CSAMN cloud security alliance® Minnesota Chapter

FRSECURE®

Managing Third Party Risk Effectively

How to Conduct a 3rd Party Vendor Risk Assessment
Prior to Signing your Cloud Hosting Contract

Evan Francen, CEO & Founder of FRSecure

evan@frsecure.com

(877) 960-1814

Thank you to our sponsors!

TREND MICRO™

RELIAQUEST

Speaker Bio: Evan Francen

- Speaker: CEO & Founder of FRSecure and SecurityStudio (https://www.linkedin.com/in/evanfrancen/)
- Co-inventor of SecurityStudio®, FISA™, FISASCORE® and Vendefense®
- 25+ years of “practical” information security experience (started as a Cisco Engineer in the early 90s) Author of UNSECURITY
- Developed the FRSecure Mentor Program; six students in 2010/497 in 2019
- Dozens of television and radio appearances; numerous topics
- Advised legal counsel in very public breaches (Target, Blue Cross/Blue Shield, etc.)

Agenda

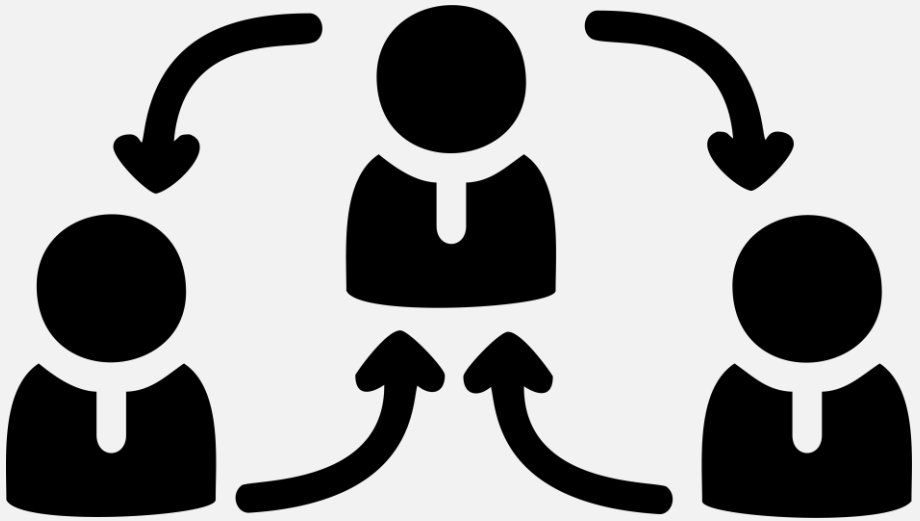
- Why should you care about your vendors?
- Four approaches to VRM
- Standardize
- Defensible
- Learning Takeaways:
  - Driven by Risk Management Program
  - Part of Contracts & Administration
  - Use SIG LITE or Equivalent
  - Review the MSA Contract for Liabilities
  - Align Risk Accordingly

NOTE: I'm a literal person. If you are too, you might notice "VRM". Vendor Risk Management (VRM) is not the same as third-party information security risk management (TPISRM).

One sort of fits into the other. We're talking about TPISRM, but for the sake of brevity, we sometimes use VRM and TPISRM synonymously.

BEFORE WE GO MUCH FURTHER…

Why should you care about your vendors?



Most of us have seen the stats…

- **69%** of respondents say they definitely or possibly suffered a security breach resulting from vendor access within the last year.
- On average, organizations spent **$10 million** responding to third-party breaches over a 12-month period in 2016.
- **63%** of all cyber attacks could be traced either directly or indirectly to third parties.
- Nearly **97%** of respondents said that cyber risk affecting third parties is a major issue.
- Nearly **80%** of respondents said they have terminated or would decline a business relationship due to a vendor's cyber security performance.

Sources: Bomgar survey, PwC, Soha Systems, CSO Online

But…

- Only **35%** of enterprise security professionals are very confident in knowing the actual number of vendors accessing their systems.
- Only **52%** of companies have security standards for third-parties.
- Just **34%** know the number of individual log-ins that can be attributed to vendors.
- **1 in 10** organizations has a role specifically dedicated to vendor, third-party or supplier risk
- No sector reported more than **50%** of respondents at a mature level with regard to managing vendor risk

Sources: Bomgar survey, PwC, Soha Systems, CSO Online

The reality is…

- We're all tired of statistics and studies.
- Most statistics and studies are commissioned by someone who wants to sell us something.
- There's a thing called "confirmation bias".
- We've all got 1,000 things on our plate.
- You won't do anything (significant) about third-party security risk management unless **you want to** or you've been told **you have to**.
  - You might want to because you understand risk and this is your next significant unacceptable risk. (could be other reasons)
  - You have to because it's the law (or the interpretation of the law).

The reality is…

You should care, right?

Yes, you should. You should care enough to understand the problem (assuming you have one) and make an educated decision on what, if anything you plan to do about it.

Figure out your "WHY".

Doing nothing will imply risk acceptance.

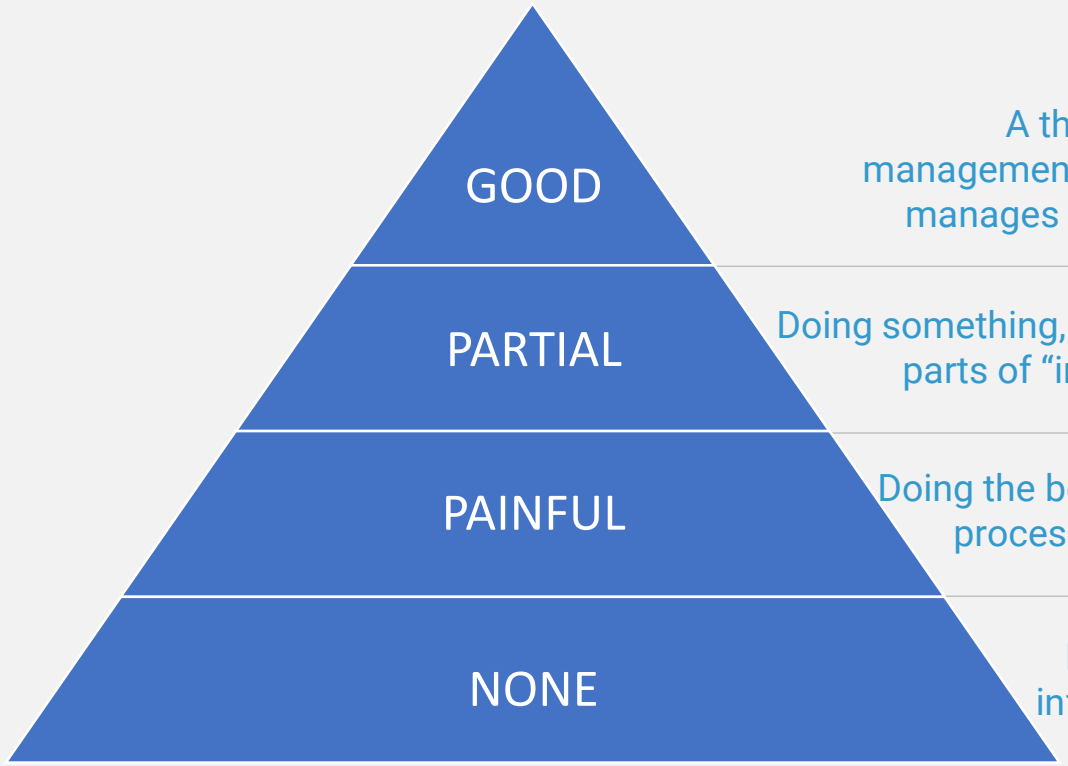
FOUR APPROACHES TO VRM

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



A third-party information risk management program that efficiently manages information security risk.

