**Governance, Risk, and Compliance (GRC) in ServiceNow GlideFast Consulting** [**link to video**](https://www.youtube.com/watch?v=TQdhyAZxDCo)

GRC is a multidisciplinary set of applications that are designed to shift the visibility of risk and compliance standpoint from the weeds (where people tend to spend their time) up to the 30K foot level (where a complete overview of risk and compliance standings can be gained by the C-Suite).

It also shifts responsibility from maintaining compliance and managing risk from those that are supposed to be in oversight (your RC managers) to those at the desktop (server engineering team, network engineering team, help desk etc).

It shifts processes from spreadsheets and databases scattered across business areas into a single port of reference for all the interconnect architecture and processes.

**GRC = Maintaining Compliance for Enterprise**

When discussing GRC, we’re talking about the idea of making sure we’re looking at things in the system which present risks or are required to be maintained compliant. This impacts servers, VPs, departments, applications etc. Anything can be part of GRC.

We have a system in place that is designed to keep enterprise in good standing with federal regulations.

Within the system, our **decisions for how/when we do [thing] is the Policy**. Prescribing the policy for how and when to do [thing] is evolving, conditional, and sometimes shifts with the view of “why” and “how” things should be done. It includes details, outlines, specifications, and best practices for completing the task. **Policy is instructing someone “This is how you should do [thing]”**.

**Promulgating the Policy to Enterprise is Policy Management.**

When we set expectations, set timeframes, design controls, and test for effectiveness through **monitoring and verifications**, this **is Governance**.

We shift policy and redesign controls according to **Audits** which **review current practices and make recommendations for improvement.**

We use the results of audits to emphasize the **Risk** of **what we can expect when we don’t update policies and use available controls**

When configuring and implementing GRC, the upfront configuration is where we spend most of our time. 90% of the project is gathering documentation, business process documentation, and configurations.

Utilizing the information, frameworks, and current risk statements (what you have identified as the risks the enterprise faces) provided from the organization’s risk management applications (such as RSA Archer), we review everything in the system that can be impacted and label those as **Entities** (servers, VPs, departments, applications etc).

We look at the authorities. We talked about policy management inside the home and those are internal policies, and every enterprise has an internal policy and ways of documenting them. Maybe they keep them in SharePoint. Service now has a policy management process and repository as part of policy management. So policy management and policy acknowledgement and the authority documents that come with it that's the external side of the house. If the policy that you set for yourself to brush your teeth is the internal side, the regulations or recommendations from the American Dental Association are the authority documents that's from outside. The IRS, the ISO, the federal government, any state and local government, any country, nationally, any international body that promulgates regulations, standards or laws would be considered an authority source and have authority documents. The pieces of those are your citations and those are the things we have to actually pay attention to.

All of that brings us to a control objective and that's just a template what should we be actually doing on a daily basis we should be configuring applications to require passwords that our date characters long at minimum 12 characters long at maximum and have an uppercase and a lowercase and a special character and a number that's a template it's something we should be doing once we've got all of that documented and we put that all into the system we let ServiceNow do what it does and that's automation. The whole goal for ServiceNow GRC is to automate, as much as possible, the management of GRC and put the responsibility at the desktop. If we set this up correctly, we end up with a bunch of entities (items in service now that must be maintained compliant or could present risk) and they're automatically generated for us from the source data tables, the risks are automatically generated for us, the assessments of those risks can be automatically generated for us. Indicators which are basically just bits of code that monitor things for us without getting anybody's perspective are automatically generated. Test plans and controls and attestations within compliance are automatically generated over time as people do their jobs and that's really the key. Getting it to the desktop, looking at daily operations as the CMDB is maintained correctly, as VIP's are noted as such on their profile, as applications are monitored and maintained and retired, all of the automation keeps running with the goal being that as a risk or compliance manager, when I log in every morning I see the ever changing architecture of what's actually going on. When an application is retired, the risks and the controls that have been monitored for that get retired as well automatically. If a new application is rolled into the enterprise and it's activated, it automatically appears and the risks and the controls automatically appear with it so it gets the risk and compliance managers to the point where they are monitoring on a daily basis things that are happening instead of trying to figure out what should be there or what applications or what servers or what VP's need to be monitored. The system does it for them and all they have to do is monitor the end results.

