**Risk Management in ServiceNow GlideFast Consulting** [**link to video**](https://www.youtube.com/watch?v=H7lMju4Q6gA)

GRC Governance Risk and Compliance is a combination of four different modules: Risk Management, Policy and Compliance Management, Audit Management, and Vendor Risk Management.

All four of the plugins are scoped. They can be used individually by themselves, but they do work best when they are all used together.

Risk Management is the process of:

1. Identifying the risks to the enterprise presented by the existence of internal and external threats and internal vulnerabilities
2. Evaluating the impact of the realization of such risk upon the enterprise
3. Prioritizing the addressing of risk according to the impact and likelihood of a risk being realized
4. Addressing the possibility of realization of a risk

Evaluating Risk

Two Options: Qualitative(subjective) & Quantitative (objective)

1. Qualitative analysis asks for the perspective of the involved business users regarding the potential impact and possible likelihood of a risk being realized.
2. Quantitative analysis asks for the specific financial range of impact and statistical likelihood of a risk being realized (cost of losses/recovery afterwards)

Responses to Risk

1. Avoid: removing either the vulnerability or the threat involved
2. Mitigate: reducing the negative impact or probability of likelihood
3. Transfer: transferring all our part of the liability to another party
4. Accept: retaining some or all of the potential or actual consequences of a risk

Risk frameworks are categorizations

Risk Statement is the enterprise view

The system automatically sees the entities that we need to monitor (it sees the enterprise risk statements that are related to them) and it will generate the risk themselves.

Advanced Risk Management lets us have a more operational view of risk. The Advanced GRC dashboard combines all the risk information with policy and compliance and gives up a single pane view of how risk and compliance are working together.

What you're looking at right now is the risk dashboard that shows the results of risk assessments and risk processing in a normal environment. The dashboards are very complex. We're looking at risk from multiple perspectives and right now we're looking at it from a qualitative standpoint. We're looking at whether the impact and this is what we talked about earlier we're looking at those high levels of impact and very low to very high we're looking at likelihood extremely unlikely to extremely likely and we're calculating the priority basically based on those two ideas those concepts.

From a standpoint of risk manager I would want to address these 2 before I address these 29. These are not going to bite me merely as hard as these 2 would. When we think of very high internal risks from an inherent standpoint we're thinking of the case analysis what is the worst possible level of impact. What is the worst possible likelihood that's inherent simply because we have a server and a network connection and a forward facing portal to the Internet that anyone can get to brings. Vulnerability there is inherent risk to that so the worst case analysis is always the inherent risk. Residual risk is our target. It's where we want to be. We want our residual risk to be much lower than our inherent risk because residual risk is if everything is going great. If all of our controls are compliant, if we're mitigating this as much as we possibly can, and we've transferred as much of the liability as possible, we've taken the steps to avoid what vulnerabilities we can't and this is all what's left over it's the best case scenario.

The difference between inherent risk and residual risk without policy and compliance is basically the perspective of we've done all we can but we can't really prove it and that leads us to the third concept of calculated risk which is what's left what is our real time when you look at how the business actually operates.

Let's go ahead and look at a risk and we're going to do so from the standpoint of the hierarchy. We've talked about our risk library is the framework and it's the way we categorize things and of course we have third party and supply chain threats to those. We have physical and environmental threats, business service laws, departmental, and corporate risks. These are all just categories. We'll go into the physical environmental threat, and we'll talk about the one that we talked about earlier and it's basically our data centers are vulnerable to physical and environmental threats. What are they? Well, there's an earthquake there's windstorms or tornadoes there's fires or floods. If I have something on the big island of Hawaii would have a fifth risk statement or volcano. Let's keep it simple and let's stick with fire from a standpoint of fire to the enterprise. Looking at the quantitative analysis I have a very high single loss expectancy. Any total loss for fire could cost me this much and that's huge however my rate of occurrence is very very low. When you put those two together it's going to give me a calculation but it's going to do so at the downstream level at the facility.

