SECURITYSTUDIO®

Vendor Risk Management

What you need to know

INTRODUCTIONS

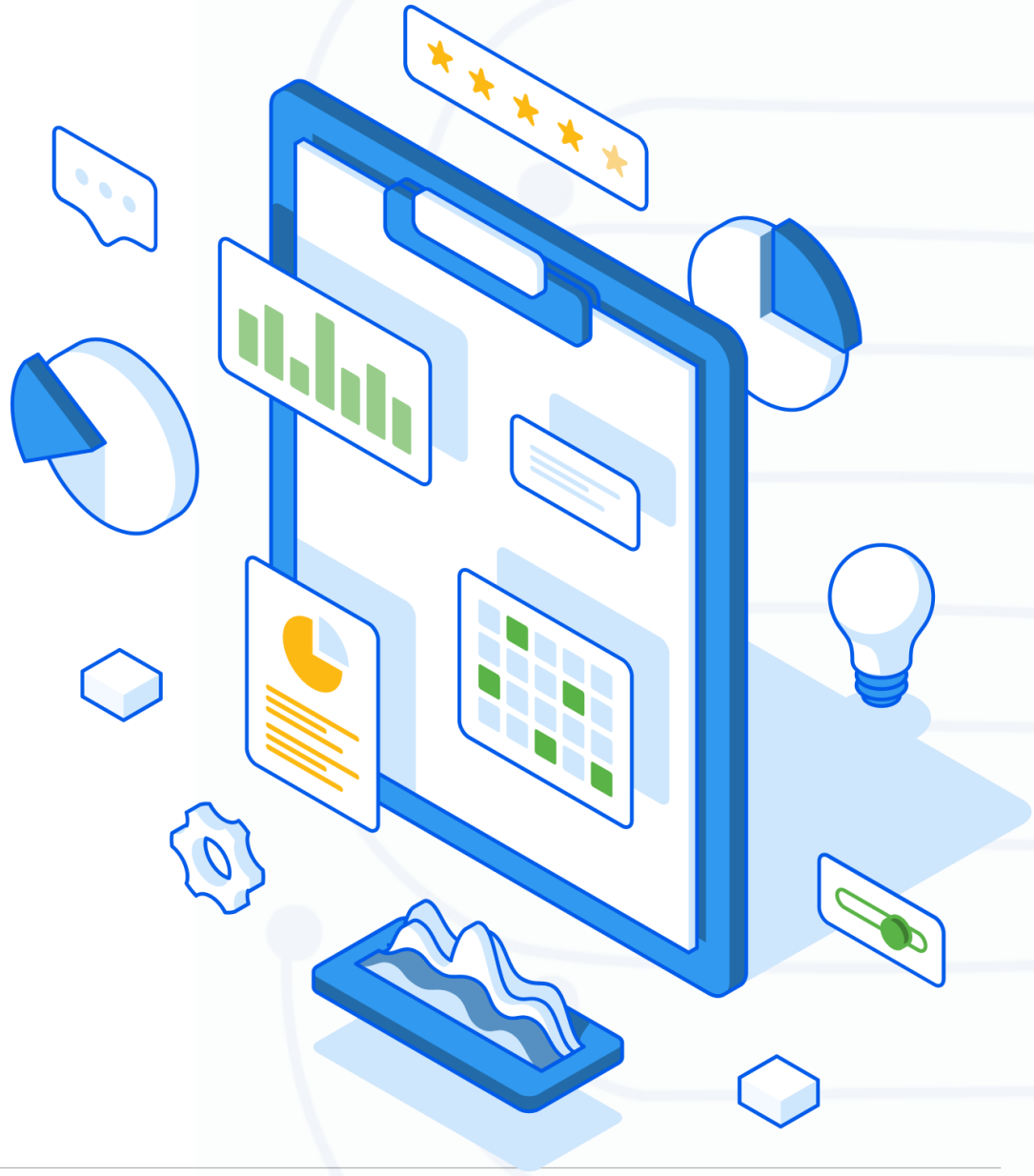
- Ryan Cloutier, CISSP®
- President of SecurityStudio®
- Over 15 years of experience in Cybersecurity
- Virtual Chief Information Security Officer
- Certified Information Security Systems Professional®

@CLOUTIERSEC

SECURITYSTUDIO®

WHAT IS A VENDOR

A Vendor is any company or person who provides a product, service or consulting to your business.



COMMON QUESTIONS

1. Who should be the first point of contact for new potential vendors?
2. When should vendors be assessed?
3. How do you build internal stakeholder support for participation in the VRM program?

