Vendor Risk Management (VRM)

Information Session

Fall 2020

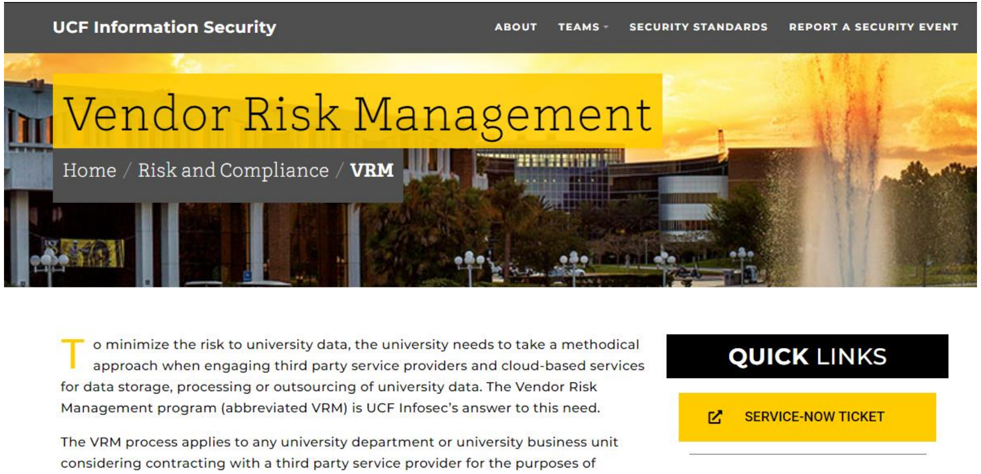
UCF | Information Security Office

Before we start

- Everything covered today can be found on the VRM website

infosec.ucf.edu/vrm

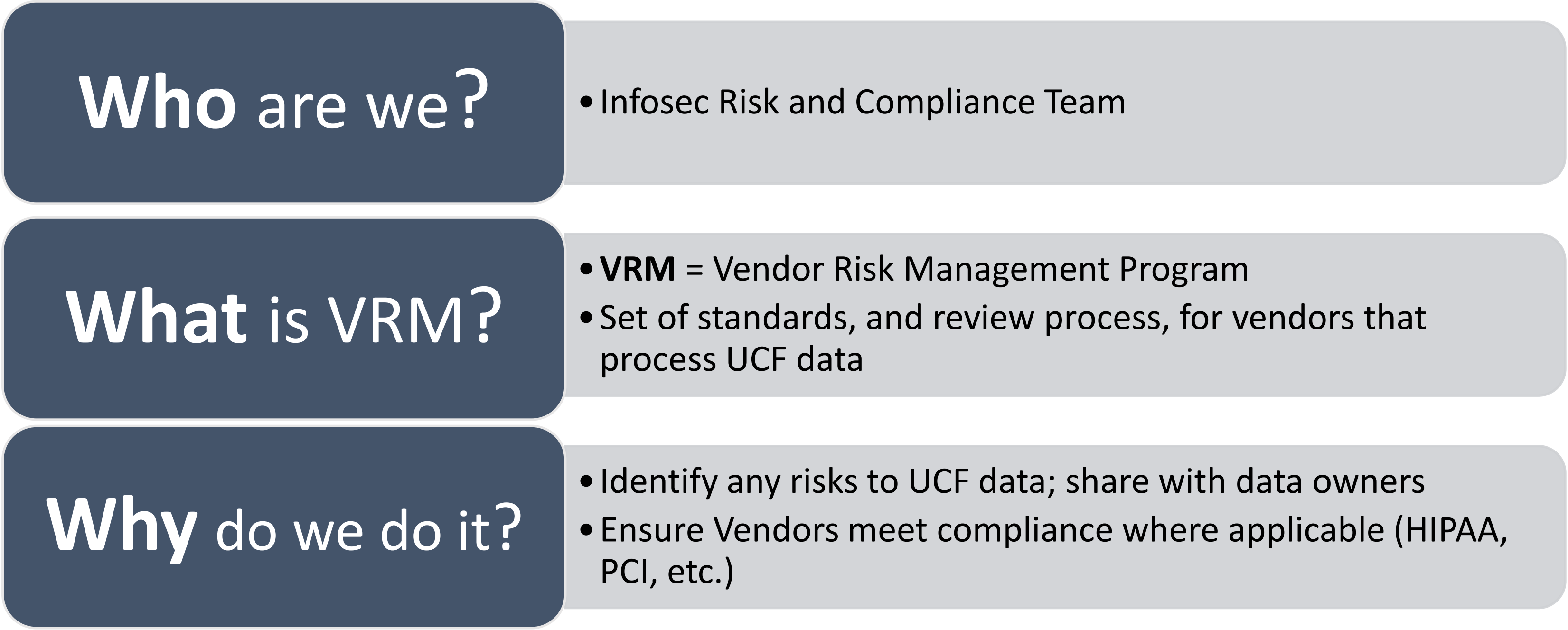
- Slides will be distributed
- Session will be recorded/shared
- Live Q+A at the end
  - Submit questions in chat, or "raise your hand" teams and we'll call on you
  - We will cover as many as we can
  - May take some offline as necessary



To minimize the risk to university data, the university needs to take a methodical approach when engaging third party service providers and cloud-based services for data storage, processing or outsourcing of university data. The Vendor Risk Management program (abbreviated VRM) is UCF Infosec's answer to this need.

