**Digital Innovation Center Infrastructure Plan**

**Introduction:**

This DIC infrastructure plan aims for providing the infrastructures for numerous POCs and Development & Staging phases of Pilot Programs in DIC, with better **Governance** approach and with **Accelerated Delivery.** This involves the simulation of ditto real time scenario for POCs and allows only shortlisted POCs to productionize i.e. moving it in the McDermott domain with access to live McDermott data. This plan has been described tersely: why we need this, how to implement it and the benefits which we get from the implementation. Further it lists the steps to be taken from the conceptualization to the productionization of any project coming out of DIC.

**Need for Independent Infrastructure:** There are following three scenarios which can occur due to which such a set-up is required:

1. **Scenario 1:** Giving the access to our Technology Partners for the required infrastructure of McDermott allows them to access infrastructural components including vessel infrastructure also in Pilot Program phase which they should not access. For e.g. I’m able to access the Vessel VMs from the McDermott Cloud VMs.
2. **Scenario 2:** Possibility of giving the access of AD (e.g. Service Account) to our Technology Partners for authentication, identification or getting user metadata for some users would result in Partners or Users getting to read all the accounts of McDermott domain and their information.
3. **Scenario 3:** Given these above credentials if a Developer checks in these credentials to Git via Code this could lead to leakage of private information to third parties even in Pilot Program phase.

Given above it becomes imperative that we isolate McDermott company data, domain and infrastructure at least from the POCs/Pilot Programs carried out by Digital Innovation Center or our Technology Partners.

Following are the benefits which this independent infrastructure provides:

* **Better Governance**: Having the independent infrastructure eliminates any kind of access of McDermott domain to our technology partners and hence enables better Governance for McDermott ecosystem.
* **Overhead Optimization**:
  + 1. **Load Optimization of Infrastructure**: Having independent infrastructure will reduce the load of POCs and Development & Staging phases of Pilot Programs infrastructure on McDermott domain.
    2. **De-Risking of Access Grants:** Stakeholders involved in granting permissions for any infrastructural component creation need not to be worried about the delegation of any authority for the POCs or Pilot Program being executed by our technology partners in our McDermott domain, all the POCs and Development & Staging phases of Pilot Programs will be executed in DIC Infrastructure.
  + **Accelerated Delivery**: Every component which is required for POCs and Development & Staging phases of Pilot Program being implemented in DIC will be created in DIC Infrastructure. This will help to pace up the development process and hence accelerate the delivery of product.

**Execution Plan:**

The DIC Infrastructure will be behind the firewall and under the McDermott VPN. Any POC or Pilot Program being executed either by DIC Team or Technology Partner requires two modes of infrastructure, one is Cloud and another one is on-premise infrastructure. The plan for both the infrastructures has been described below

* **Phases:** For every POC and Pilot Program this plan will cater two environments:

1. **Development:** This environment will be used by the developers and will be used only by the development team.
2. **Staging:** This environment will be used for the integration testing and the testing iterations will be conducted by the QAs.

* **Cloud Infrastructure**: Any POC/Pilot Program which is going to be executed by DIC Team or our Technology Partners will use our cloud infrastructure, it can be our Private or Public cloud. For Dev & Staging our cloud infrastructures will be used. Once the POC/Pilot Program is qualified to move it on the on-premise, then we will move it to the on-premise i.e. Nutanix or UCS Cisco box.
* **On-Premise Infrastructure**: UCS Cisco/Nutanix box is a part of DIC Infrastructure plan, owned and maintained by DIC Team. Once the POC/Pilot Program is moved/migrated in the on-premise server, we can produce the real time scenario by regulating the internet connectivity of the UCS Cisco Box or Nutanix box. It can be regulated to zero internet connectivity and then again giving it the internet connection to sync up the application with any data center also, just as we will have the situation on Vessel.

In this we also have the hosting plan for the applications (POCs/Pilot Programs).

* **Hosting Plan**: We will have our different domain for all the POCs/Pilot Programs being executed in or from DIC and having a wild card SSL certificate over the same domain will be suffice enough to serve the numerous applications or POCs/Pilot Programs. For e.g. <https://mdr-dic.com> is the domain and it has the wildcard SSL certificate on it and it serves multiple applications, they are <https://abc.mdr-dic.com> and <https://xyz.mdr-dic.com>. This eliminates overhead of hosting so many POCs/Pilot Programs by single <https://mcdermott.com> wherein all the POCs are not going to be finalized for productionization. The above URLs are just for the examples it can be nomenclated in any manner.