The residual is our best case. We buy insurance as the enterprise. We have insurance. We have controls in place. So our residual single loss expectancy is a much lower cost and because of that our rate of occurrence annually is even lower. This is where from a physical standpoint for facilities and assets we can usually get down to the penny. However, for the more conceptual risks of reputation and things like that we have to go back to the perspective of the subjective which we do by simply flipping a switch.

In the administrative section are the properties. Over into the correct scope because risk is scoped, and we'll go to the GRC risk application, and you'll see that we have qualitative impact and qualitative likelihood properties.

And the risk statement you can see now has a drastic change in its scoring we're now looking at the simple perspective of subjectively what do you think the impact will be and what do you think the likelihood will be. These are the standards. Out-of-the-box for simple risk. My risk scoring again is from an inherent and a residual standpoint: what is the worst case impact and likelihood versus what is the best case target impact and the likelihood.

We use the entity type to combine the two. So, the entity type for our data center goes out and finds the data center records and it uses the entity filter to find the data centers and create an entity record and the entity record is where we do our monitoring of risk and controls. The entity type is the hub, and we relate the entities to the risk statements at this point. We can also relate them directly to a framework and if we do then the automation will automatically relate the risk statements. And you can see we obviously have policies and control objectives from the compliance side of the house additionally related to this entity type. This is where you want people to get. You want them to be able to use both sides, risk and compliance, to mitigate risk and document that and we'll see that here in a moment.

The New York data center and looking at the New York data center we're going to see that it has four risks assigned to it. These are the environmental risks from the environmental framework. The earthquake, windstorm, tornado, and fire are automatically created because of the relationship that is defined at the entity type level. Let’s look at the fire risk. You’ll see that it looks very similar to the risk statement. It inherits a lot of information from its parent: the category, the statement itself, the assessment that's to be used, and the starting scoring is also inherited from the risk statement. This means that every risk that comes from that statement has a shared starting perspective.

When we look at what is submitted by the user though, that is where we get the perspective of residual risk. So this one is actually in a state where it is assess. The assessment has been sent to the respondent. The respondent can be the same as the owner but doesn't have to be. There could be a totally different person. The person is going to respond by filling out the survey and then we're going to review our score. This is where we talk about the difference in residual that target best case impact and likelihood based on the perspective of the user. This is where normally out-of-the-box we will adjust the residual impact. The inherent impact should be pretty much the same as the risk statement and it probably won't change unless something drastic happens; but residual is where we're always going to update according to perspective. Now you'll notice that the inherent scores both financial and subjective are still shown.

This is out-of-the-box and normally most clients start hiding things here. They don't want people getting confused and seeing annual loss expectancy or annual rate of occurrence on these forms. They'll start to hide anything to deal with aro. They'll just worry about the inherent scores. But let's see how this actually works together.

My inherent impact of very high but unlikely is going to give me my inherent score. I'm going to change this and say that it is actually very high and likely so our inherent risk is high. At the same time we can look at the residual side and we say our best case where the impact is moderate and our residual likelihood is kind of neutral. And both cases are going to adjust our scoring. This (residual score) is the overall risk to the entity based on the impact and the likelihood these two basically are only based on the impact and likelihood and they won't really change based on anything else. Now I’m going to save this and then we'll talk about the holy grail of risk management and that's where compliance comes into play.

You notice that I have controls that are related to this risk. They are compliant or non-compliant and some of them are not applicable and that's fine. What that means is that my monitoring is basically coming into play. For all the controls that are not applicable, I have a 100% compliance percentage. It’s fantastic, it's also very rare. The scoring then is that because I am 100% compliant on my control side, my overall (inherent) risk is the same as my residual risk. That's where we want to be. This means that our best case is being maintained on a day-to-day operational level. Our compliance efforts are basically keeping us at the minimum risk possible. Again, this is where we want to be. It's also pretty rare to have a 100% compliance rating for all the controls related to a risk it can be done you can get people to it but without a tool to show them they normally aren't there that's why GRC really exists it's to bring the compliance efforts and the risk management to the desktop level as someone in charge of the data center i want to know that here are the controls that are responsible for keeping me compliant and i can view those and these are the controls that help me maintain the minimum amount of risk to my data centers and to the enterprise. And I want to be able to see that. Very few applications out there have any concept of the relationship to this level of compliance and risk.