Doing something, but missing one or more parts of "information security risk".

Doing the best they can with manual processes. Think spreadsheets.

Not managing third-party information security risk at all.

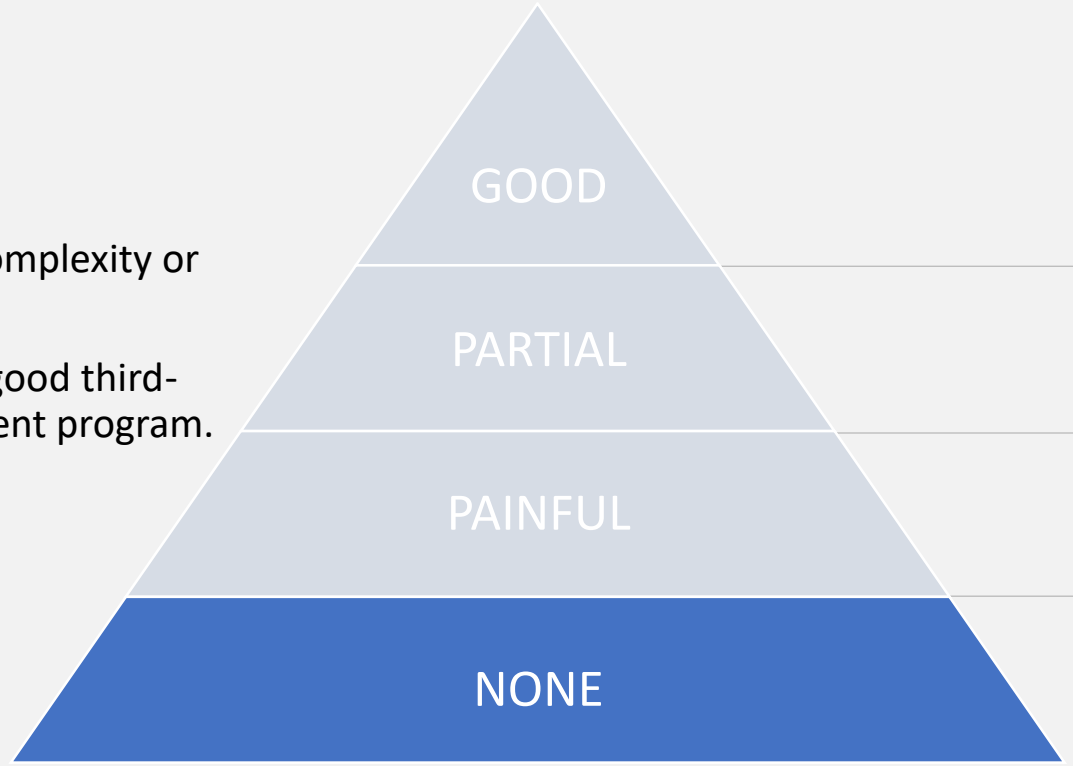
CSAMN cloud security alliance® Minnesota Chapter

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?

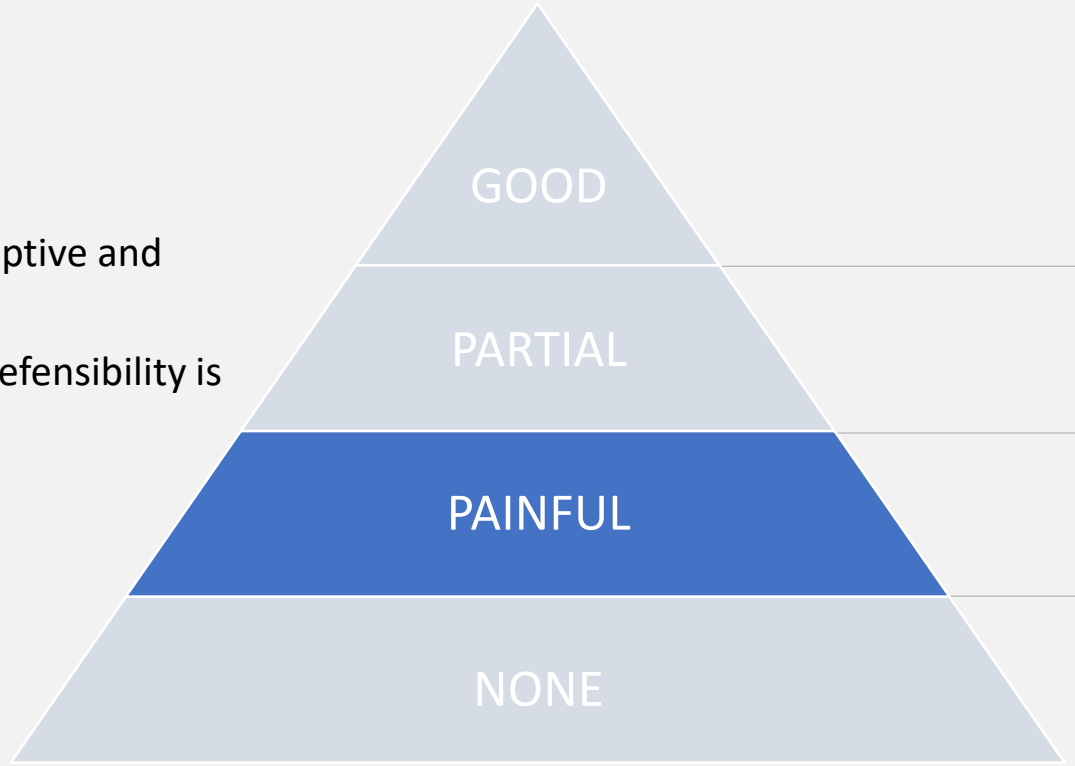


CSA MN cloud security Minnesota Chapter alliance®

WHERE DO YOU FALL?