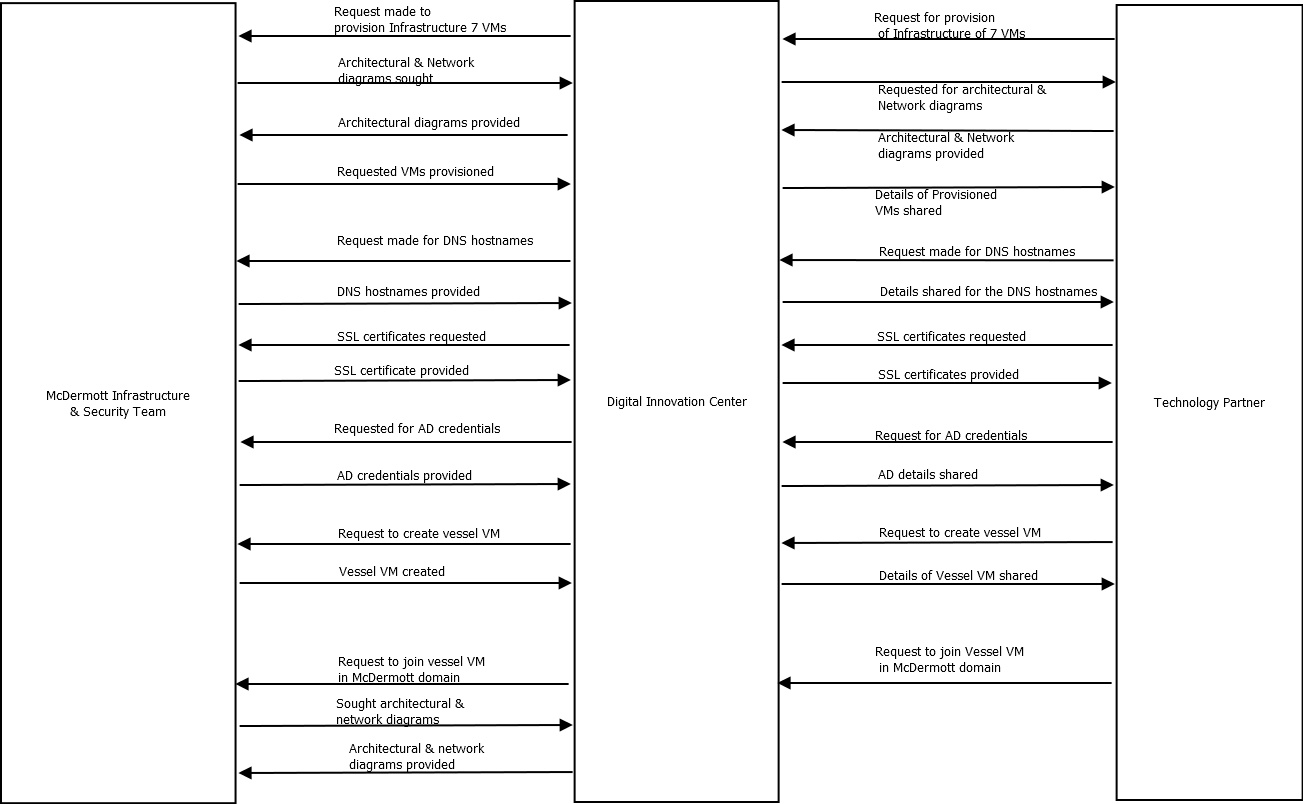
Finally, for the plan of migration/deployment in production of any POC/Pilot Program which is selected, has been detailed below:

* **Plan for Production**: In this plan we go by the same concepts as recomended by Steve Moloney in very early days of McDermott DIC. For any such application, we need to provide the Network, Architectural diagrams and every related document to Global Cyber Security Team and get their sign offs and hence then we will go forward and create the ticket to the Service desk for the creation of each and every infrastructural component and then deploy or migrate the same application in McDermott domain. The following will be the mapping of the stakeholders for the required documents:
* Cloud Architectural Diagrams & Documents----------------- Cloud Infrastructure (Ian Darce)
* Network Flow Diagrams & Documents-------------------- Infrastructure & Cyber Security (Brent Paugh)
* Security Diagrams & Documents--------------------------------- IT Manager Cyber Security (Dave Naples)
* On Premise Infrastructural Diagrams & Documents-------- Technology Manager (Emil Nabiyev)
* Final Approval------------------------------------------------------ Senior Director Technology, Infrastructure & Cyber Security (Steve Moloney)

**Promise of DIC on Security:**

1. VPN Network: Entire DIC infrastructure will be under McDermott VPN network
2. HTTPS Communication: All the communication will happen over the https network layer with digitally signed SSL certificate on URLs.
3. OS Hardening: OS Hardening will be done on Cloud and On-Premise servers to eliminate as many risks as possible even to avoid "back-door" access to the system.
4. Multifactor Authentication of the accounts.
5. SSO authentication of the accounts
6. Restricted provisioning of Infrastructure: Provisioned infrastructure will have the limited quota.
7. NACL & Security Groups: Security groups will be there to provide the IPs and ports-based access over the VMs similarly NACL will provide the access over the subnets.
8. Roles Based Access Control.
9. Security Logging & Monitoring.
10. Uploading Limitations: There will be limitations of the upload of the files and restrictions on their types from application to application.
11. Implementation of Rate limiting and the Throttling concepts.

**Following is the Diagrammatic representation of Current Set-Up:**



**Following is the flow chart of Envisaged Set-Up of DIC & McDermott Production:**

