**2. 9 Project quality**

**What Is Project Quality Management?**

Project quality management encompasses the processes and activities that are used to figure out and achieve the quality of the deliverables of a project. However, quality can be an elusive word. For project management, quality is simply what the customer or stakeholder needs from the project deliverables. By keeping the definition tied to the customer or stakeholder, quality management can have a narrower focus, which means it’s more likely to achieve its goals. Project managers oversee implementing a project quality management plan. The main idea, again, to deliver a product or service to the specifications of the customer or stakeholder. Doing so requires knowing quality management concepts.

**2.9.1 Customer quality expectations and Customer Satisfaction**

Without customer satisfaction there can be no quality. Even if a deliverable meets all aspects of what the customer or stakeholder has required but is done so where the process itself was not too satisfactory, then there is a problem. Of course, the deliverable must meet those requirements, or else the project has failed because the product of the project and the management of the project did not meet with the expectations of the customer or stakeholder. That is why implementing quality control means managing both process and people. Meet with your customer or stakeholder regularly to keep them abreast of the project’s progress. Get their feedback and make sure that you are being fully transparent with them to avoid issues arising later.

**Prevention Over Inspection**

Quality does not come free. The Cost of Quality (COQ) is the money spent dealing with issues during the project, and then after the project, to fix any failures. These are broken up into two categories: cost of conformance and cost of nonconformance. The cost of conformance can be considered a preventive cost. These costs are primarily related to training, the documentation process, equipment needed, and the time required to get the quality done right. Other costs related to this can include testing, destructive testing loss and inspections. The cost of nonconformance refers to internal failure costs. These consist of having to rework something or even scrap it entirely. Further costs can come from liabilities, warranty work and lost business.

**Continuous Improvement**

The concept of quality project management is an ongoing effort to address improvements of the deliverables over time. Whether through small, incremental changes or through large ones, the opportunity to identify and address change is always present.

Applying this concept also means constantly monitoring and documenting any issues that come up, so you can then use the lessons learned when managing future projects. This way, you run a more efficient project and likely will not repeat mistakes.

**Plan Quality**

First, the requirements for the quality of the deliverable and how the project needs to be managed have to be identified and Agreed on how this process will be documented and how that information will be delivered. Will you have regular meetings, emails, etc.?

The plan will include these specifics as well as metrics for measuring the quality while managing the project. This should include a quality checklist to collect and organize the marks you need to hit during the project.



**Quality Assurance**

Quality assurance is the planned and systemic activities implemented in a quality system so that quality requirements for a product or service will be fulfilled. Quality assurance are to make sure the processes identified are in fact working towards making the project deliverables meet quality requirements. Two ways to accomplish this is by using a process checklist and a project audit.

**Quality Control**

Every process needs a enforcer, so to speak, to make sure that the rules are being following and that the expected quality is being met. Some ways to ensure that the required quality of the deliverables is being achieved is through peer reviews and testing.

It’s essential to check the quality of the deliverables during the project management process in order to adjust the deliverables if they’re not meeting the standards that have been set. This *can* be done at the end of the project, but it’s not as efficient to redo rather than to readjust.

Having said all the above, in the present scenario, the customer expectations and deliverables are:

1. The draft IRP as designed by the CSO of Leighton+Costello has to be evaluated against the NIST publication”800-61-Computer Security Incident Handling Guide” and recommendations made on any changes that may need to be made.
2. An Incident Response Team Exercise (IRTx), as part of evaluation of the IRP and use the IRP and allow the security team of DataTrust in an exercise environment and see the shortcomings with a view for improvement.
3. Asses the effectiveness of Leighton+Costello incident handling processes
4. Assess IRT’s ability to detect and properly respond to hostile or abnormal activity.
5. Assess the IRT’s capability to determine the operational impacts of Cyber Attacks.
6. Expose the weaknesses in Cyber operations and policies as mentioned in point 2 and provide recommendations to rectify.
7. Whether or not the original timelines, that has been discussed and set has been adhered to?
8. Whether the projects are within the cost parameters that has been budgeted and had been stick to ?
9. Performance to Business case
10. Quality review for improvement at the end of the project phase, after considering, most of the IT projects affect quality like functionality, features, system outputs, performance, reliability, and maintainability. To this end, main outputs of quality control that are to be considered are – acceptance of decision by the customer, and if required rework, process adjustments, usage of some tools and techniques, if required, like Pareto Analysis, statistical sampling, Six Sigma, Quality control charts etc.