PAINFUL

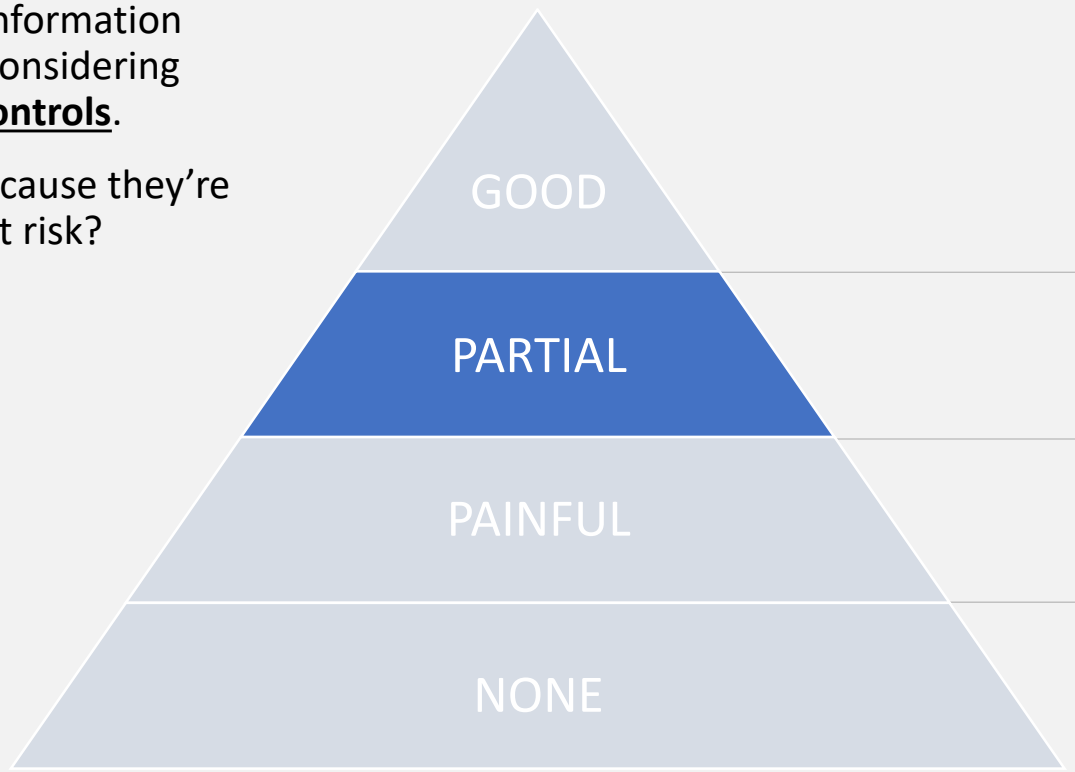
- Trying to do VRM, but it's painful
- Want to do the right thing.
- Forced to do it.
- Usually manual, difficult to manage, disruptive and subjective
- Overall ineffective at managing risk and defensibility is variable.
- **The painful approach is expensive and a waste of valuable resources.**



WHERE DO YOU FALL?

PARTIAL

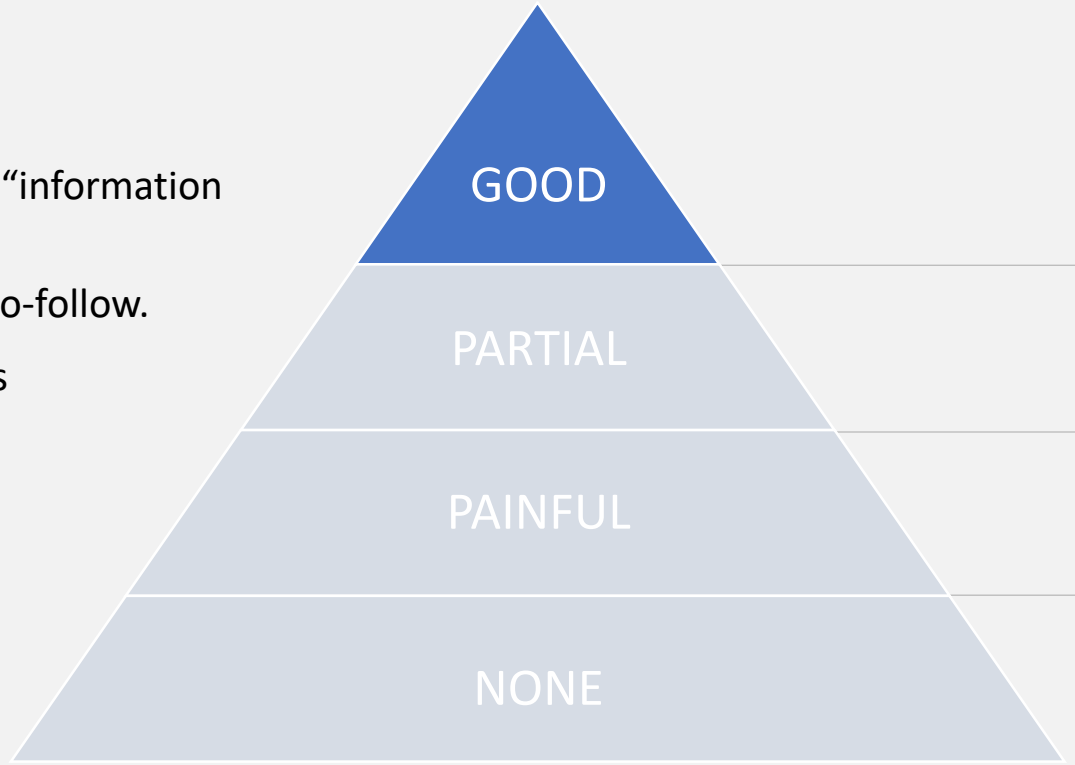
- Only covers part of “information security”
- Information security is managing risk to information confidentiality, integrity, and availability considering **administrative, physical, and technical controls**.
- Typically focused on technical controls because they’re easy; however, aren’t people the 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).**



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.

