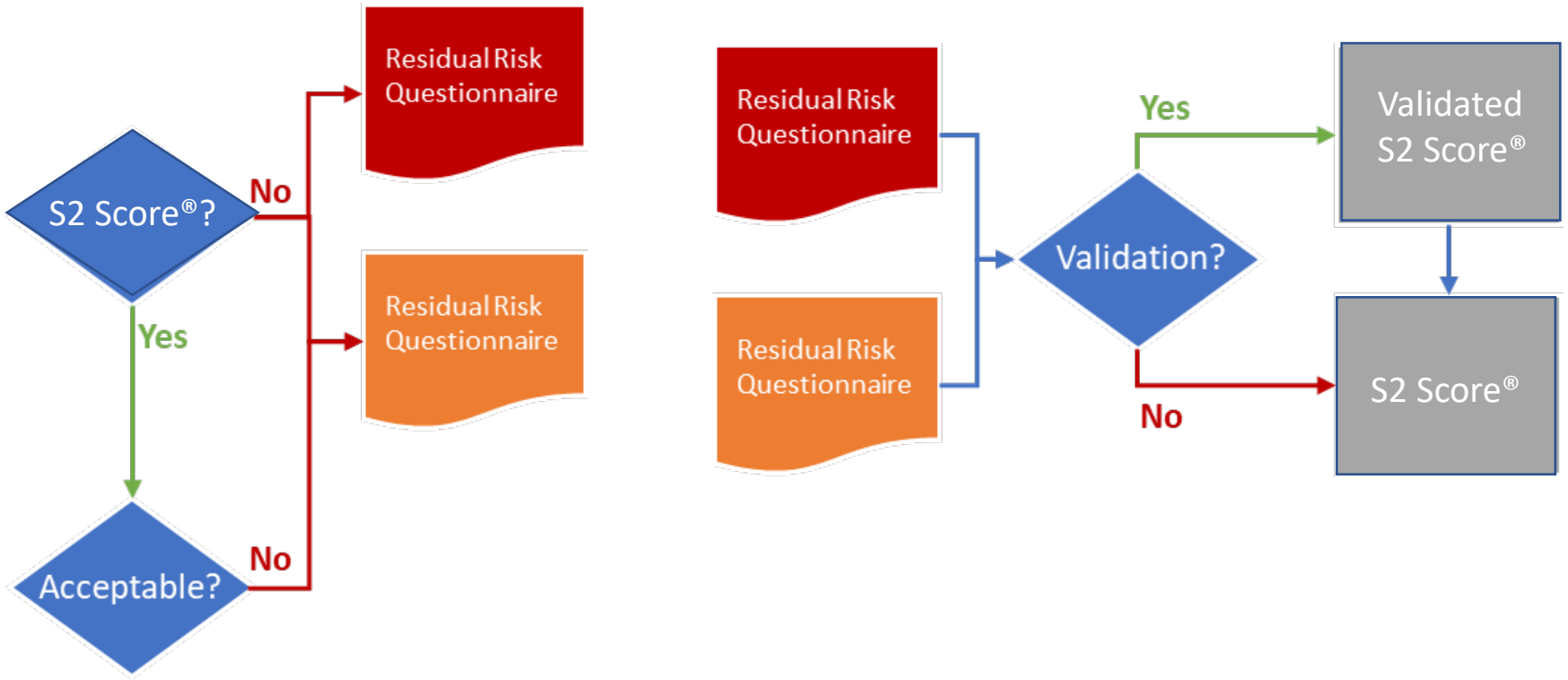
DIY, Or Get Help

Phase 3



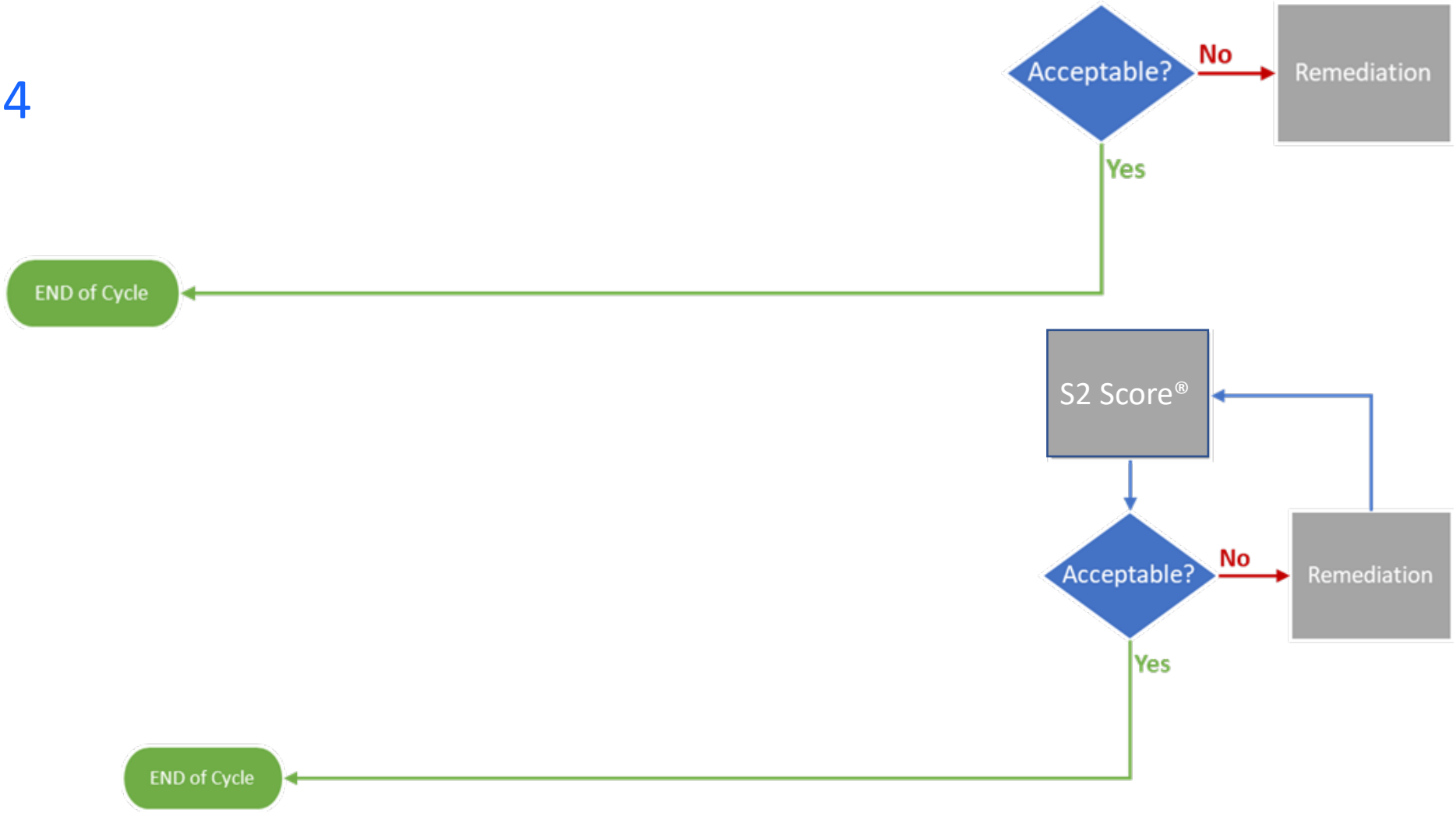
DIY, Or Get Help

Phase 3



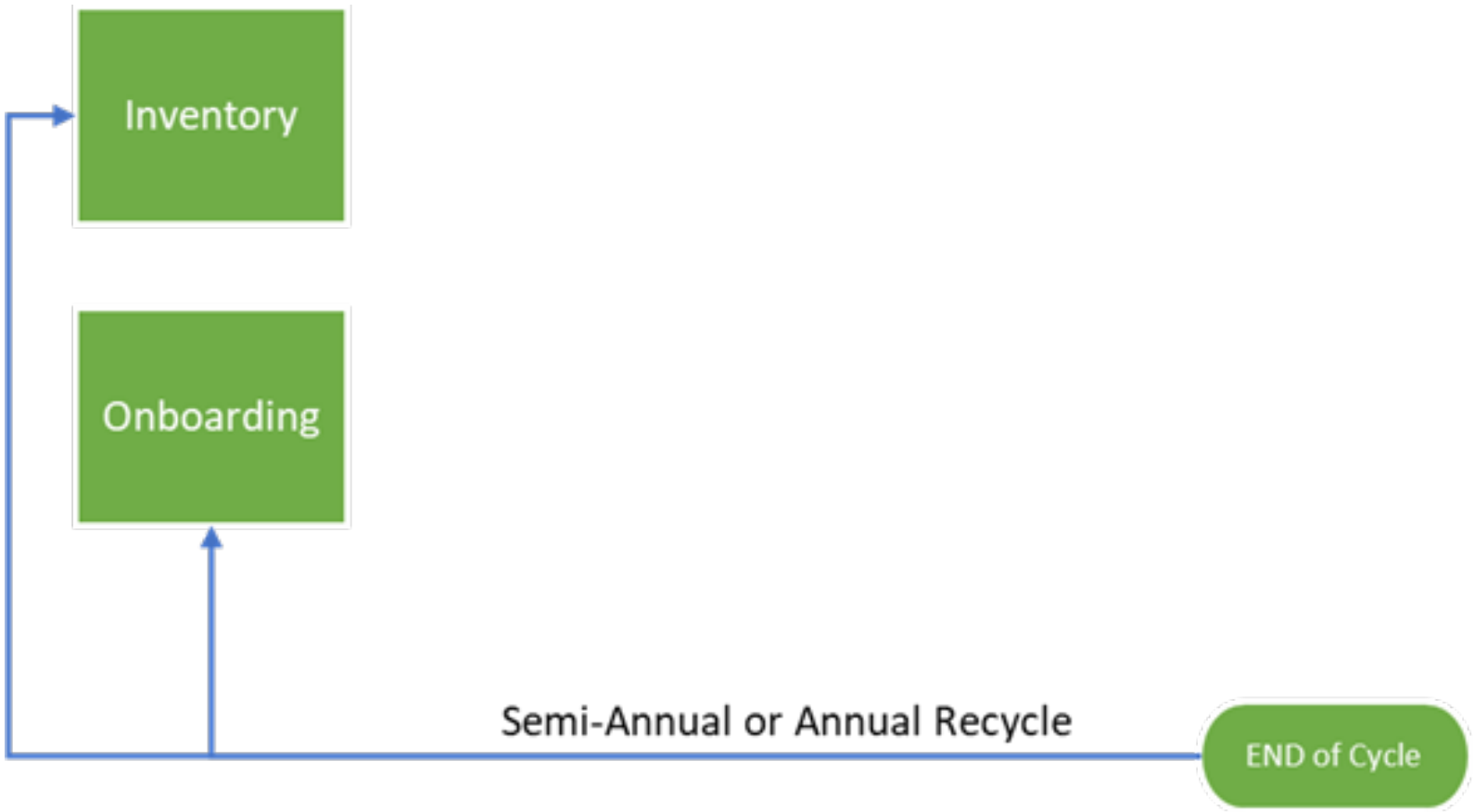
DIY, Or Get Help

Phase 4



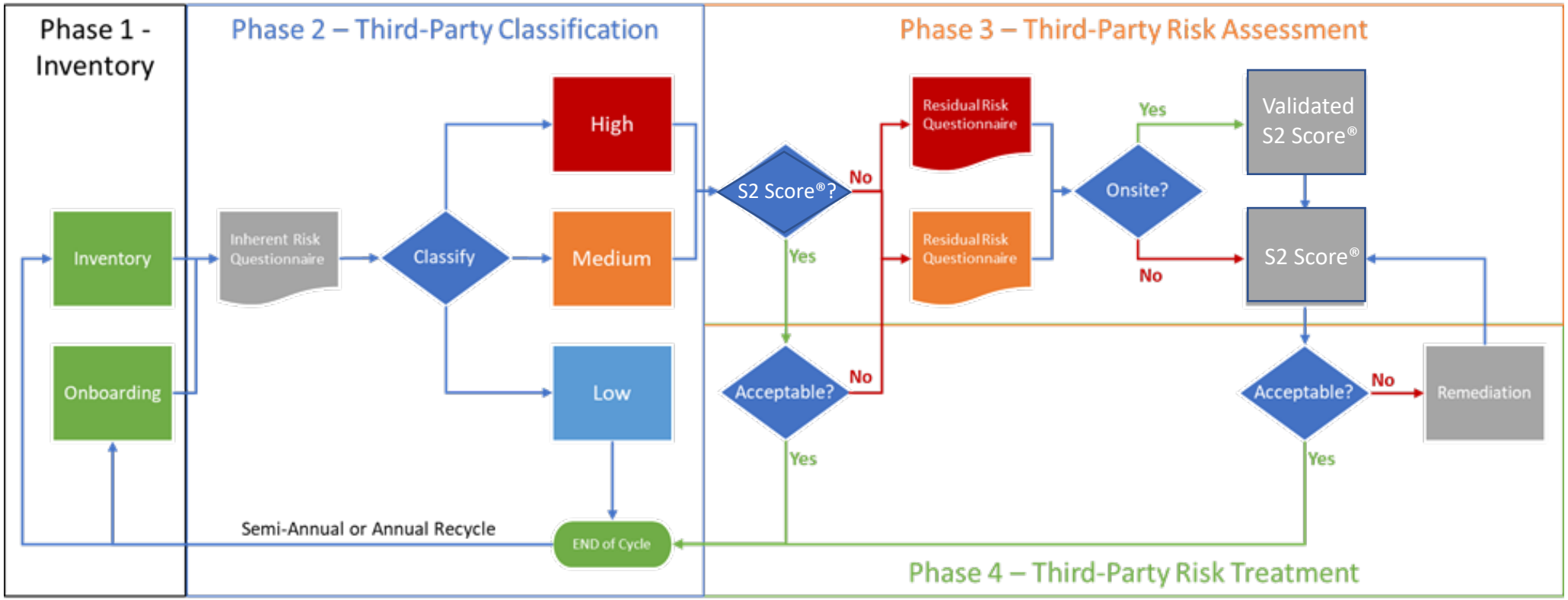
DIY, Or Get Help

Repeat



DIY, Or Get Help

Summary



Questions

InfoSaftey tools designed for People.

S²Score

Measure and communicate information security programs

S²Vendor

Manage 3rd party risk

S²Org

Assess information security programs and manage roadmaps

S²Team

Manage employee risk

Incident Response Retainer Services

Be protected from the storm, when your security disaster hits

Key Strengths

- Ethical
- Transparent
- Passion
- Mission

FRSECURE®

SECURITYSTUDIO®

How do you protect your family from cybercrime?