And we'll show you just how the two work together. This well now this is all stuff that can be configured by the risk admins not the ServiceNow admin. But the process admin directly in production. We talked about this last time where the compliance and risk admins have a lot of functionality available to them to maintain directly in production because ServiceNow considers it to be simple data. They can change the values of the risk criteria. They can expand the risk criteria. When we look at likelihood, the risk admins have the ability to say you know what I want a 7 point scoring system and they can add additional options in this table and adjust the percentile for lows directly in prod if they want to.

Our goal should always be to warn them against doing that and prompt them to work within the change management standards for their companies and say do this kind of thing in a sub prod through the standard change process to get those changes moved up into prod because you are changing the way the system works slightly even though you're just adding a data record. The same thing can be done when we look at not likelihood but the impact. You can add in impact levels.

and you'll notice that both impact and likelihood the quantitative values back to the financial values and for likelihood the statistical values of percentage. They're still there. We're not getting rid of them by moving to a qualitative side of the house but we're simply hiding them. The system is still using the values behind the scenes quantitatively to do the calculations for qualitative measurement.

And let me just explain what I’m saying here let's go back and look at our risk. The risk for fire when we look at it and adjust the impact and likelihood, ServiceNow behind the scenes is seeing a financial value corresponding to 5-very high and the statistical percentage corresponding to 4- likely. It is using those two values the financial and the statistical percentage to come up with a true behind the scenes financial value. And that's the annual loss expectancy that correlates to the inherent score.

This means that you can still look at reports and view reports that show you some of that data but it also means that people can get confused when you look at the overview we saw this I don't know if you could see this earlier but when you look at the overview presented even using qualitative analysis there are reports provided that rely upon the quantitative data you can see it right here the bubble charts look at the single loss expectancy that is behind the scenes for impact and the annual rate of occurrence which is the percentage likelihood so single loss expectancy is impact rate of recurrence is likelihood and these are still used and they can present problems if management looks at that and says well how did you get to $2,000,000 or $1.5 million of impact?

Well, we didn't. Because that's an out-of-the-box measure provided by ServiceNow for quantitative analysis. I see a lot of times those reports will be completely hidden. They'll be taken off the dashboards because except at the hardware asset and facility level they can't get to these dollar amounts. They can't get to the statistical analysis, so they'll take them off completely and only show the qualitative perspectives provided by their users.

The choices are also simply data points. for risks it's very simple, we're looking at tolerance and category. category is again a way to categorize different risks outside of the framework. we can have financial risks and operational risks or reputational or legal we can have credit risks and market risks and IT and those are just ways to categorize outside of the framework. the tolerance status we saw that as part of advanced risk but again these are simple data points the admins will have the ability to adjust directly in production if they want to. again our goal as consultants is to say stick with change management, do this in a sub prod, work with your admins to get the changes moved up during a standard change.

There are also a ton of other properties and options available to the risk managers many of which are the same as compliance management when we talk about entity classes and entity tiers. those are underpinning foundational concepts that all of GRC uses. risk managers do you have some of the same visibility as compliance managers. A risk admin is automatically a compliance manager. they can read compliance and they can view pretty much anything within compliance. A compliance Admin would be a risk manager to a certain extent because the two work together so well. And both sides have the ability to view anything within audit.

You can relate risk to vendor risk. vendor risk is what are the risks of using this specific vendor. if you look at how they are compliant and the risks that noncompliance on their side could impact the enterprise that's combining risk management, policy and compliance, and vendor risk into a single holistic view of what interacting with one single vendor can mean for the enterprise. you really want to drive people to do that. a lot of people use a lot of third party risk management and vendor risk management tools and they're very comfortable with those but nothing out there will provide a holistic overview of risk, compliance, and vendor risk altogether like ServiceNow does simply because they're all scoped apps that talk to each other and integrate directly within the system out-of-the-box.