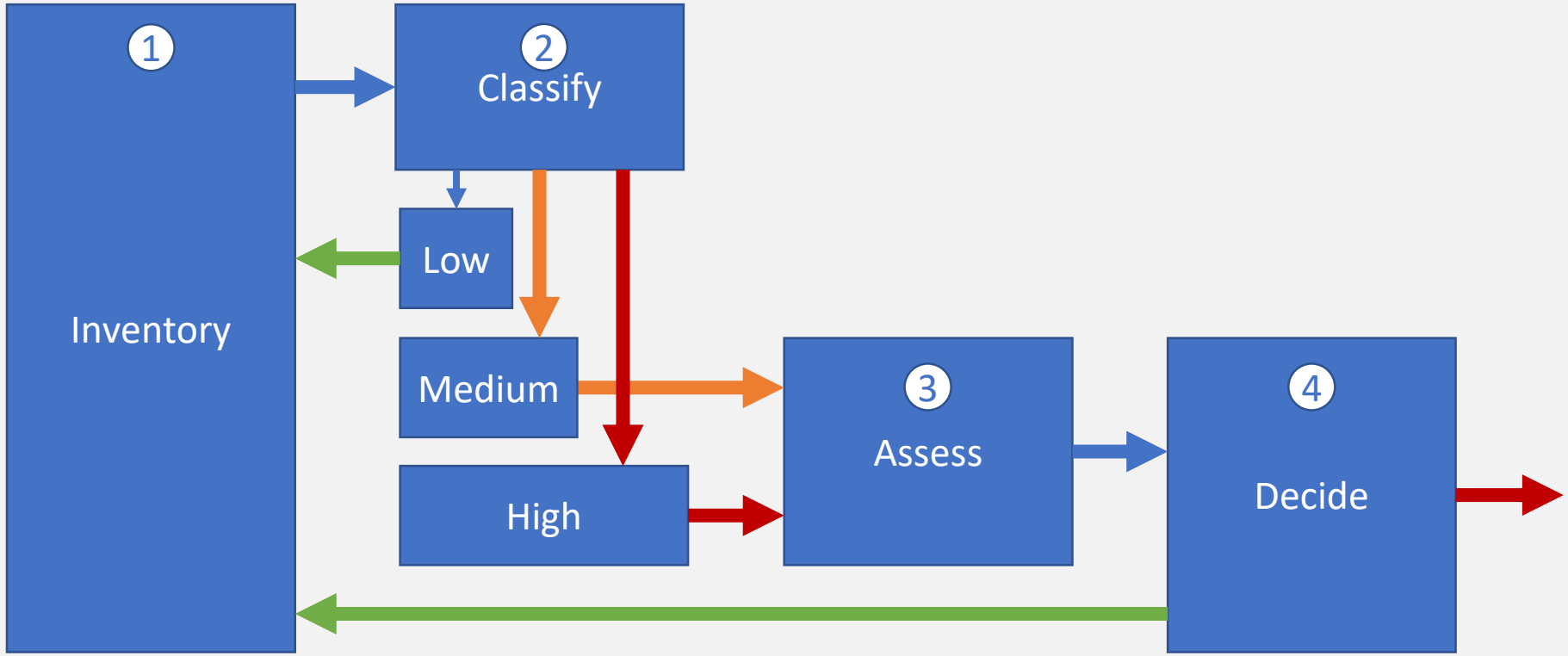


SIMPLIFY

Don’t over-complicate the matter, there are only four steps…

1. **Inventory (and inventory management)**
   - You’re paying them; existing third-parties.
   - You’re engaging them; new third-parties, procurement.
2. **Classify (inherent risk)**
   - Risk without control.
   - High, Medium, Low is fine. Don’t waste your time with the low-risk vendors, just cycle them. If you’re doing it right, the ratios (with exceptions) are typically 5/10/85.
3. **Assess (residual risk)**
4. **Decide (risk decisions)**
   - Scores and thresholds work best
   - Accept/Mitigate/Transfer(unlikely)/Avoid

SIMPLIFY

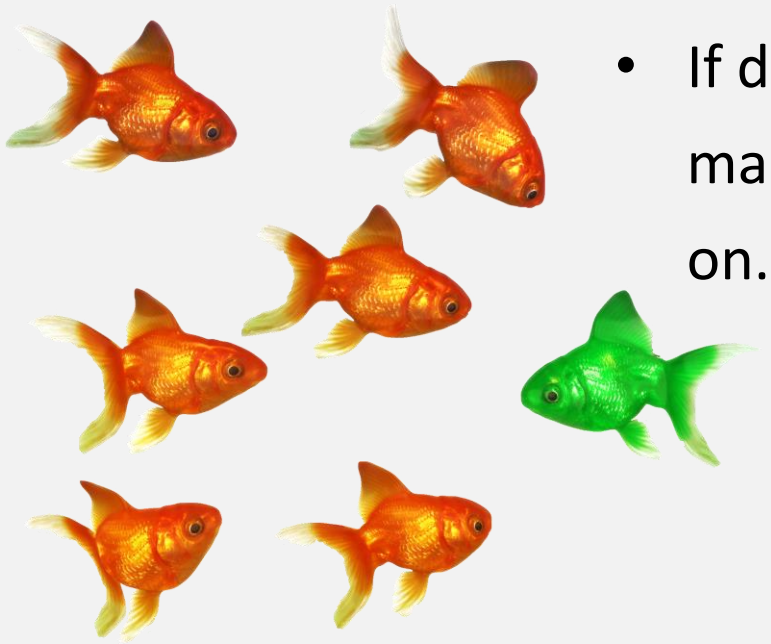


STANDARDIZE

One-Offs Hurt

STANDARDIZE

- Once we've established the standard process, don't deviate unless it's **absolutely** necessary.

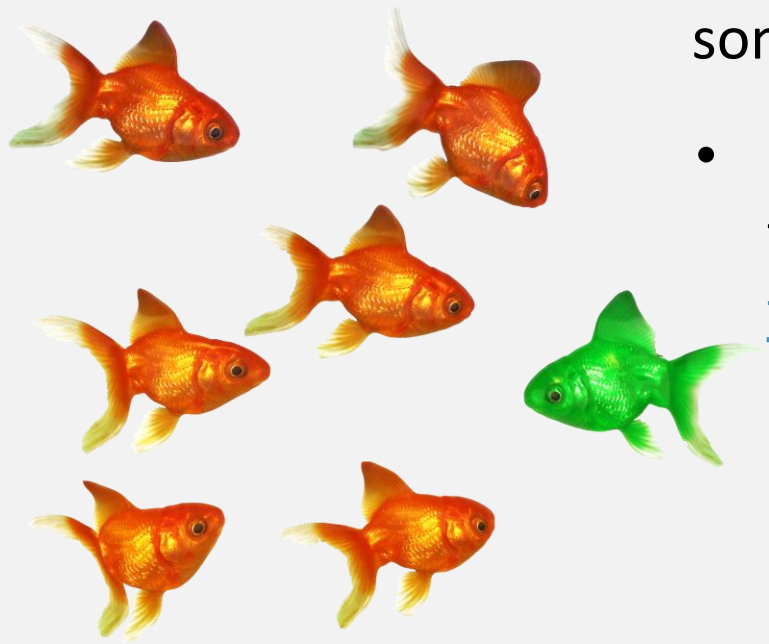


- If deviations from the standard process must be done, make sure they're **justified**, **documented** and **signed off** on.
  - Each deviation from the standard process erodes defensibility.