The VRM process applies to any university department or university business unit considering contracting with a third party service provider for the purposes of

About us!



Who are we?

- Infosec Risk and Compliance Team

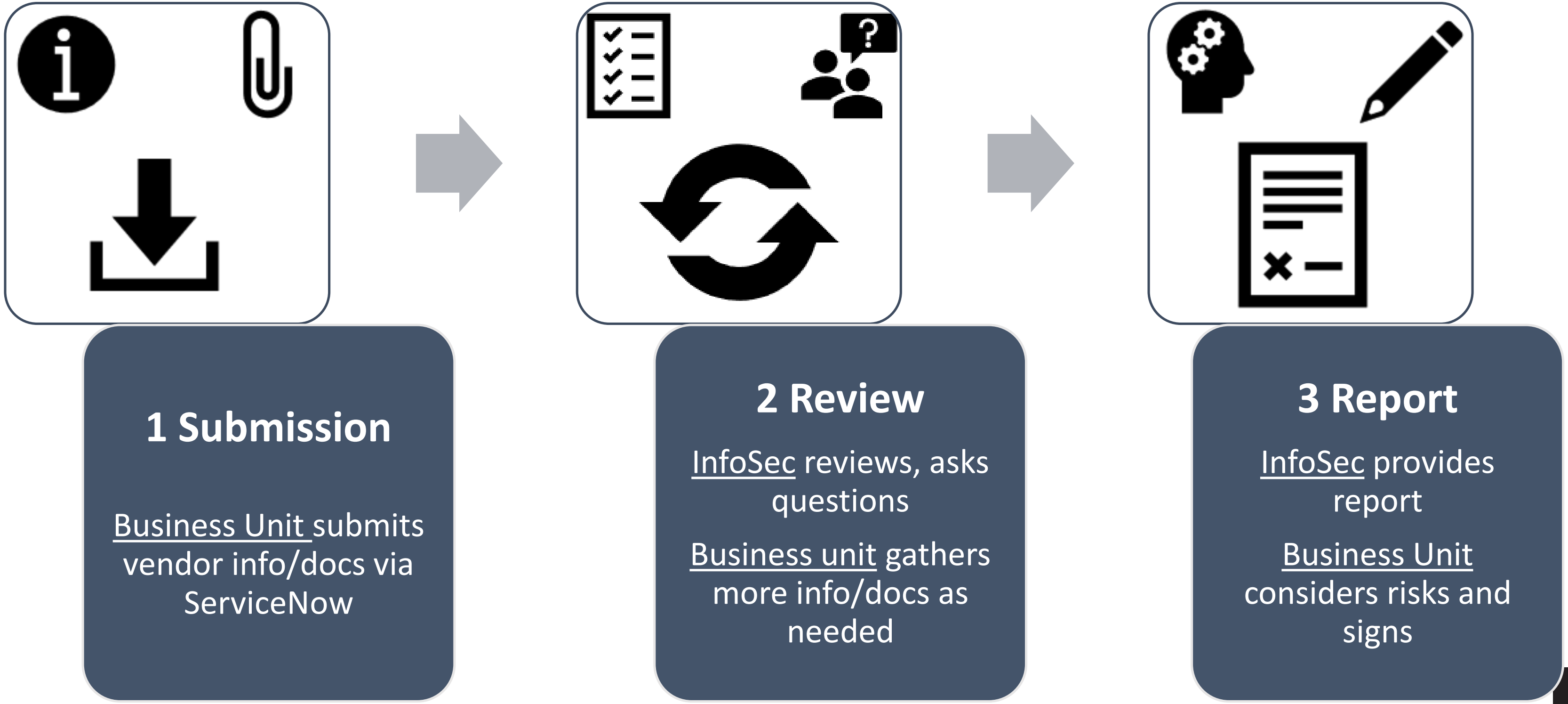
What is VRM?

- **VRM** = Vendor Risk Management Program
- Set of standards, and review process, for vendors that process UCF data

Why do we do it?

- Identify any risks to UCF data; share with data owners
- Ensure Vendors meet compliance where applicable (HIPAA, PCI, etc.)