Hopefully they get to that point and we bring in regular verification. This is the audit side of the house where people come in and maybe it's an internal IT audit and they audit how well controls are designed and how well they're actually implemented within the enterprise. They look at specific entities and say well we're only going to test our server controls this month and next month we'll do our application controls. And we have test plans that help us actually look and define for us how we can really get into the meat of daily operations and figure out is this really right for the enterprise, do we need to change how our controls are designed or do we need to change the processes where we implement controls and apply them, do they both work correctly.

And then of course we get into the remediation of any issues. Those are issues within servicenow that again go back to the desktop. If the control's not compliant it's because something needs to change at the desktop level. Maybe it's the server engineering team or the network engineering team that needs to do something just slightly different to ensure compliance with a specific regulation. That's issue generation. It gets management into the oversight role and puts compliance and risk mitigation down to the desktop.

It's really a change in perspective and a change in culture and that's probably the most important and most difficult part of GRC. Upfront configuration can take as little as 20 days. I've taken a client from nothing to full GRC risk and compliance in 24 days. They left it completely out-of-the-box. They knew what their documentation was, what they needed, we put it in, we rolled it out, and then they started making you know logging enhancements for later on. Some projects the documentation is so tedious that it takes two or three months but if you get the upfront configuration right and you get the buy in from the daily operations teams, the people at the desktop, you can achieve and it has been achieved. 100% compliance through audits being able to pass an IT audit in record time with record compliance is not unheard of. In fact it's more common but the more mature and comfortable people are with GRC, with the responsibility that comes with it so it can be done it's just it can be a tedious process especially up front.

So when it comes to what's in GRC and what's in ServiceNow the key is whatever you want to interact with has to be in ServiceNow but once it's in ServiceNow there's nothing that you cannot get to. Except for HR. HR with its special security controls is not available to GRC without customization.

But departments, vendors, the CMDB, the user table, any custom tables that you have, vulnerability response and security incident response, the request, incident, problem, and change processes and data, all of that is available for GRC to dig into; and because those are available any of the relationships are available as well.

I once had a bank they basically had a problem with their change process. they felt that there was a good chance from the incidents and problems that had occurred that change tasks were actually being done without proper approval. so being able to dig into the relationships of change requests, change tasks, and approvals allowed us to see that in six months’ time out of 2600 change requests 60% had a change task that was activated and completed before the approval had been given to do so.

so the idea of the relationships behind the scenes along with all the supporting data being available to GRC allows you to look deep into business processes and figure out where the issues actually reside. basically what's available to GRC to interact with is anything and everything except HR. as long as it's in ServiceNow. so if you're getting data from SolarWinds and Nagios, or you're pulling in vendor risk assessments through the VRM, or you're using SecOps or Qualys and Tanium or Rapid7, and all of that data is available to GRC to dig into the business processes and figure out where you need to change those processes to remain compliant, or where your elevating the realization of risk and those processes need to be changed we need to mitigate that because of it.

once you have installed the GRC plugins: policy compliance, vendor risk, audit, and there's risk. if you If you decide to go with the advanced options there's advanced risk assessment and risk events this is the Orlando version so there's a lot of information in here and a lot of options

policy compliance has a great deal of opportunity when we look at the data that can be provided to individuals. you're looking at an overview of compliance for the enterprise for a lot of different regulatory sources when we talk about the security and privacy controls, and ISO 27001:2013, the PCI DSS (payment card information for credit processes), the critical security controls, or even going in as far as the CobiT and the FedRAMP regulations all of those are available to us so we can look at compliance for the enterprise from that standpoint. There is also standard data/charting.

