CYBERCECURITY
DEFENDING YOUR ASSETS

IT/Security & Privacy GRC Solutions–Time for an Evolution

By Raymond Hutchins and Mitch Tanenbaum
Date: July 6, 2023

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Abstract and Position: CyberCecurity LLC takes the position that most current Governance, Risk and Compliance (GRC) solutions/tools do not meet the current and future governance requirements of boards and executive management. The only exception *may* be for very expensive solutions targeted at large enterprises. Our analysis has revealed that a core shortcoming for the great majority of GRC solutions is that risk assessments are not yet automated enough in terms of data collection and analysis. This conclusion drives our support for the development and deployment of artificial intelligence (AI)-driven, automated, risk assessment data collection and analysis. Such a system is intended to deliver more accurate, data-driven AI-processed, risk assessments more quickly and for much less cost. Ultimately, the new system will deliver such risk assessments on a real-time, continuous basis, which will be a huge improvement over today's typically annual, manual assessments.

Note: This position paper and associated GRC Solution Assessment are the first products of our ***long-term, "living" GRC solution assessment project.*** We hope that you have found this research of professional value. Now that we have created a baseline of knowledge in this domain, we intend to continue our research to expand our expertise in this subject matter. We intend to provide regular updates on our progress and the associated content to interested parties. If you have no interest in this subject, please advise us and your name will be removed from our list.

Disclaimer: This position paper and any associated research documents represent the authors' and CyberCecurity LLC's best efforts to collect and present information we believe is of value to our clients and the general public. We make no claims or warranties regarding the accuracy or validity of any information presented, other than *it is our best effort at this time*. Additionally, things are changing so quickly that information presented by us could already be out of date. Please do your own research prior to making any GRC solution purchase or evaluation decisions. If you have information which you believe would help us better understand this subject matter, please feel free to reach out and share it.

Table of Contents

1. GRC Solutions--Our View of the Elephant **3**
2. Conclusions and Findings **4**
General Observations 4
Risk Assessments and Data Collection 4
Automation and SaaS Integrations 5
4. GRC Organization **6**
GRC Business Category Coverage 6
GRC Program Elements (Content Modules) 6
Software as a Service Line of Business (LOB) Applications 7
5. GRC Capabilities **8**
Data Collection and Analysis Capabilities 8
Data Input Sources 8
Data Analysis/Output 9
6. Data Collection and Analysis Challenges **9**
APIs and Associated Processes 9
Inadequate Risk Assessment Processes 10
Limited or No Data Analysis Capabilities 11
7. Security Challenges **11**
8. Solution Pricing **12**
About the Authors **13**

NOTE: To request a copy of our full GRC Solution Assessment-2023 please send a request to Ray Hutchins rh@cybercecurity.com

1. GRC Solutions--Our View of the Elephant

GRC is a very broad, large topic and in this report we discuss GRC technical solutions but we are aware that for most companies GRC starts as an internal strategy. Once that strategy is decided upon, then the organization is ready to find technical solutions that will support it. Understanding the available technical solutions will help inform the GRC strategy side of the equation.

There are many different types of GRC solutions, including:

- Those for entry, mid-range, and enterprise users.
- Solutions for different sub-markets such as corporate governance, compliance management, enterprise risk management, business resilience, and more.
- Solutions whose data collection processes are specifically targeted at different business sectors such as business and finance, information technology and security, manufacturing and engineering, healthcare and life sciences, legal and professional services, and more.

The specific focus of our analysis is ***IT/Security and Privacy GRC solutions*** which support the incorporation of data security and privacy into the governance, risk management, and compliance processes. This is important because any organization's foundation is based on its information technology infrastructure, and cyber risk is no longer considered separate from any other sort of business risk.

NOTE: It is important to understand our definition of IT. It not only means the "nerds" who stare at monitors all day (and night). IT encompasses virtually every part of every business. HR? Are you keeping employee records on ledger books? Sales? Are you meeting all of your prospects at a local Starbucks? Accounting? Are you still using an abacus? You get the idea. IT is involved in every part of your business and all of that needs to be included in your GRC process.