CSAMN cloud security Minnesota Chapter alliance®

STANDARDIZE

- Big vendors (Microsoft, Google, Amazon, etc.) may not participate in our process; these are common deviations and are exceptions that can easily be explained away should something bad happen.



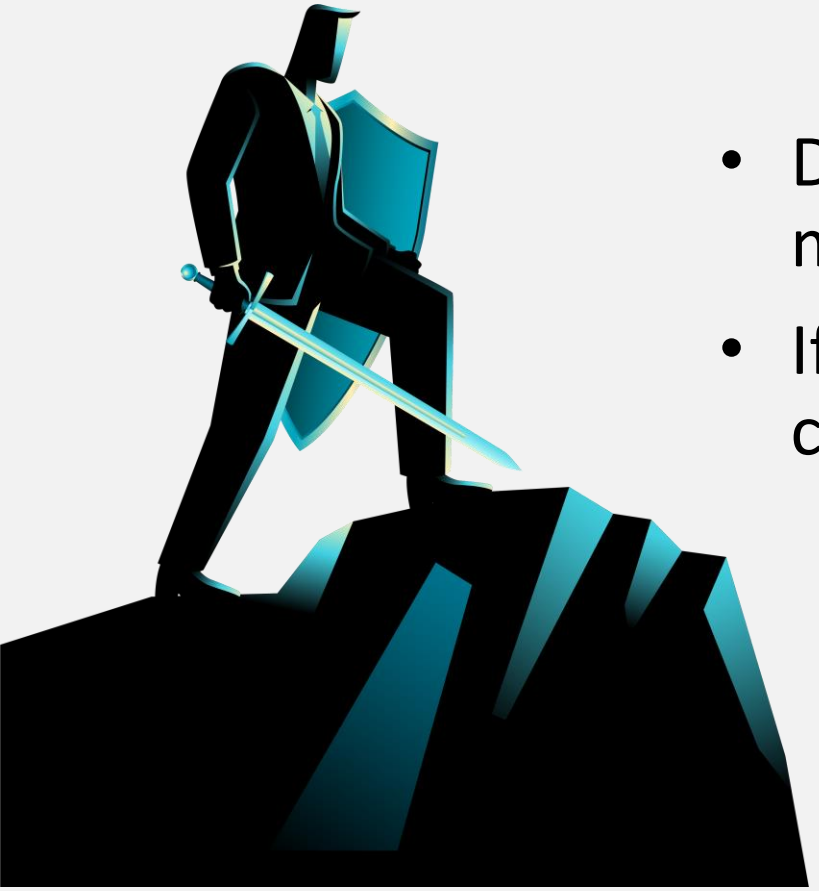
- Standardization comes through documentation, training, and automation. Every step in the process that **can** be automated **should** be automated.

DEFENSIBLE

The True Motivator

Full Transparency: This would be my motivator.

The True Motivation: Defensibility



- Defensibility in your VRM practices 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.

The True Motivation: Defensibility

- If defensibility is your “**why**”, ensure that it’s carried out in your “**how**” and “**what**”.

Do you have answers to these questions?

- **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.

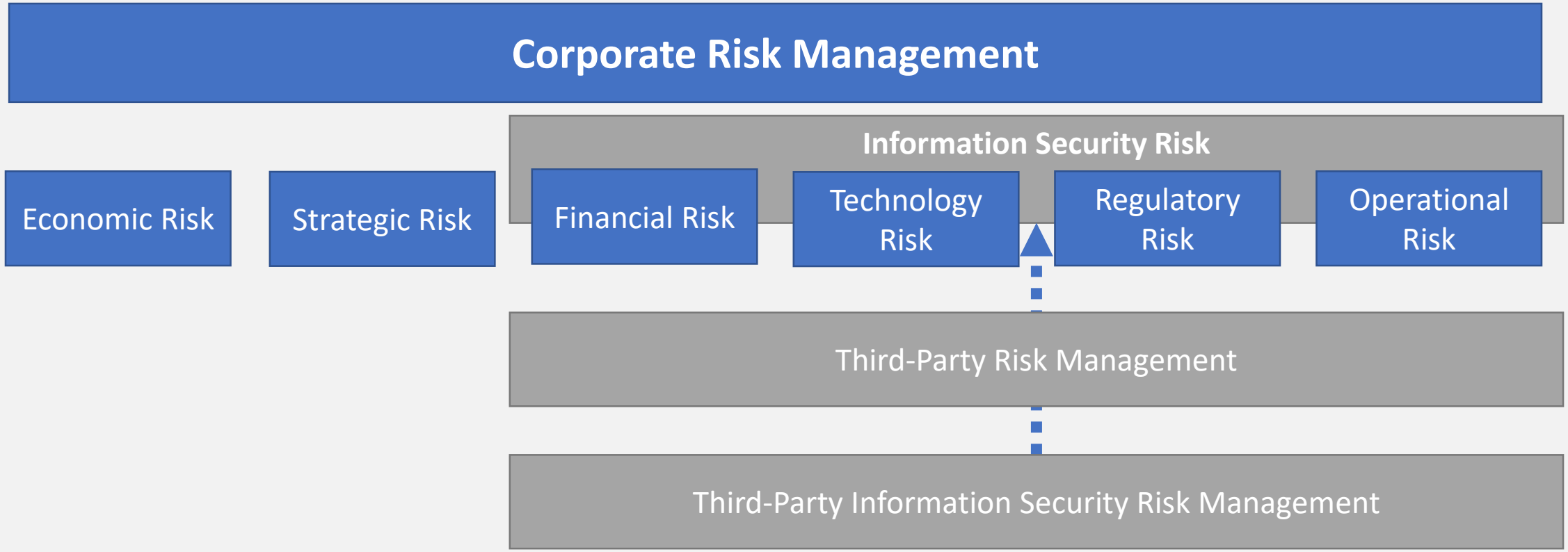
Learning Takeways

Driven by the Risk Management Program.

- You have a risk management program, right?
- Where does third-party information security risk management fit into risk management?
- No two risk management programs are the same, but in general:
  - **Third-party information security risk** is a subset of:
    - Third-party risk management (in procurement or other), which is a subset of:
      - Supply chain, operational, and/or financial risk management.
    - Information security risk management, which is a subset of:
      - Corporate risk management

Learning Takeways

Driven by the Risk Management Program.



Learning Takeaways

What about the assessing 3rd-party cloud providers?

This is CSA after all?!

- Inventory and inherent risk questions and ratings don't change (usually).
- Residual risk is where things change, because it's where controls change.
- The Cloud Security Alliance Consensus Assessments Initiative (CAI)
  - Launched to perform research, create tools, and develop industry partnerships
  - Enable cloud computing assessments
  - Developed the Consensus Assessments Initiative Questionnaire (CAIQ), often pronounced "CAKE".
- Do residual risk assessment and make decisions **before signing contracts or agreements (unless there are stipulation)**.