There is a PA version where we can activate performance analytics if you have performance analytics then this is available to you you have to subscribe to performance analytics in order to get it and basically all it does is add additional filtering the interactive filters that you may be familiar with performance analytics is just added to the different dashboards but when it comes to the overall compliance that's the data you can get into.

from an internal standpoint the same type of data is also available. so looking at internal policies so policy overviews exempted controls so policy exceptions your compliance score percentages and issue counts over time. all of this is provided out-of-the-box. a lot of clients when they see what's provided out-of-the-box from a reporting standpoint they're just blown away. this is just demo data but when you show them what's available and how they can dig in just through ongoing operations of running controls, documenting risk, and going through audits, it really kind of blows them away because this is basically what they've been looking for and never knew that they needed it. I don't know how many times I've actually heard of that

Policy Acknowledgement is actually pretty new and it's basically the idea of if I'm going to create a policy I might want to go in and see how many people have actually read that and acknowledge that it exists. it allows you to create a campaign of surveys where you can identify the audience that is impacted by that policy and gather a person-by-person's perspective of whether they have acknowledged it. So if you have not read the policy here you've declined to read it or you feel that you're exempt from the policy it will gather all of that information for you no more using SurveyMonkey.

Policy exceptions are the idea that you may have a policy in place but it does not apply to me or it does not apply to my application or to my server or to my entity. sometimes this is the case. some applications that are homegrown believe it or not I have clients that still run them on old versions of Windows enterprise server that are not secure anymore but they don't have a choice because they would have to rebuild the application or find something else in order to get rid of that Windows Server so they have to have an exception to the policies and the controls that are in place and this is where you document them

we talked earlier about the idea of what's accessible in ServiceNow and this is the idea of scoping. we all scope projects but the first scoping of a project for GRC is the scoping of the entities. we look at the scoping of entities and we say what are the applications in the system; what are the business capabilities; what are the companies, the computers, the databases, the departments and the facilities; anything in ServiceNow can be a (entity) class and can be an entity and we find those by running simple queries.

basically you can say what are my data centers; I'm going to look at the risk and controls around my data centers; and right now I have one in New York.

the best example of risk and compliance for facility that I can come up with is the concept of a volcano in Hawaii. I had the fortunate experience of living in Hawaii for two years and visiting the Big Island. the volcano on the Big Island hasn't done much but of course with all volcanoes you don't know when it's going to do something. bank America has bank locations all across the United States and in Hawaii when I look at data centers and facilities, if I have a data center or a facility on the Big Island of Hawaii I will have additional risks and controls for that specific location that don't exist for everything else because I have an additional risk (the volcano that's sitting there next to me).

this allows you to dig into the data in your system that is maintained through the normal course of business operations and apply controls, risks, and policies to specific items or classes of items, and maintain compliance and risk, and monitor that discrete specific fashion.

The entity type record is the hub. it is the most confusing lengthy process of all of the GRC processes in my experience. the concept of what do you find presents the most risk, what needs to be maintained compliant, getting into the weeds of that is where you really have to start and the entity type is the hub.

As we identify the frameworks (the physical and environmental threats, the financial threats, the operational risks for the enterprise) that's where we start identifying risk statements and we'll get into those in a couple of weeks

Risk statements are just basically generic general statements of what might happen but we can identify the various entities the data centers, the facilities, the applications that those statements apply to, and those give us our risks that can be discreet. And

we have our internal policies: what we have promulgated that we say you should do and how should you handle things

the control objectives are the external standards. these come from different ISO 27001and NIST, RMF, and CoBIT. the control objectives come from the external regulations but they can be tied to the internal so they can maintain compliance at both sides

the filter is where the magic happens and of course that's where we simply dig into a table somewhere and we apply the attributes and we basically say well I'm going to look for all data centers that are active and I'm going to assign anything for that data center either risk or control to the owner of it (the person who manages it) those basically come up with a list of entities and

From the entity record we end up with a list of risks and controls. as you can see this one is owned by an individual. It is 100% compliant. there are 4 risks that are assigned to it. there are 32 controls assigned to it. some of them are non-compliant. some of them are compliant. then we have the engagements where they've been audited. we have the issues that are currently being addressed through those audits. we have any tasks that need to be acted on for those engagements as well as any exceptions that have been submitted for any issues; and then if you're going to run the advanced risk and use vulnerability you would see any risk events and any risk assessments that are being done as well

So again the entity type is the hub it's where we always start and creation of an entity type. looking at the actual applications or servers that are part of a NERC SIP regulatory architecture setting up all of this is what allows the magic to happen behind the scenes regular basis. as things act as according to this filter/this query, as that data changes from a day-to-day basis the risks and the controls are applied, the entities are created, and those relationships result in new entities, new risks, and new controls.

if something falls out of this filter it'll go the opposite direction. any entity that is no longer part of the filter condition will be inactivated and any controls or risks will be retired. any in flight assessments will be cancelled. that's just part of the normal day-to-day operations. and again it gets down to the idea of who's actually responsible. it's not the risk manager and the compliance manager that are responsible for making sure that an application or a server is added and documented correctly in the CMDB. it's the CMDB manager. it's your network engineering team, your application developers, or your server engineering team.