In today's world, security as it applies to data privacy has become one of the main drivers in increasing the importance of GRC. Over the past few years, extensive new laws, regulations and requirements have been rolled out with respect to protecting personal data. Please refer to our position paper: *Privacy Laws-An Executive Overview*.

GRC provides a framework to better leverage automation and AI to integrate security and privacy with the organization's overall goals. This will provide boards and management with the data and solutions required to make much more informed decisions regarding data security risks quickly, while mitigating the risk of compromising privacy, facing lawsuits, and paying fines.

2. Conclusions and Findings

Our *2023 GRC Solution Assessment link)* assessed *forty* different GRC solutions, including those presented by Gartner, IDC, and Forrester.

General Observations

a. The actual capabilities of most GRC solutions are difficult to ascertain and understand from the language presented on each vendor's websites. There is not yet any "standard" approach to collecting, analyzing, organizing data and then presenting GRC findings. There is also no standard for what data to export or what format to export it to.
b. Virtually no useful solutions exist yet for SMB companies that lack serious development capabilities and resources.
c. A company needs to set internal expectations correctly and then get outside support to reduce their risks of wasting money and time on the wrong GRC solution. Even if all the data a company wants is exposed, it still takes a lot of effort to get that data into a usable format for boards and management.

Risk Assessments and Data Collection

a. When discussing an ***IT/Security and Privacy GRC Solution***, much of the relevant data required is predicated upon the organization's risk assessment (RA). Most GRC solutions today still rely upon what are basically manual RAs, and manual RAs are notorious for being very subjective and risky. For example, in the case of a SOC 2, the

assessment part is limited to “there are x controls and you have entered some information for x/2 of them, so you are 50% done”.

b. The ability to extract data from both SaaS and internally developed custom applications is a limiting factor in being able to automate the risk assessment process.

RA risk and quality are impacted by:

- The complexity of the IT infrastructure being assessed
- RA requirements and type
- Whether RA responses are verified or not
- The quality of the RA questions
- The experience of the assessor
- Time allowed for the RA
- Domain knowledge of the participants
- The extent of truthfulness of the participants
- The level of commitment to a quality RA

NOTE: A perfect example of the RA discussion above is DoD efforts to bring the 300K+ Defense Industrial Base (DIB) companies into compliance with the CMMC. At this time, less than 1% of the DIB companies are in compliance with CMMC contract requirements (only about 40 companies). The DoD knows this and wants to implement a *verified* risk assessment process. The current *verified* process requires 3-5 people, on-site for 3-5 days. This type of verified, manual risk assessment is hugely disruptive, time-consuming, and expensive. But DoD is moving forward with this implementation because DoD has NO confidence in the current manual/limited data collection assessment process–and there is nothing better.

By correctly *automating* the RA process, costs and risks associated with RAs would be radically reduced and/or eliminated.

Automation and SaaS Integrations

a. Perhaps *THE* major consideration for boards and top management with respect to IT/Security and Privacy and other GRC solutions is ***automation***.
b. Virtually no GRC solutions provide out-of-the-box automation. The solutions that exist today only support limited automation and we see no evidence that that is changing any time soon.
c. As more applications move to the cloud, the automation problem is going to get even harder because cloud services typically aren’t set up to allow you to extract the data you need to conduct automated GRC risk assessments.
d. Current GRC solutions are still primarily manual and are capable of automating only a small portion of the process.

e. Most current GRC solutions are capable of collecting only a small portion of the data companies require to understand their risk.
f. Most GRC solutions provide APIs that allow you to automatically import some data from the business applications you typically use, but the value of this depends upon:

    - The type and quantity of the data that those applications make available.
    - Your knowledge of the internal data structures within the SaaS application you need data from and how to map that to the correct location within the GRC solution.

> **NOTE**: This is likely a time-consuming and expensive process which results in additional cost to you above the initial cost of the GRC solution. This process must be maintained and reapplied as the target SaaS applications evolve over time. We know of one larger client who engaged Deloitte to come in and handle this for them. How much did that cost?