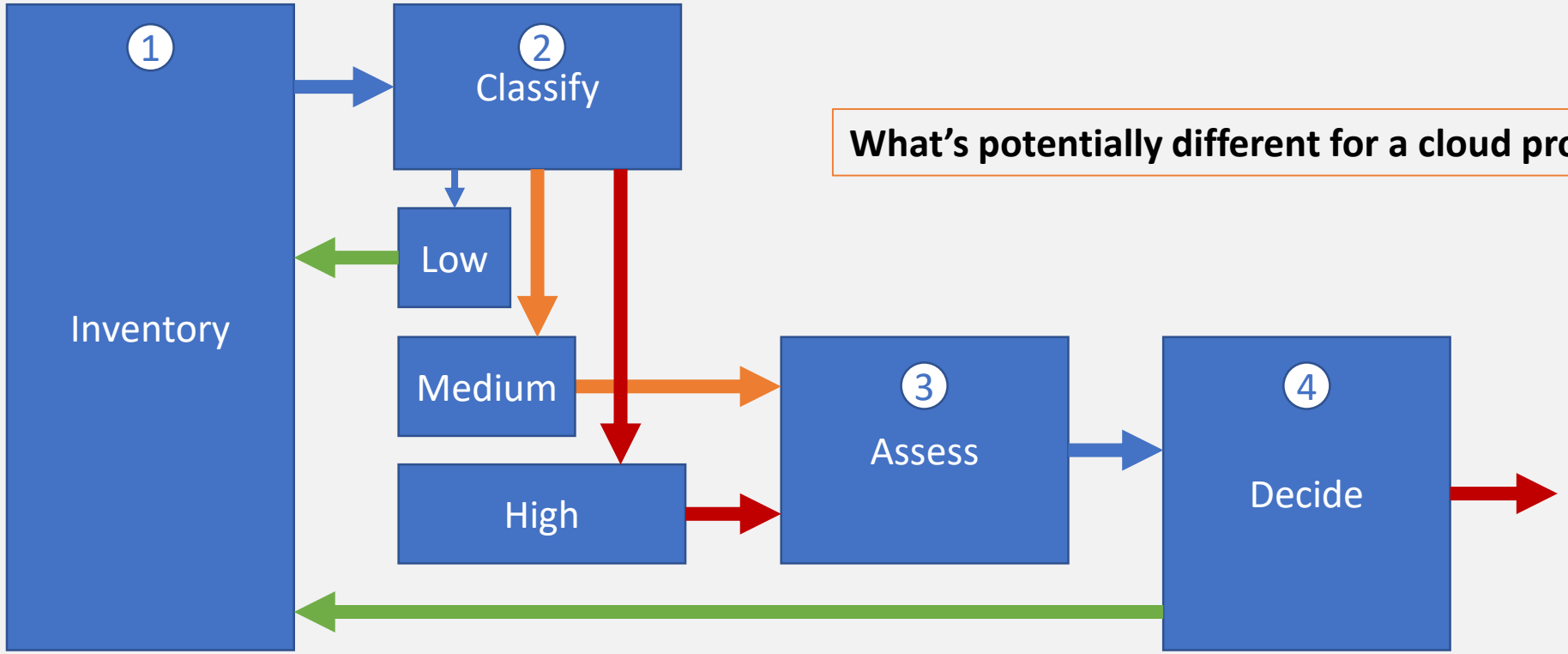
Learning Takeaways

More information about STAR:
https://cloudsecurityalliance.org/star/#_overview

One way to assess cloud providers (High/Medium Risk)

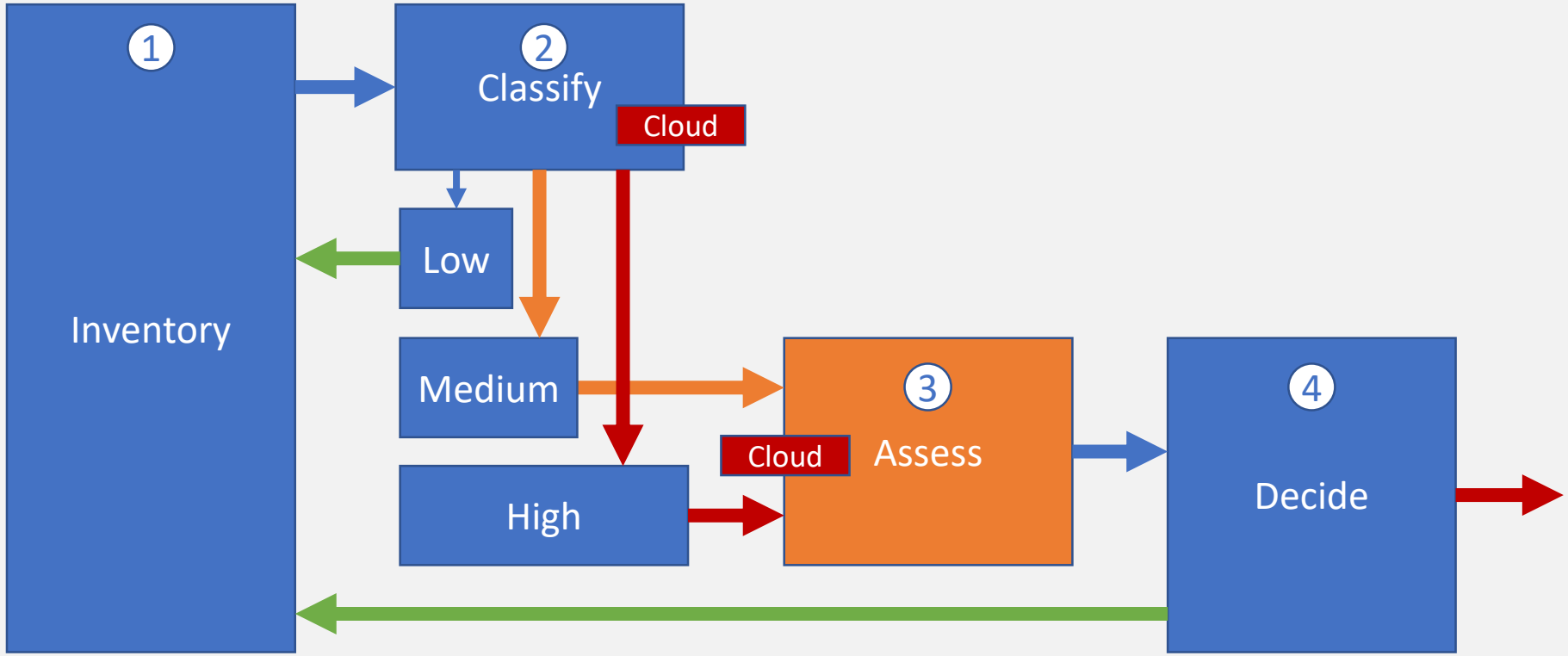
- **Check the STAR Registry** (https://cloudsecurityalliance.org/star/registry)
  - Based on CAIQv3.01
  - Self-Assessment, Certification, or C-Star (a little more to it than this)
  - Create a scoring methodology or review for KRIs.
  - Not acceptable or not present…
- **Use the CSA CAIQ as is or customize:**
  - https://cloudsecurityalliance.org/articles/consensus-assessments-initiative-questionnaire-caiq-v-3-review/
  - https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/
  - Develop scoring methodology and/or identify KRIs.