SECURITYSTUDIO

COMMON QUESTIONS

1. What is unacceptable risk?
2. Who has the authority to replace vendors with unacceptable risk?

SECURITYSTUDIO

COMMON QUESTIONS

1. Are there exceptions to the process?
2. How do you deal with an exception?

SECURITYSTUDIO

WHAT IS A VRM POLICY

A **Vendor Risk Management Policy**

The purpose of a **vendor management policy** is to identify which **vendors** put your organization at **risk** and then define controls to minimize **third-party** and fourth-party **risk**. It starts with due diligence and assessing whether a **third-party vendor** should have access to sensitive data.

An effective and thorough VRM Policy can simplify the management of vendors' risk

WHAT A VRM POLICY IS NOT

- VRM policy is NOT (just) a document.
- VRM policy is NOT (just) words.
- VRM policy is NOT (only) for compliance.
- VRM policy is NOT meant to be read by everyone (it's a reference).

VRM Policy is NOT the end it’s the start

WHAT A VRM POLICY IS NOT

- VRM policy is NOT a policy if executive management hasn't approved (and supported) it.
- VRM policy is NOT a policy if it hinders business more than it protects it.
- VRM policy is NOT a static document, it must change with the business.

VRM Policy is NOT the end it's the start

POLICY AND S2VENDOR

Your VRM policy should cover the following:

- Who, how and when to enter vendors into S2Vendor
- Grants you authority to enforce cooperation (internally and contractually)
- Provides instructions on exceptions

SECURITYSTUDIO

POLICY AND S2VENDOR

- Helps enforce accountability
- Establishes acceptable risk thresholds
- Gives the authority to act on results from your vendor assessment

GETTING STARTED WITH VRM POLICY

Start with the basics, keep it simple and small(Focus on the critical components)

Purpose

Define assessments

Audience

Define management processes

Definitions

Waivers

Policy language

Enforcement

VRM POLICY DEEP DIVE

Purpose:

(Your ORGANIZATION) utilizes third-party products and services to support our mission and goals. Third-party relationships carry inherent and residual risks that must be considered as part of our due care and diligence. The Third-Party Information Security Risk Management Policy contains the requirements for how (Your ORGANIZATION) will conduct our third-party information security due diligence.

VRM POLICY DEEP DIVE

Audience:

This policy applies to all individuals who engage with a third-party on behalf of (Your ORGANIZATION).

VRM POLICY DEEP DIVE

Definitions:

•**Employee** – defined as a person who is a part-time or full-time hourly or salaried employee who is performing work for (Your ORGANIZATION) as an employee, and not an independent contractor. Sometimes referred to as a "W2 employee".

•**Third-party or 3rd-party** – any person or organization who provides a service or product to (Your ORGANIZATION) and is not an employee.

•**Information Resources** – any system involved in the creation, use, management, storage, and/or destruction of (Your ORGANIZATION) information and the information itself.

•**Inherent information security risk** – the information security risk related to the nature of the 3rd-party relationship without accounting for any protections or controls. Inherent risk is sometimes referred to as "impact" and is used to classify third-party relationships as an indicator of what additional due diligence may be warranted.

•**Residual information security risk** – the information security risk remaining once all applicable protections and controls are accounted for.

VRM POLICY DEEP DIVE

Policy:

The policy is organized into three sections; general, physical, and technical according to the precaution or requirement specified.

Assessments

•Every 3rd-party granted access to (Your ORGANIZATION) Information Resources must sign the (Your ORGANIZATION) Third-Party Non-Disclosure Agreement and Business Associate Agreement (if applicable).

•All 3rd-party relationships must be evaluated for inherent information security risk prior to any interaction with (Your ORGANIZATION) Information Resources.

•Criteria for inherent risk classifications must be established; “High”, “Medium”, and “Low”.

•All 3rd-party relationships must be re-evaluated for inherent information security risk bi-annually and any time there is a material change in how (Your ORGANIZATION) utilizes the third-party product or service.

VRM POLICY DEEP DIVE

Policy:

The policy is organized into three sections; general, physical, and technical according to the precaution or requirement specified.

Assessments

•3rd-party relationships with significant inherent risk (classified as “High” or “Medium”) must be evaluated for residual risk using questionnaires, publicly available information, and/or technical tools.

•Residual information security risk assessments must account for administrative, physical, and technical controls.

•Residual information security risk thresholds must be established for 3rd-party relationships with significant inherent risk (classified as “High” or “Medium”).

•3rd-party relationships that do not meet established residual information security risk thresholds:

- Must be terminated,
- Must be formally approved by executive management following an established waiver process, and/or;
- Changed in a manner that reduces inherent and/or residual information security risk to meet (Your ORGANIZATION) established thresholds.

•3rd-party relationships concerning industry and/or regulatory requirements (i.e. PCI-DSS, HIPAA, etc.) must be reviewed on no less frequent than an annual basis.

