**How to Understand the Real Role of a GRC Analyst**

**(The 8 Laws of GRC)**

**By Maryam**

**Welcome**

If you're reading this document, I assume that you're probably embarking on your journey to becoming a GRC (Governance, Risk and Compliance) Analyst, a role which has around 750,000 vacancies in the USA alone.

As Techpreneurs Club, we understand that we’re living in the age of the “solopreneur”(people who want to own businesses and ditch the 9-5), however most of you are probably just craving the financial and time freedom that a well-chosen career can actually provide.

GRC roles are in demand across all industries, pay in the six-figure range and many of times have flexible hours.

No wonder cybersecurity is becoming more and more popular.

However, the hype has now caused a lot of confusion as to what GRC Analysts actually do, how compliance is related to cybersecurity, and what the day in the life of an Analyst actually looks like. We address some of these topics on the Techpreneurs Group on Facebook and we’ll go into further detail as time goes on.

For now, I'm going to delve deeper into the habits you need to build in order to work in this field and some lesser spoken about issues that you need to keep an eye out for.

Before we begin, let's talk about what the standard definition of a GRC Analyst is.

A GRC Analyst assesses a company's likelihood of experiencing a security breach by analyzing their security practices, then making sure that they comply with the correct regulations according to the current business practices and objectives that they have.

The consequence of non-compliance with security and privacy regulations can be imprisonment for c-suite executives, companies being fined in the millions that can drive them into debt, and the destruction of a company’s reputation.

See yourself as a middleman advisor that can protect the interests of customers who give their information to these companies, and the businesses that are trying to make sure that they can continue operating into the future whilst protecting their online presence and safety.

Not only will this help you break out of the employee mindset that can act as a mind block to you providing consultant-level advice, it should also help you recognize the value that you provide to organizations is of great importance.

With the following “8 laws of GRC”, you’ll understand how to compact this value to elevate your worth (and therefore income) within the job market.

***PS: In this guide the titles, Security Analyst and Compliance Analyst are used interchangeably to refer to the GRC Analyst position which all involve similar roles and responsibilities***

1. Understand Technical Terms:

GRC is branded as the least technical entry-level role in the whole tech industry. Although it’s less technical than being a hacker, you still need to learn the basics of network security in order to do security interviews with different departments within a company. There are many Youtube channels that you can use to build your knowledge as a complete newbie to IT.

Within our Techpreneurs Club Facebook Group we hold a weekly podcast where we teach our members how to build essential cybersecurity and compliance skills. In our third podcast episode, Marcus (a GRC Analyst who’s worked a year in the job) and I discussed our favorite resources for learning IT security and we shared how we would improve our self-study methods if we had to start all over again.

[Click here to watch that episode!](https://drive.google.com/file/d/1HbymHqjkI1G937Z2pCj45wJ-cYQqrbAd/view?usp=sharing)

1. Self-study:

Leading from our first law of teching yourself cybersecurity concepts, self-study is equally as important when trying to make it in GRC. The threat landscape changes so often so there are new risks with matching solutions that you would need to be aware of to give legitimate advice to the executives that you report to.

In order to study regularly, you need to be able to manage your time effectively. To help with this, I’ve created a [time management podcast episode](https://drive.google.com/file/d/1cfiqBv0GIej1M3DtZXKq1DeHf9GtN6iY/view?usp=sharing) with Marcus where we discuss our methods of balancing our personal and professional responsibilities. Also, we have a [worksheet and guide](https://docs.google.com/document/d/1yuO_qhc2vNHDscTJImBTfxxSeecYwSExeM-MZ-rnG8U/edit?usp=sharing) that you can use to practice planning out your day so that you guys can create a new routine that will compliment your transition.

1. Know How to Ask Follow up Questions

When speaking with an expert in Software Development, he mentioned that when Compliance Consultants approach him for security interviews, they often try to read questions from the Sig Lite questionnaire verbatim. The staff at his company could sense that the consultants had no idea of what they were talking about, and started to disrespect or outrightly lie in their answers.

Having great technical skills will allow you to create fantastic follow up questions if you’re not satisfied with the answers that you’ve been given!

Here’s a good example:

If a Systems Administrator for a company tells you that they comply with password standards based on a specific framework or that they delete employee login data within 30 days of them leaving the company, you should ask for evidence!

The biggest lesson here is to not take anyone’s word for something if you know that you can cross-check the validity of the information.

You could create a throwaway account and try logging in to see if you actually have to meet password standards before accessing a company’s database.

Keep this in the back of your mind during every risk assessment.

1. Know When You Need to Get Certifications:

Contrary to popular belief, you don’t actually need certifications to get a job as a GRC Analyst. Some of you may have already completed the CompTIA Security+ which gives you a good understanding of IT and network security for when you first start out.

However, as you progress through your career, there are certain certifications that signify to employers that you’re advanced in your knowledge. These three main certifications are:

CISA: Certified Information Systems Auditor

CISM: Certified Information Security Manager

CISSP: Certified Information Systems Security Professionals

Though these are usually for people 3-5 years into their career, they can still be done earlier on for those who want to start off consulting rather than working in-house. For now, focus on your ability to meet the key performance indicators that companies prioritize. This may include:

* Response time to a data breach.
* How many people will complete the security awareness training that you create.
* How much the risk of a company has reduced after implementing your security solutions.