SIMPLIFY

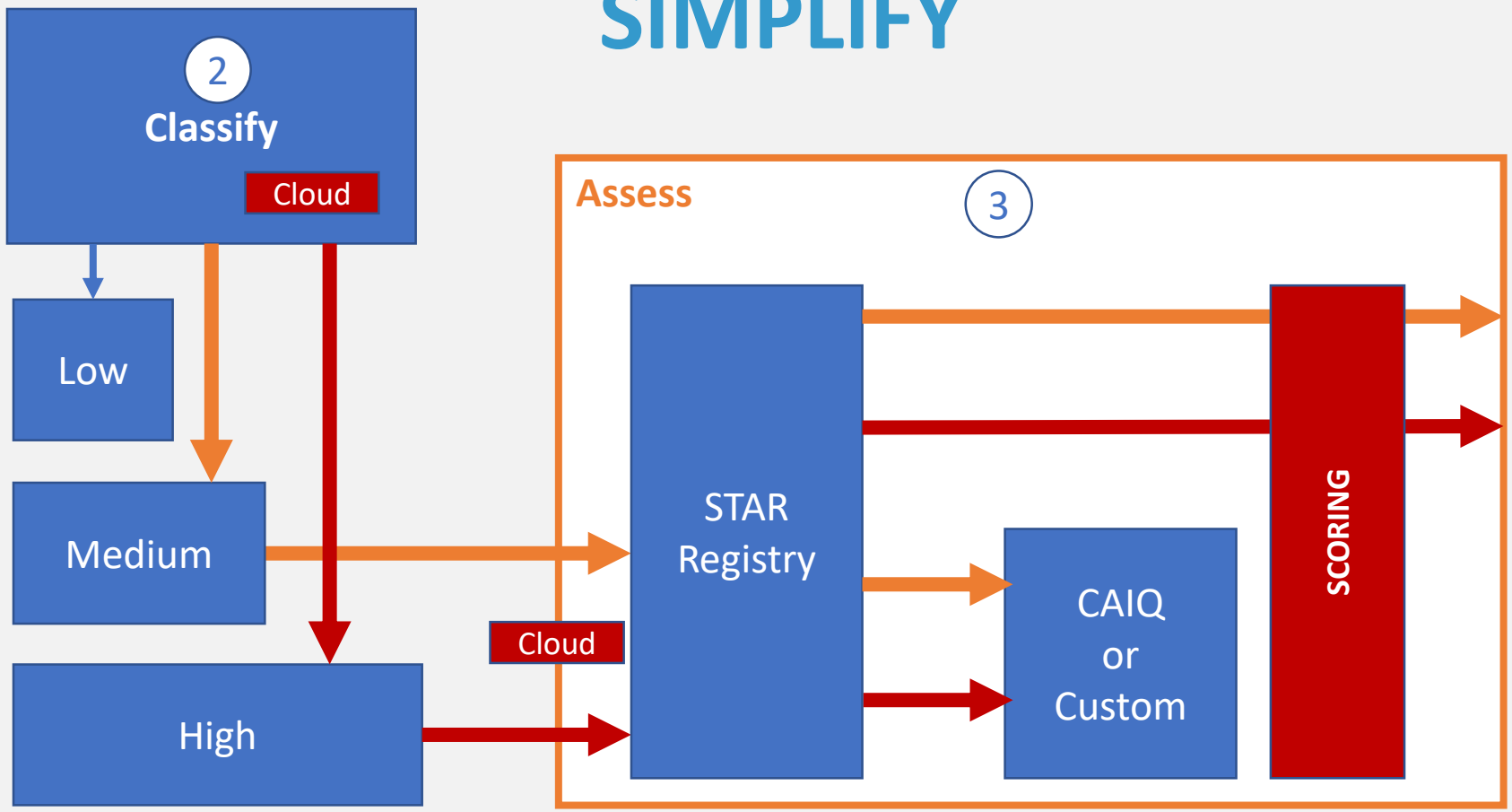


What's potentially different for a cloud provider?

SIMPLIFY


1
Inventory
2
Classify
Cloud
Low
Medium
High
3
Cloud
Assess
4
Decide

SIMPLIFY


2
Classify
Cloud
Low
Medium
High
Cloud
Assess
3
STAR
Registry
CAIQ
or
Custom
SCORING

Learning Takeaways

Part of Contracts & Administration

- How will you enforce/demand/request that a third party comply with your requirements?
- No third-party access/use until contract negotiation is complete.
- Must haves:
  - Risk assessment
  - Right to audit (try exercising it sometime, build the process 1st)
  - Incident notification and process

Learning Takeaways

Use SIG LITE ~~or Equivalent~~

- For assessing residual risk.
- 71% of organizations use a custom risk assessment methodology and/or assessment.
- SIG – Shared Assessments - https://sharedassessments.org/sig-faq/
- Not free.

Designed to provide a broad but high-level understanding about an Assessee's internal information security controls. This level is for Assessees that need a basic level of due diligence. It can also be used as a preliminary assessment before a more detailed review. – Santa Fe Group

Learning Takeways

Use SIG LITE or Equivalent

- For assessing residual risk.
- 71% of organizations use a custom risk assessment methodology and/or assessment.
- SIG – Shared Assessments - https://sharedassessments.org/sig-faq/
- Not free.