> **NOTE**: In a recent security assessment we conducted for a 40-person company, they identified 225 cloud applications that they had to log into, a key indicator of where the company's data exists. The vast majority of these were SaaS applications. Most companies don't even have this type of inventory, nevermind including these applications in their risk assessments.

g. Most reviewed GRC solutions claim they are automating the collection of the data. But many times this only applies to a small portion of the data needed to conduct a robust cyber risk assessment. Then they review the answers manually to get an estimate of compliance status. Those tools that "automate" the review process do not look at the quality of the answers, but rather that the field is not blank and you checked the "done" box.
h. Almost all GRC solutions claim they can accommodate all business categories if the client customizes the platform. In order for the client to do this, the solution provides API documentation to the client, so the client must have this technical capability.
i. The success of the GRC solution is limited based on the overlap of the SaaS applications that the client uses and the SaaS applications that the GRC solution can automatically extract data from.
j. The first step in selecting a GRC vendor is to ask for their list of SaaS application integrations that they have already done and what data they can extract from each app. That's the first step we took.
k. Some vendors will say that they provide the API and you can do the integration yourself. This only works if you have a development team, the budget and the bandwidth to do this, and the SaaS application you want to work with has an API that will enable this.
l. If you are evaluating a GRC solution based on the integrations they have, you need to make sure that the data you want is available through that integration.

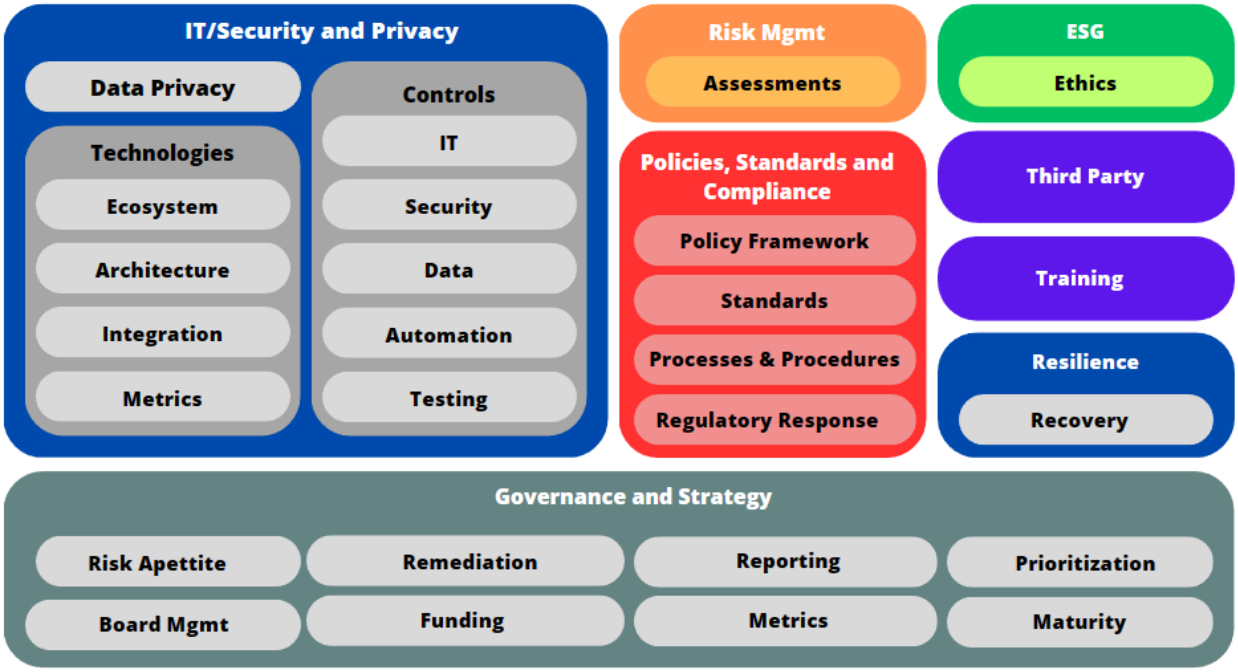
4. GRC Organization

GRC Business Category Coverage

Many discussions regarding GRC solutions might lead the reader and potential user to believe that certain GRC solutions are specific to particular industries. If a GRC solution is specifically designed to cover a particular industry, then one would expect APIs that were built for industry specific SaaS applications, but in reality, what they mean is that they ask the compliance standards appropriate for that industry. For example, they ask HIPAA questions for healthcare and CMMC questions for defense. As we got deeper into our assessment process, we came to understand that what GRC solution providers were offering was to customize their solution to your industry at your request. Most solution providers offer this, usually for a significant annual cost.