General Process Overview



1 Submission

Business Unit submits vendor info/docs via ServiceNow

2 Review

InfoSec reviews, asks questions

Business unit gathers more info/docs as needed

3 Report

InfoSec provides report

Business Unit considers risks and signs

Data Classification

Highly Restricted Data

- Data encryption required
- Governing body / fees associated with improper handling of data

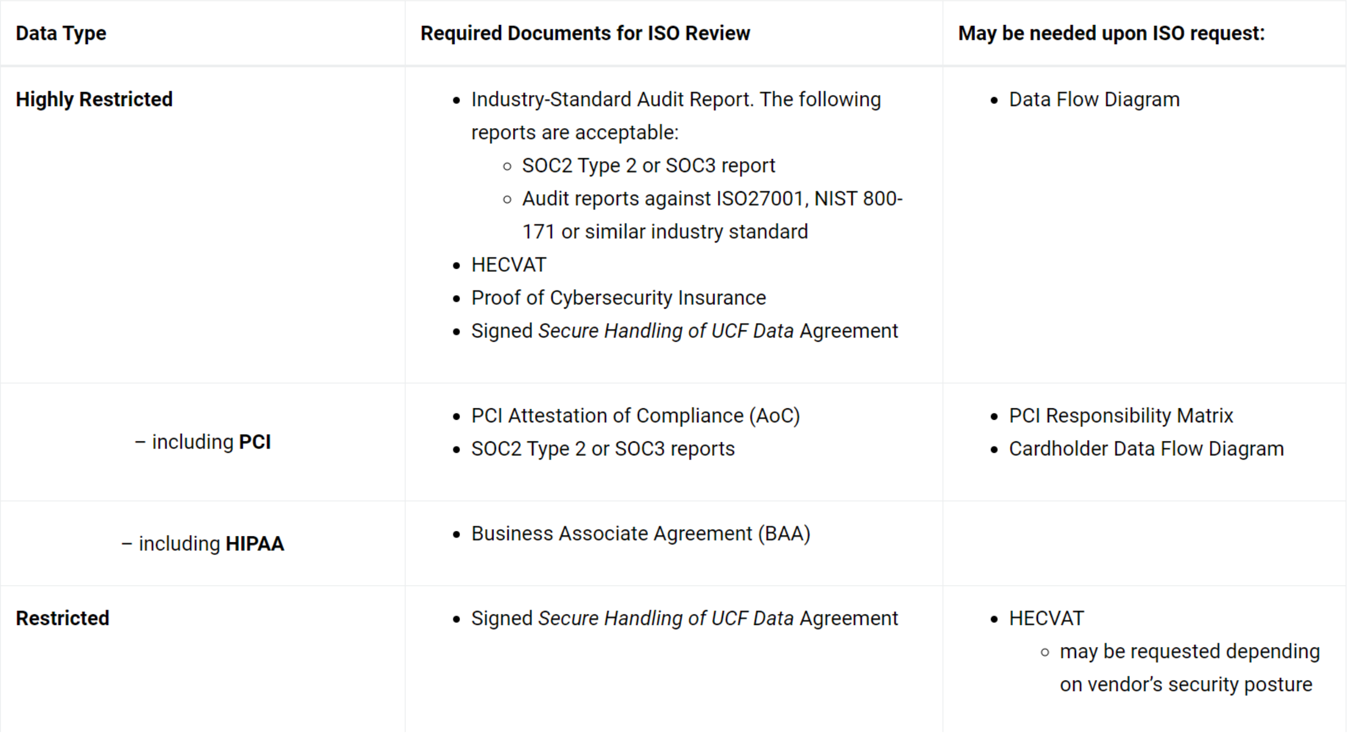
Restricted Data

- Reasonable protection required
- Reputational damage expected

Unrestricted Data

- Data intended to be public

VRM Review – Documentation Requirements



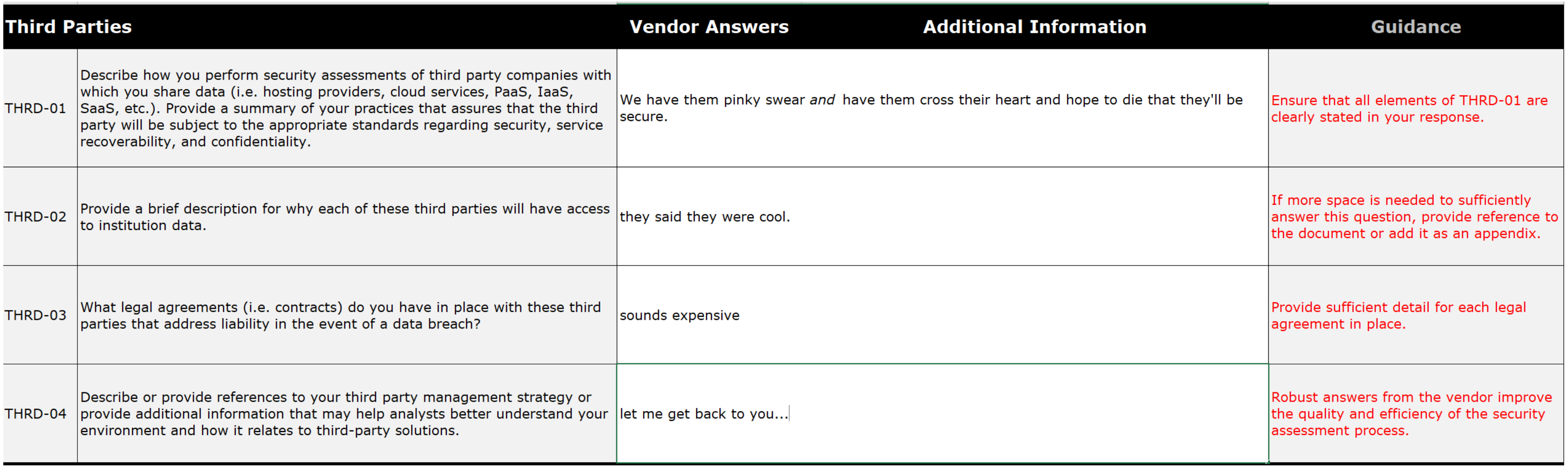
Data Type	Required Documents for ISO Review	May be needed upon ISO request:
Highly Restricted	• Industry-Standard Audit Report. The following reports are acceptable: ◦ SOC2 Type 2 or SOC3 report ◦ Audit reports against ISO27001, NIST 800-171 or similar industry standard • HECVAT • Proof of Cybersecurity Insurance • Signed *Secure Handling of UCF Data* Agreement	• Data Flow Diagram
– including **PCI**	• PCI Attestation of Compliance (AoC) • SOC2 Type 2 or SOC3 reports	• PCI Responsibility Matrix • Cardholder Data Flow Diagram
– including **HIPAA**	• Business Associate Agreement (BAA)	