When we talk about our risks we talked about how our risks are scoped and we've talked about how they are actually addressed from an assessment side of the house. so let's talk about how we respond to them. out-of-the-box like I said we have four different options to respond to a risk and in this case they've chosen to transfer the risk to a third party. now what this means is there is a risk response task that is created.

let's go ahead and look at a risk that's in the response state or monitor. we're going to group these by state and look at one that is specifically for a response. this is for the tableau application: the inability to grow in new markets for our use of this application is the risk for the project management team. in looking at this they have decided well the impact of this is very low, the likelihood is very low, they're both the lowest possible, and that means that basically the residual is the same. I can't get any lower in this stamp case.

though when we look at our controls and again this is kind of demo data we want to get to where our residual and our calculated is the same. from a response standpoint we can do one of four things. we talked about acceptance: accepting is I acknowledge there's risk and I'm OK with it; I'll deal with it; I'm not going to make any changes.

if I accept the risk I will get an acceptance task. the acceptance task is basically the plan for how you intend to deal with it should it ever occur and it does require an approval by the owner of the risk and the entity. it does go through a review process and you would expect a policy exception if you're running policy and compliance to go with this. Because if I'm going to accept it there's probably something that I'm not going to address from a compliance side that I will need an exception for.

now I can do as many of these in the response state as I need to. I can address the acceptance; if I do it's going to throw this back into review. I can say you know what let's avoid the risk, and I'm going to save this, and it will actually cancel that in flight acceptance task and say OK you don't want to accept it let's avoid it.

the avoidance tasks are very simple points of documentation how are we going to avoid this; we're going to upgrade our systems to the latest version; we're going to apply a patch that's going to get rid of the vulnerability. if you can truly do so and avoid that risk the next step would be frankly to retire the risk. if the risk has truly been avoided it no longer exists. One of the two points, the vulnerability or the threat, is gone. It’s actually probably the rarest used response because truly avoiding a risk is so difficult.

If I choose to mitigate a risk again it's going to cancel that avoidance task and it's going to create my mitigation task. exactly the same type of record, looks the same and if you look at it there's just a couple of different changes to the fields but it's what is your plan to mitigate this risk. And the plan can be reviewed once the plan is reviewed we can then look at any controls that need to be put in place and then work on those controls to further mitigate the risk

The final piece of the response is to say you know what I realized there's risk. I can't mitigate it. I don't want to accept it. I can't avoid it. So I'm going to transfer it. I'm going to buy insurance. The transfer response it will cancel the existing mitigation task and I get a transfer task. Now transfer does expect me to do a little bit more: who's the vendor we're going through for insurance, what is the contract (if you're using contract management and service now it's an easy way to maintain all of that information within the system but contract management again is optional and) you could simply provide the plan that you're going to work with with the vendor to transfer that risk. Once the response has been reviewed and closed, the risk will go to a review state and can then be Simply put into a monitor state. Now unlike policy and compliance, there is no way out-of-the-box to automate the re review of risk at a certain time frame. Risks are monitored until something happens that makes a reassessment necessary.

Now we'll talk about in policy compliance how that can happen but risks are simply, out-of-the-box, left in that monitor state until they're retired. That's the whole process: we define our frameworks and we define our statements of risk from an enterprise standpoint, we associate those statements to our entity types and let servicenow automatically create the risks for each of those entities, and then we assess the risks to figure out what is truly the impact and the likelihood. We respond to those risks by accepting, avoiding, transferring, or mitigating that risk. We then review our current standing. We can go back and reassess and re respond or we can simply choose to monitor that risk going forward. That's risk management in a nutshell.

But it's designed to put risk management, what you are doing in daily operations to maintain compliance or address risk, at the desktop level and it's designed to give the owners of the facility, the data center, the application, or the asset a view into truly what they are dealing with at a daily basis. That's the whole goal of GRC holistically: drive compliance and risk management down to the desktop.