I’ve made a video assessing job description requirements in the GRC space and went through how you can meet the standards. We also review how security teams are set up and how that determines the communication flow during an incident response.

[Click here to watch that episode!](https://drive.google.com/file/d/1UdJw4Xw0lqBIQCevxkUZB0F8Wak4Y2bv/view?usp=sharing)

1. Security and Privacy Analysts are Different

Security Analysts ensure that a company's online presence is at its lowest risk from cyber attacks whereas Privacy Analysts ensure the data protection of those customers who give companies their information, perhaps in a form, and inform customers about who their data is being shared with.

As you’ll come to know, Security and Privacy Analysts have similar roles in terms of helping companies comply with compliance regulations, but the depth of knowledge that’s expected from each varies.

Privacy laws tend to differ across regions of the world, and particularly in the United States these can vary from state to state. Many Privacy Analysts have practiced law before, and in fact, collaborate with lawyers when drafting state privacy policies. A very common privacy law that GRC analysts are expected to know is the California Consumer Privacy Act, which is, as implied, implemented in California/ California-based businesses of a certain size. On the other hand, security frameworks and standards like NIST CSF and ISO 27001 are seen as international requirements for companies.

Many Security Analysts use their knowledge of local privacy laws in the location of the job role that they’re applying for as a competitive advantage. Temi Akinlade, a virtual Compliance Consultant that I interviewed earlier on in the year, shared how he used to do this.

[Check out our interview on how he built his personal brand within GRC.](https://share.descript.com/view/JFjXAT6Rfgl)

*Quick Top Tip*

You should be looking to work in organizations that already have a General Counsel (which are in-house lawyers) within them so that you can have guidance in understanding how a security program works and is adapted overtime. Some organizations do not have a security program in place and oftentimes the law (privacy) acts as a foundation to implementing other relevant regulations.

*Misconceptions*

**Security Analysts need to implement the program.**

GRC Analysts are first and foremost advisors for companies. These organizations must use the monitoring report from your risk assessment and decide whether or not to take action from it. This means you’re not liable to any fines that the company incurs for not complying with regulations.

If you feel nervous about giving the “wrong advice” remember that the Chief Information Security officer (CISO) is responsible for developing and leading the information security program. Therefore, they’ll cross check your work. Even as a Compliance Consultant, you may be working under a Manager or Lawyer so you’re not completely alone in your decision making.

1. You Must Spot Red Flags Within a Company’s Work Culture

In order to get the work life balance that you dream of, you need to focus on the culture of the company that you work at.

One of the best ways I do this is by using the website Glassdoor that shows company reviews from existing employees. This helps you get an idea of the company hiring cycle, what a typical work day is like, and even the interviewing process which will help you prepare for it.

John Rouffas, a part-time CISO gave me his advice on how you can cross check organizations to increase the chance of entering a work environment that honors your mental health.

[You can watch it here.](https://share.descript.com/view/r9BvgiYddy3)

1. You Must Have Public Speaking Skills

Whether it’s you being interviewed for a job or interviewing companies as part of a risk assessment, you need to know how to speak to a group of people, confidently, accurately, concisely. Some of you may find this difficult and will feel uncomfortable in this process, but within our Techpreneurs Club Facebook Group we will be practicing body language and speech exercises that will polish your presentation skills for your audience.

Keep in mind that you’ll be presenting results from your risk assessments to c-suite executives so the language that you select is important as well. For example, never contract words in formal documents.

A good way to learn these presentation skills and revise at the same time is to tune into cyber news. In interviews, you will be asked about how you keep up to date about changes in the threat landscape and you should reference the cybersecurity shows that you watch.

We have a [resource page](https://drive.google.com/file/d/1i5BXPE1oD7m2IW92Q6UkoXLVhN9jACHZ/view?usp=sharing) where we share a list of the shows and podcasts that we watch, misconceptions within cybersecurity that need to be cleared up and YouTubers who teach people how to make it into the compliance field.

As you build your skills, you should be able to apply certain cybersecurity stories to incidents you’ve seen in your personal life because your ability to connect your theoretical knowledge to a company’s situation is one of the main indicators for a recruiter to gauge your level of talent.

1. Be Patient

The final law to mastering GRC is by appreciating the level of patience it takes to go through the whole process.

* It takes time to understand concepts in IT and GRC enough to create your own independent analysis of certain situations.
* It can take time to do security questionnaires and make sure that your answers are satisfactory.
* It may take a while to be able to speak about GRC fluently to company stakeholders and be considered an expert by them.

Internalize this before going forward in this journey as the beginning stages are usually the part where people start to feel down or discouraged with their progress. When you understand that you are actually supposed to be studying and learning along the way, you won’t be hard on yourself when things aren’t perfect!

**The End**

Thank you for going through this list. Make sure that you keep it on hand as you go through your GRC journey. Remember to read through all of these resources and make sure that you understand them thoroughly.

We have weekly Q&As on Techpreneurs Club’s Facebook Group if you’d like to ask questions about anything that you feel unsure about. Along with even more podcasts, competitions and testimonials from people in the GRC industry to help guide you along the way.

If you haven’t already joined our Facebook group, [click here to make a request.](https://www.facebook.com/groups/techpreneursclub/?mibextid=oMANbw)

Thank you.

**PS: Please answer all of the membership questions if you want your application to be considered.**