Again it's the concept of getting responsibility down to the desktop so that management can have an oversight view of how the enterprise is truly being affected.

on the risk side of the house we get kind of the same thing: we have our frameworks; we have the overview of risk where we actually can sit. we can see the number of risks where the impact of the realization of that risk is very high and it's likelihood is extremely likely.

This is where we get into the concept of risk scoring and there are several different ways of assessing and scoring risk ServiceNow provides 2 out-of-the-box but they have a couple of integrations with other companies that do completely different style of risk scoring.

risk loans it's probably the most widely used outside of just the standard versions that we have here; and there's an integration with them that allows you to send them your data and they do the risk assessment outside of service now in their own systems and then sends it back to you after a couple of days later.

risk always has a financial factor. the realization of risk (which is basically I have a threat and a vulnerability, the two of them, should they ever get together will create the realization of risk and they will have an impact) most of the times there is a financial impact whether it's the cost of mitigation, or the cost of a lawsuit, or the cost of a payout. so being able to document the financial realization of risk is probably the second hardest thing that companies have to deal with.

So looking at inherent loss, the annual loss expectancy that I might have should a risk be realized is part and parcel of what risk management brings in. you'll notice that we have a scoping section here and scoping again it's all one in the same. scoping an entity is an entity. you run risks and controls and audits against that same entity. it's not multiple records but if I look at the entities and entity types it's the same here for risk as it is for control and the entities are exactly the same for risk and control and audit.

Audit again is just the idea of verifying that the controls you have in place are working correctly. you test two different ways: you test whether the design of the control is adequate and whether the application of the control or the performance of the control is correct. quite often what auditors find is that the design is great but it's not being implemented. it's much more common to have the operational factor of the control fail versus the design

The premium of course adds different interactive filters but basically this is just an idea of status of current audits. there's not a lot to be gained here other than this is how things are doing because most of the work when it comes to an audit is done on the issue side. issues are created and remediated as they relate to the controls and questions. This is why they work together so well.

you can run risk and do risk management without controls and without audits but you'll never be able to tell what controls are in place that mitigate risk unless you're running policy and compliance management

you can run compliance management without risk and audit but you will not be able to tell in service now how well you're doing applying those controls operationally and you'll never to be able to tell the mitigating impact of the correct application with those controls to the financial aspect of risk

if you're running all three together the overall gain is: this is what we do every day this is how well we do it and this is the money we're saving potentially by doing it this way.

If you can enforce that perspective on people who you're talking to about using GRC or people who are looking at it, it becomes quite clear that all three are vitally important to the enterprise. do you have to do all three at once? no most of my clients they run policy and compliance first. as part of a wave 2 they will add in risk and as part of the wave 3 they will add in audit. a lot of that is done because audit regulations require audits normally every 90 days and you can do all three in that 90 day timeframe. normally however they're in the middle of an audit as they're implementing some of the other two so audit is normally the last that people put in.

The 4th is like I said vendor risk and vendor risk is completely separate. it has a different entitlement skew, totally different billing cycle etcetera; but it's the idea of looking at the vendors who provide services to you and looking at how well they are doing from a compliance standpoint. You can run vendor risk by itself without policy compliance but what you lack if you do that is the ability to tie the controls that they're supposed to be adherent to to the actual answers that they're giving you vendor classifications by tier are basically what is the risk of using this vendor and when we look at issues that are created through this that the vendor can then help you resolve those directly impact the vendor risk rating and then your risk is 2 parts: there's the tiering assessment which is your internal perspective of how do your vendor managers feel versus the vendor risk assessment itself which is what does the vendor actually say looking at the two together can give you a very good overview of what is the risk to the enterprise of the use of this specific vendor

so these are the four primary modules and we'll be covering each of these in the next 4 weeks in detail so I wanna open it up now for if