Restricted	• Signed *Secure Handling of UCF Data* Agreement	• HECVAT ◦ may be requested depending on vendor's security posture

Totally Legit Vendor LLC

- Data Involved
  - Highly Restricted
    - SSNs
  - Restricted
    - FERPA Educational Records

- Users Involved
  - UCF Faculty
    - Faculty members will have administrative privileges within the vendor’s solution
  - UCF Students
    - Will log in to take exams

HECVAT Responses

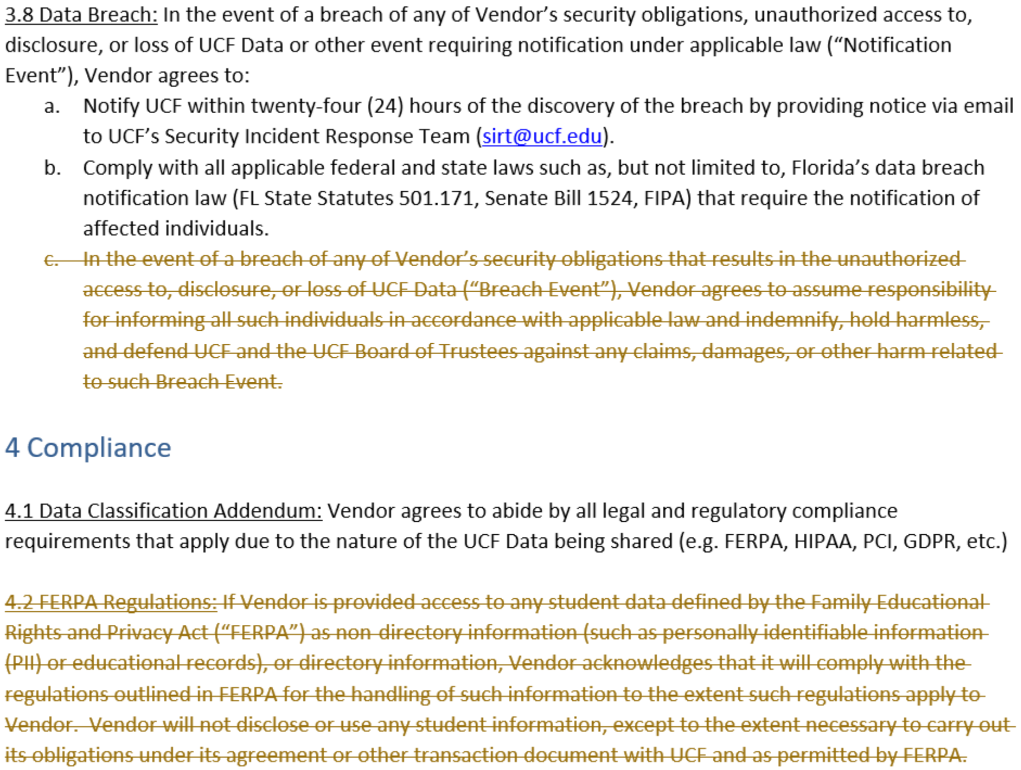


Third Parties		Vendor Answers	Additional Information	Guidance
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	We have them pinky swear *and* have them cross their heart and hope to die that they'll be secure.		Ensure that all elements of THRD-01 are clearly stated in your response.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	they said they were cool.		If more space is needed to sufficiently answer this question, provide reference to the document or add it as an appendix.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	sounds expensive		Provide sufficient detail for each legal agreement in place.
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	let me get back to you...		Robust answers from the vendor improve the quality and efficiency of the security assessment process.