GRC Program Elements (Content Modules)

Much is revealed about a GRC solution's capabilities by the various program elements or "content modules" offered. Content modules are the GRC knowledge domains identified by the solution and indicate the data targets of the GRC solution. Various solution providers may describe their knowledge domains in other ways besides content modules, but the idea is the same. Possible content modules/knowledge domains should include:



Note the inclusion of IT/Security and Privacy. No current solution providers cover this topic. That is a mistake, since, in an IT centric world…EVERYTHING operates upon this foundation.

Once you have an idea about the content modules offered by the GRC solution, then you can drill deeper to better understand what the solution can or cannot do.

Software as a Service Line of Business (LOB) Applications

SaaS LOB applications are highly customized for a specific business. Home mortgage companies have loan origination systems that are customized to the particular type of mortgage loans the company will be originating. Doctors' office applications are customized to the *type of medical practice* the doctor has. That means that there are thousands (or more) very narrowly focused applications that cater to a particular market segment.

These applications, unlike, say, Google Workspace, have a relatively tiny market size. Vendors focus on adding capabilities that the target market needs and not on generalized APIs that allow a GRC application to extract system configuration, log and event data–assuming the right data is even collected inside the application.

For many SaaS (cloud) applications, the application runs in a shared environment where users are separated by a very thin layer of tinfoil called access control lists (ACLs). These ACLs stop one company from seeing another company's data, but the APIs often do not apply to the underlying management data that is needed for the GRC process. That means the vendor must extract the data for the company manually, if they are willing to do it at all. Alternatively, you can ask the vendor to build a custom API, which they may not be able to do or may be able to do at a price you cannot afford.

5. GRC Capabilities

Data Collection and Analysis Capabilities

A GRC solution is nothing without current, trusted information about the organization's IT infrastructure (which must include business-critical and other 3rd-party vendors). Historically, the only real way to collect such information was manually and nothing was verifiable. Clearly, that approach is inadequate, but at this time, there are NO fully automated data collection and analysis solutions. What everyone is forced to do is to cobble together two or more solutions to make this happen, while still requiring a lot of manual work.

A secure data collection and analysis process is comprised of the following:

- Manual and automated data collection of internal system and 3rd-party vendor system data.
- Manual and automated storage and organization of that data.
- Manual and automated data processing and analysis.
- Concise and understandable presentation of the processed data.

- Manual and automated project management and monitoring related to risk mitigation.

While it does not exist today, the ultimate goal is to have a GRC solution that provides on-going, real-time, internal system and 3rd-party system data collection and monitoring after the initial RA, data collection, and analysis are done.

Data Input Sources

Whether or not a GRC solution is capable of ingesting and processing the various potential data input sources is an important consideration. Many potential data input sources exist. They include:

- Questionnaires (self-administered or live).
- Inventories (data, hardware, internal applications, SaaS vendors/apps, configuration, IoT, IIoT, SBOM).
- Vulnerability and penetration testing.
- SIEM data (log, monitoring, EASM, MXDR, etc.).
- 3rd (and 4th, 5th, & 6th) party SaaS application/vendor data (industry specific data, training, etc.).
- Database data (CMDB).
- Incident response.
- Threat intelligence/law enforcement data/other threat intelligence (TTPs–tactics, techniques and procedures). This is fed into a SOAR process/solution.

Data Analysis/Output

Once the data has been collected, it must be organized, processed, analyzed and formatted for presentation to the end-users,management and the board of directors. This includes:

- Organize/prioritize vulnerabilities revealed by questionnaires or live assessments
- Organize/prioritize application inventory/vulnerability information
- Organize/prioritize vulnerabilities within assessment/scan reports
- Organize/prioritize answers provided by the client via self-assessment
- Organize/prioritize CMDB database vulnerabilities scan
- Ingest law enforcement/other threat intelligence and apply to the RA environment.
- Generate reports for management, the board and other users.
- Build PoAM and incorporate it into the project management process.