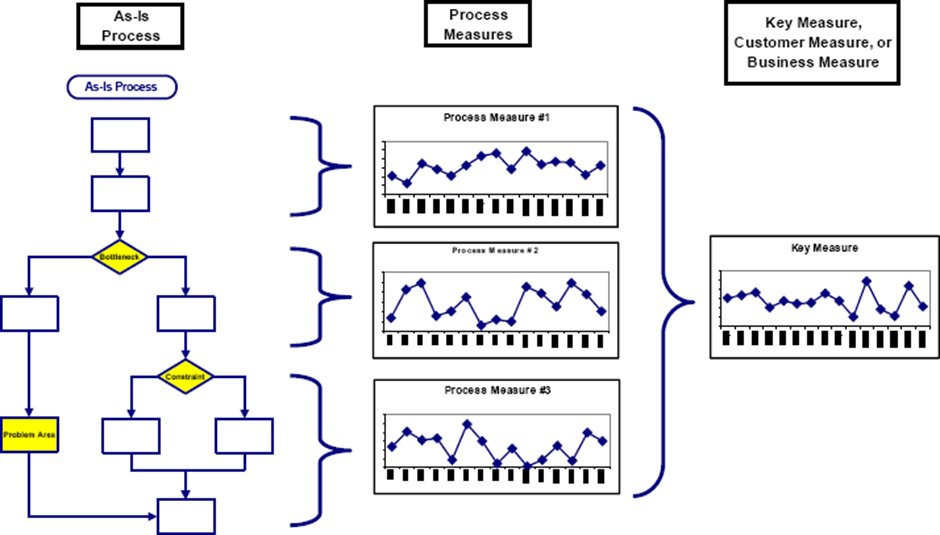
**2.9.2 Acceptance criteria**

1. The projects delivers all or most of the objectives and goals discussed with Leighton+Costello, and accepted by all the relevant stake holders. In other words, (a) it meets the business requirements (b) are delivered and maintained on schedule, (c) are delivered and maintained within budget, and (d) delivered the expected business value and return on investment.

2. All the activities related to satisfying the relevant quality standards for this project

3. Quality improvement

4. Quality Audits – to identify the lessons learned that can improve the performance on current or future projects. – Process improvement, fact-based management, and empowered performance of the future.



**2.10 Risk Management**

Technically speaking in a Cyber Security environment, Risk is really the intersection among organisation’s asset, vulnerabilities, and threats. Hence, to state parameters of Risk Management, it has to be understood as to what risk is, how we measure it, and how we can mitigate it to the maximum extent possible. Asset can be any item that has value to the organization. It can be things like workstations or laptops. It can be desktops or servers. It can be smartphones and mobile devices and tablets. It can be switches and firewalls and routers. Pretty much any of these things can be considered an asset. In addition to these tangible items, there is also some intangibles that could become assets, too. That would be things like information and data. It could also be the processes that are used in the organisation. It could be some specific software that has been developed by the organisation or that may have been purchased. It could also be organisation’s people. All these things make up organisation’s overall pool of assets that have to be protected. The organisation, having, all of these assets, need to start thinking and worrying about the vulnerabilities and the threats that are out there that are facing these assets and the risk associated with them**.**

A vulnerability is any weakness that exists inside a system. This may be because of the system design, organisation implementation, organisation’s software code, organisation’s lack of preventive measures. This includes things like software bugs, security breaches that can occur because there is a hole in organisation’s fence around organisation’s office building, or things like misconfigured software, misconfigured network devices, and other kinds of controls that are just not properly being utilized. Threats are any person or condition that could cause harm, loss, damage, or compromise of an asset.