Other Documentation issues

✓	3rd party audit	SOC report is from 8 years ago
☒	Insurance Certificate	Missing and Minimal Coverage
	Secure Handling of UCF Data (SHUDA)	Major edits and removals of sections

SHUDA Edits



3.8 Data Breach: In the event of a breach of any of Vendor’s security obligations, unauthorized access to, disclosure, or loss of UCF Data or other event requiring notification under applicable law (“Notification Event”), Vendor agrees to:

a. Notify UCF within twenty-four (24) hours of the discovery of the breach by providing notice via email to UCF’s Security Incident Response Team (sirt@ucf.edu).

b. Comply with all applicable federal and state laws such as, but not limited to, Florida’s data breach notification law (FL State Statutes 501.171, Senate Bill 1524, FIPA) that require the notification of affected individuals.

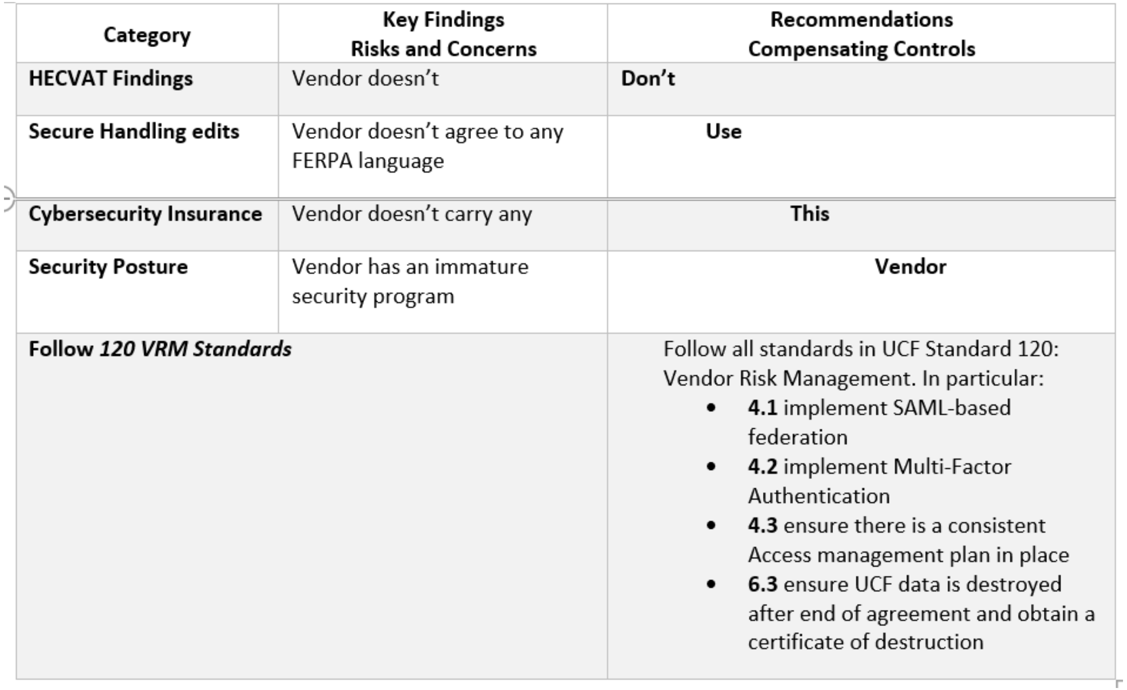
~~c. In the event of a breach of any of Vendor’s security obligations that results in the unauthorized access to, disclosure, or loss of UCF Data (“Breach Event”), Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and indemnify, hold harmless, and defend UCF and the UCF Board of Trustees against any claims, damages, or other harm related to such Breach Event.~~

4 Compliance

4.1 Data Classification Addendum: Vendor agrees to abide by all legal and regulatory compliance requirements that apply due to the nature of the UCF Data being shared (e.g. FERPA, HIPAA, PCI, GDPR, etc.)

~~4.2 FERPA Regulations: If Vendor is provided access to any student data defined by the Family Educational Rights and Privacy Act (“FERPA”) as non-directory information (such as personally identifiable information (PII) or educational records), or directory information, Vendor acknowledges that it will comply with the regulations outlined in FERPA for the handling of such information to the extent such regulations apply to Vendor. Vendor will not disclose or use any student information, except to the extent necessary to carry out its obligations under its agreement or other transaction document with UCF and as permitted by FERPA.~~

The End Result?