Ideally, all data inputs are fed into an automated machine-learning application for analysis, prioritization, response and reporting to management and the board.

Whether or not any one particular GRC solution has access to all the above data types or is capable of correctly processing and reporting on that data must be determined.

6. Data Collection and Analysis Challenges

In our opinion, most current GRC solution providers mostly offer a glorified checklist with a dropbox for saving artifacts. The solution is basically a project management solution with a document repository. Good stuff...it helps people get organized,but it does not improve the quality of the result.

What is needed is automating the collection of usable data, but doing so is difficult.

APIs and Associated Processes

A useful GRC solution should have APIs designed to allow users to collect all the application data their customer needs using automation in order to understand their IT infrastructure. Additionally, (and ideally) these APIs should be “out-of-the-box” and operate in a fully automated manner–with minimal client interaction and custom development required. The client may be required to make some basic configuration decisions and provide some minimal inputs such as: user IDs and passwords to specific applications, date ranges of desired data, customer numbers, etc.

Some GRC solutions are robust in this regard. Vanta is an example of this and they provide extensive API integration information and support to clients.

Most GRC solution providers claim they are “API First.” This insinuates that this API automation requirement is built into their solution. However, even if the application is built around the concept of APIs, that does not mean that the vendor has exposed those APIs to their customers. Upon closer examination, we find that before you will really have an automated GRC solution, in many cases, you must work with an internal or external development team to integrate any GRC solution providing APIs to applications where you want to collect data. This requires the cooperation of the GRC solution provider and any SaaS applications that have the data you want.

Some GRC solutions have built many APIs that you can use and others have built none. In some cases, the GRC solution will not let us import our desired data due to limitations of what internal data structures are exposed by the API.

Assuming that there are issues with the process above, you’ll need to determine how robust the GRC solution’s capability is to integrate data which is of interest to you.

Here are a few questions to ask:

- How comprehensive is the out-of-the-box solution?
- What data are you interested in from the application you are looking at and what data can you import into the GRC solution?

If you have a dev team and you have a budget and you have time, which of the things above can you do with the various solutions?

Inadequate Risk Assessment Processes

For modern IT infrastructures, the following, interconnected systems and associated data must be analyzed as part of an accurate and useful risk assessment:

- The internal on-premise and cloud IT infrastructure.
- All 3rd-party SaaS vendors that have access to your systems and/or that you use to store critical business data.
- All other vendors that have access to your systems and/or that you share other non-public data (infrastructure, service providers, staff augmentation, dev teams, etc.).

Based upon the NIST Cybersecurity, Privacy and Software Development frameworks, the following high-level areas must be correctly assessed in order to understand any enterprise's true risk profile.

1. Governance: board and management engagement, policies, risk analysis, regulatory, compliance, etc.
2. Assets: hardware, software, data, vendor and SBOM inventories
3. Technical assessments: system access control, data security, system security, maintenance, and monitoring, etc.
4. Vulnerability detection, response and mitigation
5. Supply chain: vendor risk, etc.
6. Awareness and training
7. Resilience: incident response, disaster recovery
8. Secure software development
9. Threat intelligence

It quickly becomes apparent that current GRC solutions are not collecting anywhere near the quantity and quality of information required to perform risk assessments that accurately represent the risk that your company faces and that your board and management need to mitigate. Unsurprisingly, this report verified that statement.

Vendor Cyber Risk Management

In order to accurately represent risk to your board and management, you have to repeat everything you have done above with all vendors that have access to your systems, access to your data, or to whom you provide data in order to conduct your business.

Almost all of the reviewed GRC systems are unable to collect log data and configuration data from vendors. Only the most expensive systems allow you to collect such data from such widely used SaaS apps such as Adobe, Drop Box, etc. If you have, for example, 100 different vendors (which, by the way, is a very low estimate for most companies nowadays), the problem is really 100 times harder than it already seems.

During the manual compliance assessment (self or consultant-led), most assessment questions are focused on only the top-level compliance requirements. This results in incorrect/incomplete risk assessments that do not meet management requirements. Correct assessments will go three or four levels deeper in an attempt to accurately ascertain the correct situation.