Now, cybersecurity and IT professionals have to be aware that there are lots of vulnerabilities in our platforms and our systems. After all, there is no perfect computer system, nor is there any perfect network out there. So as a cybersecurity and IT professional, whole job is to manage the risk associated with these vulnerabilities. The purpose is to reduce the vulnerabilities, to the lowest level possible. But at the end of the day, there is still going to be some vulnerabilities out there. You can never eliminate 100% of the vulnerabilities, but you can control a lot of them through proper risk management. Because of this, vulnerabilities are considered an internal factor. This is something that is within the organization's own control. So while an organisation may not be able to stop the vulnerability from attacking organisation’s systems yet, an organisation, can control whether or not there's a bug in an organisation’s software. The organisation can decide and control whether the organisation’s IT department, install a security patch when Microsoft puts out a known exploit against one of their software products. Organisation can control whether or not to install a security device or a patch based on IT risk decisions and based on organisation’s IT vulnerability management program.

A threat (s)s is any person or condition that could cause harm, loss, damage, or compromise of an asset. These can be technical things like a cyber-attack, but it can also be something like organisation’s files being corrupted by ransomware. It could be a breach of data integrity. It could be malware getting into organisation’s system. All these technical things are threats that are out there that occur from outside of organization and outside of organisation’s control. Threats can also be natural disasters, though. This can be something like a fire, a flood, a hurricane, a tornado, or an earthquake. While an organisation cannot stop these things from happening, but, an organisation, can mitigate against them. And an organisation, does this, by attempting to manage the risk that is associated with these threats and their ability to harm organisation’s valuable assets. As a cybersecurity and IT professional, the IT department cannot control all the threats that occur outside of the organisation’s platform or organization, but yet can try to manage them and mitigate them. Remember, threats are external factors. Organisation fully cannot control them but can mitigate them and can manage them.

Thus, Risk is located at the intersection of our assets, our vulnerabilities, and our threats. Risk is the probability of the realization of a threat. That bad thing that may occur if it is realized and if it occurs, that probability of that happening is what risk is. Now, risk is kind of a funny thing because it needs both a vulnerability and a threat to exist. If you do not have a vulnerability, then there is nothing for a threat to exploit and therefore, there's no risk.

Conversely, if there is no threat, then even if there is a vulnerability that's present, there's still not going to be any risk. If one of those two things is missing, there simply is no risk. For example, if a hacker is attempting to attack the organisation, all day long, and they are trying to break into organisation’s network from the Internet, we have a valid threat. However, if we have no network connection to that Internet, guess what? There is no vulnerability there. And in turn, we have no risk of being attacked successfully by this attacker.

Another example might be if they are trying to run a Windows exploit against a Linux system. They are simply not be successful here. There is no vulnerability there to exploit, so no risk exists in this situation. Now, let's consider a vulnerability with no threat. As I mentioned earlier, you could leave the door unlocked to your house and it would be a vulnerability. But if there was no threat, then we have no risk of our stuff being stolen, correct? That is the idea here. When we look at risk in mathematical terms, we express this as vulnerability times threat. What we are doing here in risk management is constantly trying to balance the vulnerabilities against the threats that are out there.

Having stated all the above, under the Risk management, for the present IRTx, the following are the risk factors that may occur namely:

1. Scope change - After demonstrating the plan and prototype to the client – then the client changes the directions of the project.
2. Team cohesion – Lack of communication and team spirit among the team members in the respective team members feel that they are lost while in the middle of the project – being rudderless directions.
3. Project design and deliverable definition is incomplete due to the ongoing complexity of the project deliverables.
4. Team members become sick and become incompetent to finish their roles.
5. Adhoc and unplanned work schedules due to no direction or no supervision
6. Time delays due to dynamics of Realtime project scenarios
7. Cost overrun due to delays and unexpected expenditures like the IT infra failures and have to be replaced suddenly.
8. Environmental factors which is out of Project Manager’s control – like sudden Covid full lockdown preventing staff from moving out of the house, extreme weather conditions like flood, Tsunami etc, loss of resources, Loss of premises, Internet non connectivity due to planned outage or sudden NBN failure and so on.