Category	Key Findings Risks and Concerns	Recommendations Compensating Controls
HECVAT Findings	Vendor doesn't	**Don't**
Secure Handling edits	Vendor doesn't agree to any FERPA language	**Use**
Cybersecurity Insurance	Vendor doesn't carry any	**This**
Security Posture	Vendor has an immature security program	**Vendor**
Follow *120 VRM Standards*		Follow all standards in UCF Standard 120: Vendor Risk Management. In particular: • **4.1** implement SAML-based federation • **4.2** implement Multi-Factor Authentication • **4.3** ensure there is a consistent Access management plan in place • **6.3** ensure UCF data is destroyed after end of agreement and obtain a certificate of destruction

Reviewing VRM standard

The intensity of review depends on the classification of data being shared with a third-party vendor. This follows in line with the levels of data classification: Highly Restricted Data, Restricted Data and Unrestricted Data.

The 120 Vendor Risk Management Standards was developed to empower business units to analyze vendors independently. Failing that, the standard was meant to help business units to understand the steps of the VRM process.

There are specific requirements for each level of data outlined in the VRM standard. The appendices delineate legal requirements associated with all vendor agreements, as well as the necessary precautions for establishing local accounts.

Applicability

SOFTWARE AS A SERVICE (SAAS):

Cloud based software used to store or process UCF Data needs InfoSec review to ensure adequate measures are taken to protect our data in transmission.

SAAS

A cloud hosted electronic Medical Records system.	✓	Yes!
A system that sends marketing emails on UCF's behalf .	✓	Yes!
A service that has already been approved / assessed.	✗	No!

Applicability

LOCAL SOFTWARE:

Generally, local software does not need VRM review; however, any local software that shares or sends data through a third party or with a vendor should be reviewed.

LOCAL SOFTWARE

A file transfer tool that sends data through the third party before reaching the destination.	✓	Yes!
Software that has a cloud account or portal associated with it where files or other data are stored.	✓	Yes!
Software that will be installed on a UCF owned desktop or laptop, or within a UCF-owned environment (UCF datacenters, UCF cloud providers like UCF's Azure or AWS environments)	✗	No!
Computer hardware that will be installed in a UCF-owned environment.	✗	No!

Applicability

CONSULTING:

Vendors that only offer consulting services, and don't store or produce UCF data beyond the scope of the consultation itself.

CONSULTING

A consultant builds a web site that has forms that collect student data, but the site is hosted on the consultant's servers.

✓ Yes!

Consulting, where a vendor will just be performing some work on a UCF system and not storing or capturing any UCF data.

✗ No!

Applicability: Research

Many research contracts only involve receiving data from a third party or sharing research results from that contracted research study. These don't require VRM review. Use existing research contract review processes for these (Huron)

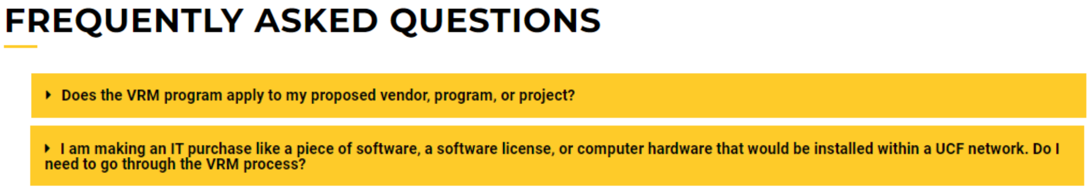
What if I want to use third party services as part of my research? AWS, Dropbox, Google Cloud, etc.: Use university-level agreements wherever possible. If you use services under a university agreement, no VRM review is needed.

A VRM review is required if you want to use a <u>new</u> third party service to process data as part of your research: Particularly if Restricted (Confidential) or Highly Restricted (Federal CUI, HIPAA, etc.) research data is involved.

Not sure if VRM applies?

1.) See the FAQ’s on the VRM website

infosec.ucf.edu/vrm



FREQUENTLY ASKED QUESTIONS

- Does the VRM program apply to my proposed vendor, program, or project?
- I am making an IT purchase like a piece of software, a software license, or computer hardware that would be installed within a UCF network. Do I need to go through the VRM process?

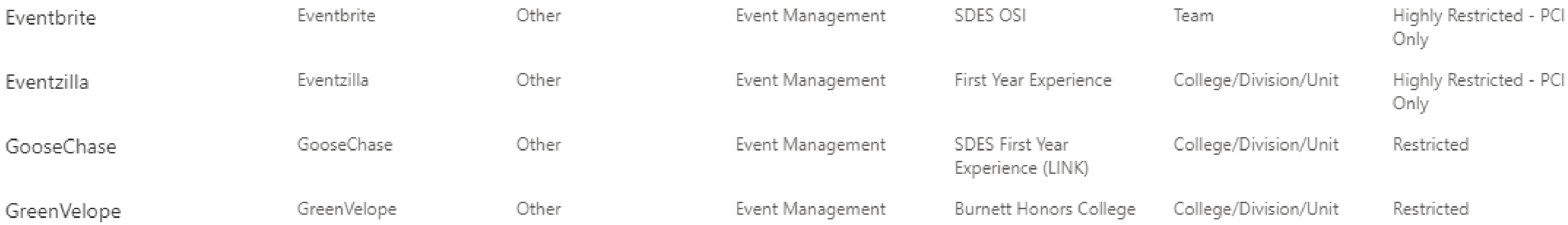
2.) Still not sure? No problem!!