During the manual compliance assessment (self or consultant-led), most respondents either don't know the correct/full answer or bend the truth. This results in incorrect/incomplete risk assessments that do not meet management requirements.

Limited or No Data Analysis Capabilities

Do today's GRCs do any manual/automated data analysis? No. If you talk about a small sliver of the pie, then there are some small amounts of data being analyzed. They will give you a score based on the answers you lied about and then give you a score on your lies. What is the true quality of the result? Should management put any trust in the numbers coming out of that?

7. Security Challenges

Anytime multiple IT infrastructures must communicate and share data, security risks increase. In the GRC environment, the GRC solution provider's systems must access the client's systems and those of multiple (and many) 3rd party Saas applications and store that data inside the GRC solution. This is clearly risky business and care must be exercised when evaluating and architecting the interaction between your systems and the GRCs systems.

Security scenario 1: The GRC solution has developed and/vertically integrated all the required data gathering/analysis solutions and can internally control all client and 3rd-party system data collection and analysis. In this best case scenario, the owner of the GRC solution is positioned to address the greatest number of security issues/risks.

Security scenario 2: The GRC solution is dependent upon internally or externally developed APIs in order to access and share data with third-party SaaS applications that contain client data.

In this case, the client system, the GRC solution provider system and the 3rd-party SaaS applications are all talking to each other and sharing data. The GRC solution provider must now assume responsibility for the protection of all client data and systems involved in this multi-party situation.

In this case, the owner of the GRC solution must ensure the security of not only their system but those of the data partners, as well, since they all have access to the GRC solution owner's clients' systems and data. If the feed from the SaaS application is read only, then there is much lower risk to the GRC solution provider. If this feed is bi-directional, then this is a much larger threat.

Security scenario 3: The client or the GRC solution provider creates a protected data warehouse and imports the relevant data (in real time) into the data warehouse. The GRC solution integrates with the data warehouse. This type of architecture shifts the reliance for integration and security from a third-party vendor to the company being assessed itself. Companies with a high requirement for secure data can create or implement the API integrations and are not dependent on the GRC solution provider to do it. Also, when the data collection sources change API or other requirements (a fairly common occurrence with SaaS applications), the client can quickly respond and is not dependent upon the GRC solution provider to release a new version of its GRC solution.

8. Solution Pricing

At this point in the evolution of our GRC Solution Assessment process, we have collected pricing information via two sources: 1) the solution provider's web site and 2) open-source data gathering. In many cases, pricing looks incomplete. For obvious reasons, solution providers don't want to advertise this information. During phase two of our assessment we'll be reaching out directly to the solution providers to collect this information, so please check back with us.

Pricing for the forty GRC solutions we reviewed varies widely. Many times pricing is predicated on the number of users or the number of GRC modules the client wants access to. Also, buyers should ask about set-up and other charges.

Here are a few examples based on our very limited information thus far:

- Metric Stream charges a one-time $90,000 fee.
- One Trust charges $15,000 per module.
- Scrut charges $10,000 per year.
- Vanta charges between $7,500-15,000 per year for 20 users.
- SAP charges $25,000 per year plus a $6,000 setup fee.
- NavEx runs between $31,200 and $78,000 per year.
- Witfoo charges $60-80 per user per year.
- IBM is $75,000-100,000 per year.

NOTE: Our full analysis and pricing information is available in our 2023 GRC Solution Assessment. If you would like a free copy, or if you are a vendor who wants to update our pricing information, please contact us.

About the Authors

Raymond Hutchins Managing Partner rh@cybercecurity.com 303-887-5864	Mitch Tanenbaum CISO/Partner mitch@cybercecurity.com 720-891-1663

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/

CyberCecurity, LLC offers full board support including recruiting, training and consulting. Please go here for more info: Cyber Board Talent

Did you find this position paper of value? Here are some of our other papers and reports:

1. Questions to Ask Potential GRC Vendors (please request)
2. The Global Cyberwar and Societal Response
3. Privacy Laws: An Executive Overview
4. Hiring, Managing and Firing MSPs
5. Caremark and More Propel New Board Risks