VRM POLICY DEEP DIVE

Policy:

Management

•3rd-party agreements and contracts must specify:

- The (Your ORGANIZATION) information the vendor should have access to,
- How (Your ORGANIZATION) information is to be protected by the 3rd-party,
- How (Your ORGANIZATION) information is to be transferred between (Your ORGANIZATION) and the 3rd-party,
- Acceptable methods for the return, destruction or disposal of (Your ORGANIZATION) information in the 3rd-party's possession at the end of the relationship/contract,
- Minimum information security requirements,
- Information security incident response and notification requirements,
- Right for (Your ORGANIZATION) to audit 3rd-party information security protections and controls.

VRM POLICY DEEP DIVE

Policy:

Management

•If the 3rd-party subcontracts part of the information and communication technology service provided to (Your ORGANIZATION), the 3rd-party is required to ensure appropriate information security practices are followed throughout the supply chain,

•The 3rd-party must only use (Your ORGANIZATION) Information Resources for the purpose of the business agreement and/or contract,

•Work outside of defined parameters in the contract must be approved in writing by the appropriate (Your ORGANIZATION) point of contact.

•3rd-party performance must be reviewed annually to ensure compliance with agreed upon contracts and/or service level agreements (SLAs). In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.

•The 3rd-party's major IT work activities must be entered into or captured in a log:

- Made available to (Your ORGANIZATION) IT management upon request, and
- Must include events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

VRM POLICY DEEP DIVE

Policy:

Management

•Any other (Your ORGANIZATION) information acquired by the 3rd-party during the contract cannot be used for the 3rd-party's own purposes or divulged to others.

•3rd-party personnel must report all security incidents directly to the appropriate (Your ORGANIZATION) IT personnel.

•(Your ORGANIZATION) IT will provide a technical point of contact for the 3rd-party. The point of contact will work with the 3rd-party to ensure compliance with this policy.

•3rd-parties must provide (Your ORGANIZATION) a list of key personnel working on the contract when requested.

•3rd-parties must provide (Your ORGANIZATION) with notification of key staff changes within 24 hours of change.

•Upon departure of a 3rd-party employee from a contract, for any reason, the 3rd-party will ensure all sensitive information is collected and returned to (Your ORGANIZATION) or destroyed within 24 hours.

VRM POLICY DEEP DIVE

Policy:

Management

•Upon termination of contract, 3rd-parties must be reminded of confidentiality and non-disclosure requirements.

•Upon termination of contract or at the request of (Your ORGANIZATION), the 3rd-party must surrender all (Your ORGANIZATION) badges, access cards, equipment and supplies immediately.

•Any equipment and/or supplies to be retained by the 3rd-party must be documented by authorized (Your ORGANIZATION) IT management.

VRM POLICY DEEP DIVE

Policy:

Waivers

Waivers from certain and specific policy provisions may be sought following the (Your ORGANIZATION) Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

VRM POLICY DEEP DIVE

Policy:

Enforcement

This Third-Party Information Security Risk Management Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between (Your ORGANIZATION) policies, they must be brought to the attention of (Your ORGANIZATION) for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

GETTING STARTED WITH VRM POLICY

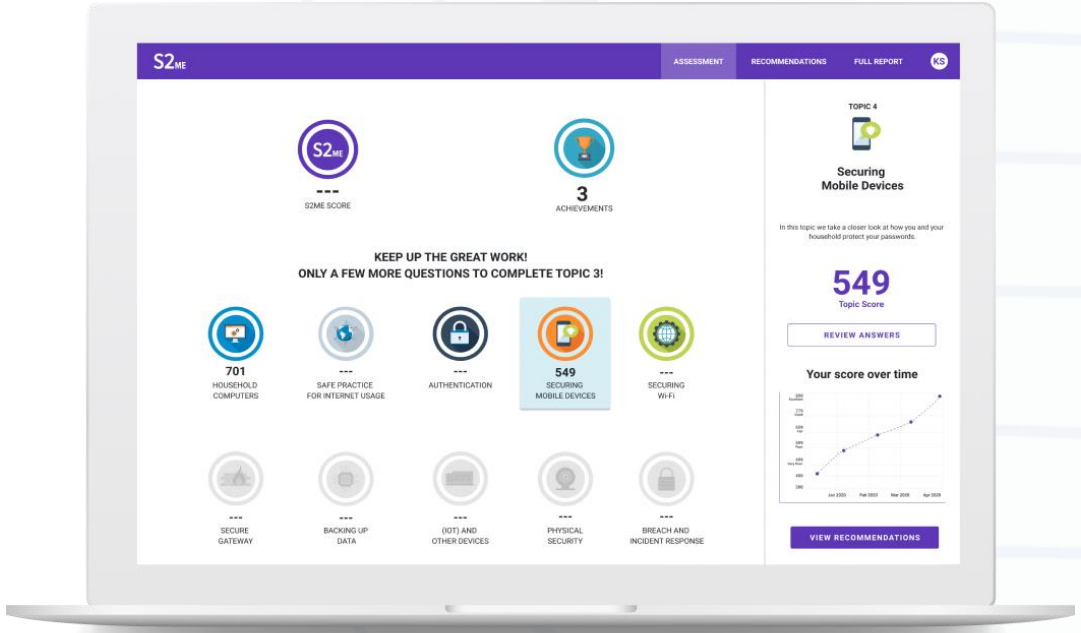
Resources:

https://securitystudio.com/policy-templates/third-party-information-security-risk-management-policy/

https://securitystudio.com/vrm-assessment/

S2ME

- https://S2me.io
- Comprehensive
- Focused on at home and personal
- Roadmap for improvement
- Free, Really, it’s free no catch



SECURITYSTUDIO

QUESTIONS

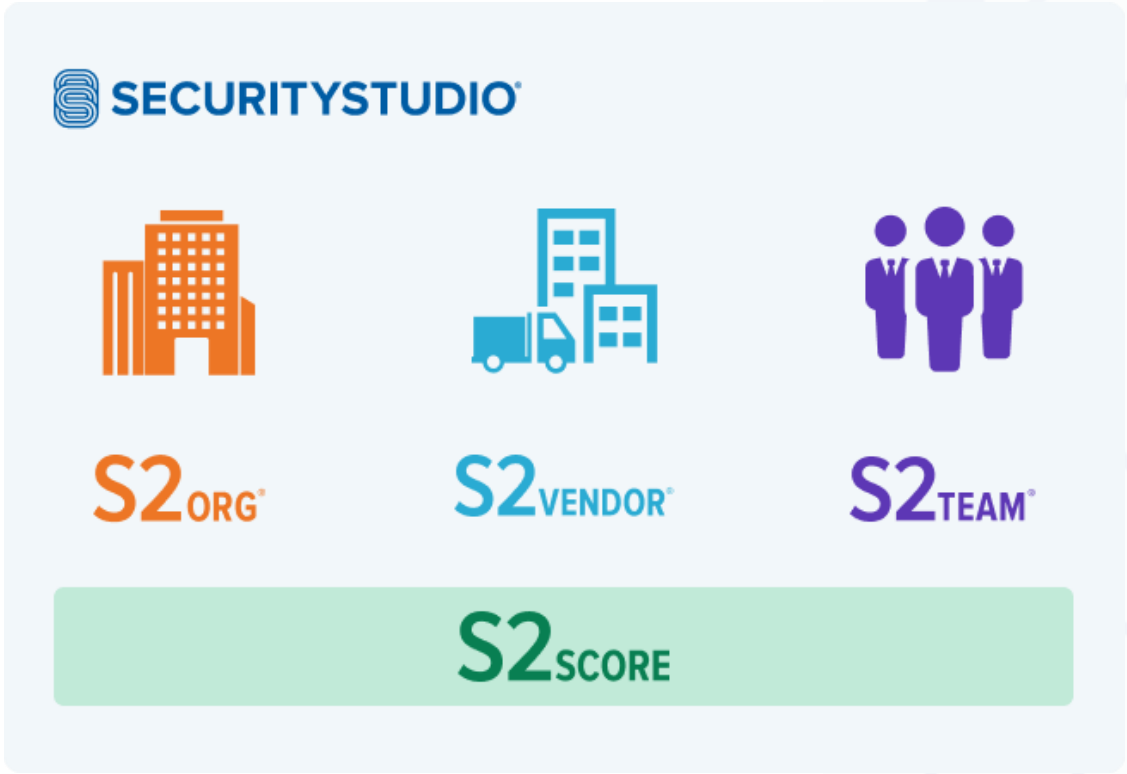
INFOSAFTEY TOOLS DESIGNED FOR PEOPLE.

S2SCORE

Measure and communicate information security programs

S2VENDOR

Manage 3rd party risk



S2ORG

Assess information security programs and manage roadmaps

S2TEAM

Manage employee risk

SECURITYSTUDIO

CONTACT US

SecurityStudio
5509 Baker Road, Suite 500, Minnetonka, MN 55345

WEB

Company - https://securitystudio.com

S2ORG - https://securitystudio.com/s2org/

S2VENDOR - https://securitystudio.com/s2vendor/

S2TEAM - https://securitystudio.com/s2team/

S2ME – https://s2me.io

SOCIAL

Twitter - @StudioSecurity and https://twitter.com/StudioSecurity

LinkedIn - https://www.linkedin.com/company/securitystudio/

Facebook - https://www.facebook.com/SStudioMN/


SECURITYSTUDIO®