Submit a VRM ticket and we can help!

Duplication

Our goal is to avoid the duplication of services

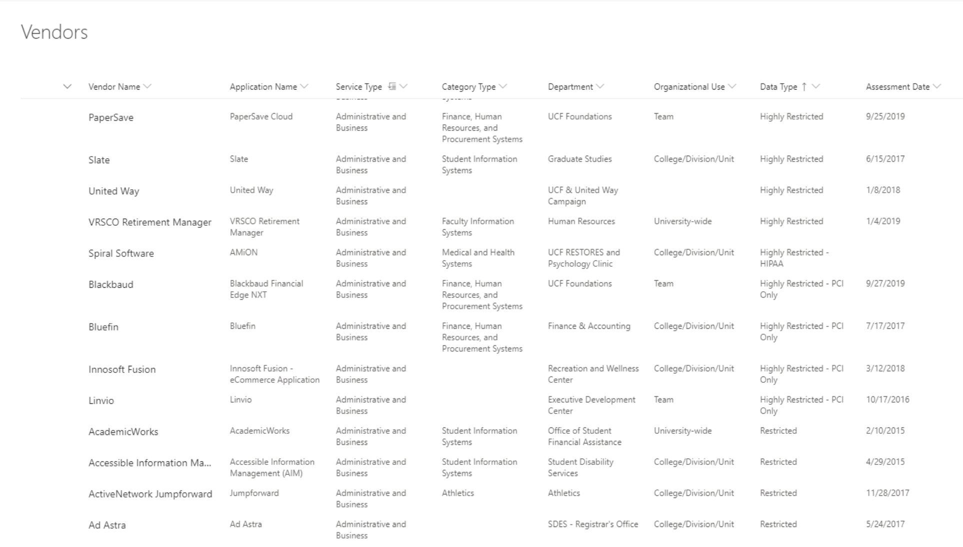
Example: Various vendors providing event management services



Eventbrite	Eventbrite	Other	Event Management	SDES OSI	Team	Highly Restricted - PCI Only
Eventzilla	Eventzilla	Other	Event Management	First Year Experience	College/Division/Unit	Highly Restricted - PCI Only
GooseChase	GooseChase	Other	Event Management	SDES First Year Experience (LINK)	College/Division/Unit	Restricted
GreenVelope	GreenVelope	Other	Event Management	Burnett Honors College	College/Division/Unit	Restricted

Approved Vendor List

- Before engaging with a new vendor, approved solutions can be found on the ITRCC SharePoint
- Each approved vendor lists the data type involved (unrestricted, restricted, highly restricted)



Vendors

Vendor Name	Application Name	Service Type	Category Type	Department	Organizational Use	Data Type ↑	Assessment Date
PaperSave	PaperSave Cloud	Administrative and Business	Finance, Human Resources, and Procurement Systems	UCF Foundations	Team	Highly Restricted	9/25/2019
Slate	Slate	Administrative and Business	Student Information Systems	Graduate Studies	College/Division/Unit	Highly Restricted	6/15/2017
United Way	United Way	Administrative and Business		UCF & United Way Campaign		Highly Restricted	1/8/2018
VRSCO Retirement Manager	VRSCO Retirement Manager	Administrative and Business	Faculty Information Systems	Human Resources	University-wide	Highly Restricted	1/4/2019
Spiral Software	AMiON	Administrative and Business	Medical and Health Systems	UCF RESTORES and Psychology Clinic	College/Division/Unit	Highly Restricted - HIPAA	
Blackbaud	Blackbaud Financial Edge NXT	Administrative and Business	Finance, Human Resources, and Procurement Systems	UCF Foundations	Team	Highly Restricted - PCI Only	9/27/2019
Bluefin	Bluefin	Administrative and Business	Finance, Human Resources, and Procurement Systems	Finance & Accounting	College/Division/Unit	Highly Restricted - PCI Only	7/17/2017
Innosoft Fusion	Innosoft Fusion - eCommerce Application	Administrative and Business		Recreation and Wellness Center	College/Division/Unit	Highly Restricted - PCI Only	3/12/2018
Linvio	Linvio	Administrative and Business		Executive Development Center	Team	Highly Restricted - PCI Only	10/17/2016
AcademicWorks	AcademicWorks	Administrative and Business	Student Information Systems	Office of Student Financial Assistance	University-wide	Restricted	2/10/2015
Accessible Information Ma...	Accessible Information Management (AIM)	Administrative and Business	Student Information Systems	Student Disability Services	College/Division/Unit	Restricted	4/29/2015
ActiveNetwork Jumpforward	Jumpforward	Administrative and Business	Athletics	Athletics	College/Division/Unit	Restricted	11/28/2017
Ad Astra	Ad Astra	Administrative and Business		SDES - Registrar's Office	College/Division/Unit	Restricted	5/24/2017