Designed to provide a broad but high-level understanding about an Assessee's internal information security controls. This level is for Assessees that need a basic level of due diligence. It can also be used as a preliminary assessment before a more detailed review. – Santa Fe Group

Level	Description	Risk Control Focus	Example Function and Systems Types	Example Data Types
LITE	Designed for organizations with non-critical functions, data and/or systems.	Baseline controls – to address risks and threats with low (inherent) risk functions, data and/or systems.	• Hosting web site • User control of application security • Test and Development environments • Simulation • Non-business critical systems	• Web site hosting public information • Obfuscated data
CORE	Designed for organizations that run business critical functions, data and/or systems.	Stringent controls - to address internal vulnerabilities and external threats.	• Business critical systems • Business critical data • Business critical Functions	• Personally Identifiable Information (PII) • Email • Customer Relationship Management (CRM) • Credit Card Data (PCI) • Protected Health Information (PHI) • Merger/Acquisition Information
FULL	Designed as a library of potential situation-specific additions to a CORE or LITE SIG that address best practices and industry or service-specific requirements. Shared Assessments does NOT recommend sending an un-scoped FULL SIG to an Assessee.	Best Practice controls - to address the highest levels of (inherent) risk and advanced persistent threats.	Includes all of the above in addition to any additional organization specific requirements.	Includes all of the above in addition to any additional organization specific requirements.
MASTER	All of the SIG questions are displayed and two additional columns for Optional Scoring and Question Level information are provided. This level is used to create a Master SIG; a repository of the completed SIG questions and answers that an Outsourcer expects to receive from an Assessee(s). A Master SIG documents what the Outsourcer feels should be the correct answer for each question. It also lets the Outsourcer document the relative importance of each question.			

Learning Takeaways

Use ~~SIG LITE or~~ Equivalent

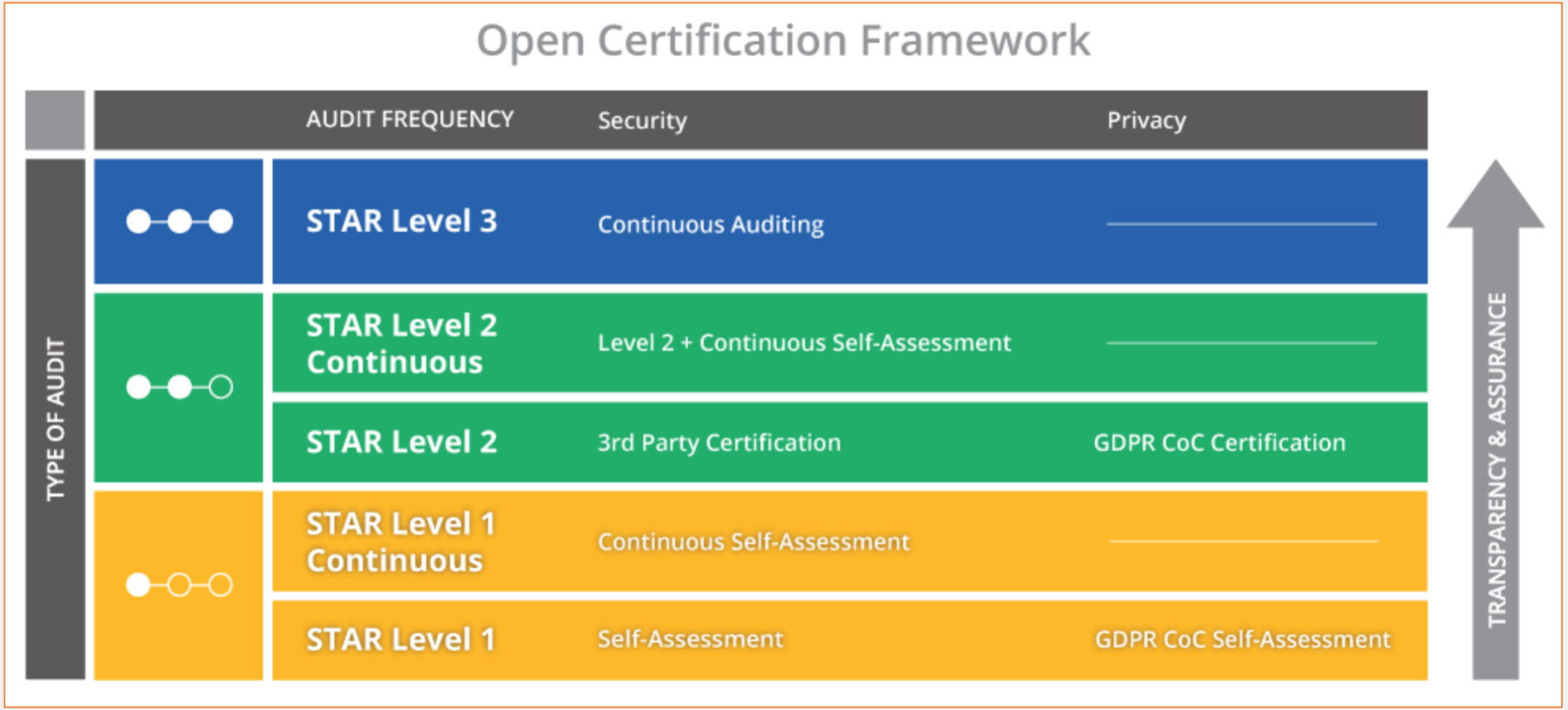
- 1000's of different methodologies and questionnaires.
- Choose one that fits with:
  - Your understanding of risk
  - Your organization's understanding of risk (risk management program)
  - Efficiency goals
  - Your own due diligence requirements
  - Your regulators requirements.
- ISO Certification, SOC 2, HITRUST, etc. are all common.
- We use the FISASCORE®, now used by more than 1,000 organizations.
- **Security Trust Assurance and Risk (STAR) Program**
  https://cloudsecurityalliance.org/star/#_overview

Learning Takeaways

Use ~~SIG LITE or~~ Equivalent

- 1000's of different methodologies and questionnaires.
- Choose one that fits with:
  - Your understanding of risk
  - Your organization's understanding of risk (risk management program)
  - Efficiency goals
  - Your own due diligence requirements
  - Your regulators requirements.
- ISO Certification, SOC 2, HITRUST, etc. are all common.
- Security Trust Assurance and Risk (STAR) Program https://cloudsecurityalliance.org/star/#_overview

Learning Takeaways



Learning Takeaways

Review the MSA Contract for Liabilities

- Your Master Service Agreement must be reviewed and squared away prior to using a third-party.
- If you don’t review, make sure someone who’s qualified does. Someone in Legal/Legal Counsel.

Download the Presentation

For a copy of these slides, visit:

https://info.frsecure.com/csa2019

Quick Recap

Covered a lot, but it was all simple.

1. **Figure out your WHY.** – If you don't have one, then don't do anything.
2. **Figure out the WHAT.**
   - The type of program you build depends on your WHY; Painful, Partial, or Good.
   - Make it SIMPLE.
   - Make it STANDARD.
   - Make it DEFENSIBLE.
3. **Figure out the HOW.**
   - Details like the specific contract language, questionnaires, scoring, etc.
   - This is also a feedback into #2 and #1 above.

Thank you!


@evanfrancen


https://www.linkedin.com/in/evanfrancen/

Thank You for Participating in Today's Event!

FRSECURE®

CSAMN cloud security alliance®
Minnesota Chapter

TREND MICRO™

RELIAQUEST

Heads Up! Next Event is on…

Threat Hunting

June 21st 2019 at 1:00pm – 4:00pm