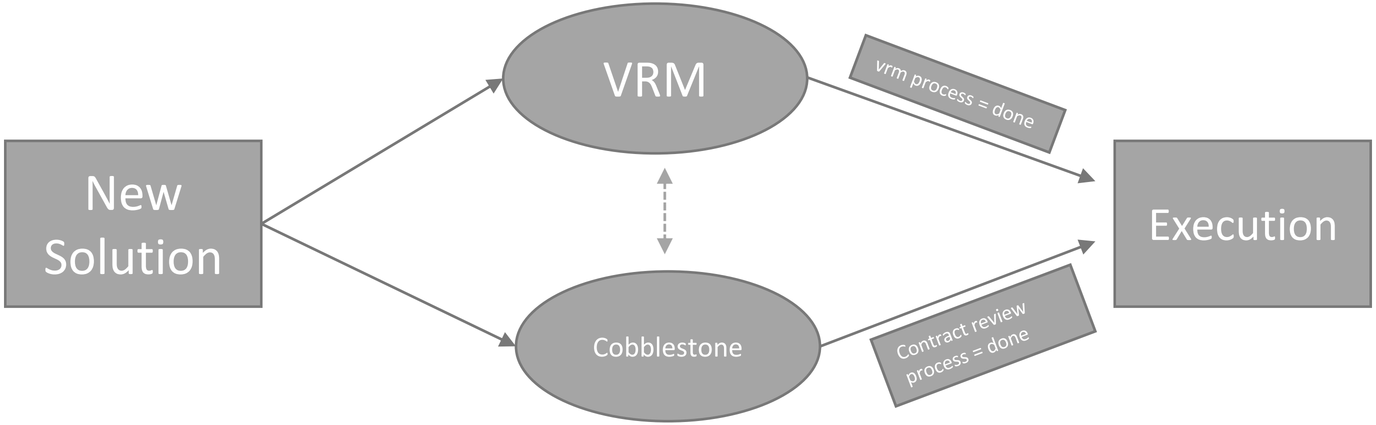
University Process Information

Where does VRM fit into other UCF processes?

- Contracts? Legal review?
- What do I do first?
- How do I know when it is okay to proceed?

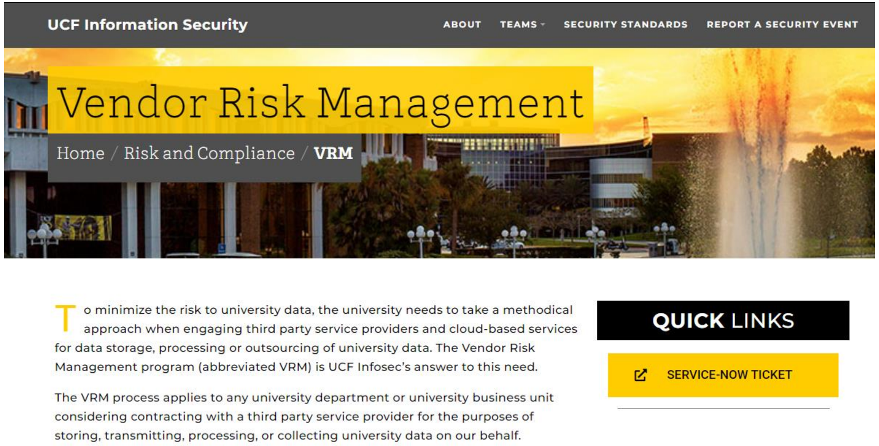
University Process Information

VRM should work in parallel with the contract review process



VRM Site

- https://infosec.ucf.edu/vrm
- UCF Process Documents, Vendor Documents, Service-Now Ticket
- FAQs
- 120 Vendor Risk Management Standard



To minimize the risk to university data, the university needs to take a methodical approach when engaging third party service providers and cloud-based services for data storage, processing or outsourcing of university data. The Vendor Risk Management program (abbreviated VRM) is UCF Infosec's answer to this need.

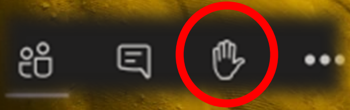
The VRM process applies to any university department or university business unit considering contracting with a third party service provider for the purposes of storing, transmitting, processing, or collecting university data on our behalf.

Q+A

Submit text questions in the Teams meeting chat

or

“raise your hand” in Teams and we’ll call on you



Thank you!

infosec.ucf.edu/vrm