

Course: Data and Disaster Recovery

Instructor: DR. David Khoury

Date: 7 / 1 / 2023

Students:

Fadi Dabaja (22030052)

Jamil Arabi (21930126)

Elie Kazan (22032026)

Hozaifa Ibrahim (220300202)

**ABSTRACT**

1. YLB bank, is a very big business, that may face different types of threats, for example, Cyber-attacks (phishing scams, ransomware, MITM…), Natural Disasters (earthquake, flood, fire…), Political instability (force closing due to a disease ) , Economic Instability (Failure of the country coin value in the market ), Human Error (an employee deletes data ),Supply chain disruption (supply chain impacted by a natural disaster ) and etc.. These threats must be measured even by quantitative or qualitative methodologies according the threat type. The YLB must use risk mitigation strategies, limitation , avoidance and transfer , accepting a risk is not a solution . Moreover, it must implement several services and ideas to limit/reduce or avoid the exposure to the risk, or it can transfer the impact into another assurance company that pay to the losses that might happen. A company like this has several key functions, Marketing (Developing marketing campaigns, Conducting Market Research …), Financial (Financial Reporting and analysis, Risk Management), Disaster Recovery (Site Failover; Switching to the backup) , Data Storage (Data-Replication: Real-time Synchronisation , Data-Backup: Creating copies of data and storing them in separate locations ) , Customer Service (Handling customer inquiries and complaints,

Developing customer loyalty programs), and too many other key functions and processes, all these must have RPO, RTO, WRT, MTD. To keep the operations ongoing and functioning well.

**2 - Risk Assessment**

**2-1) YLB may face several major threats :**

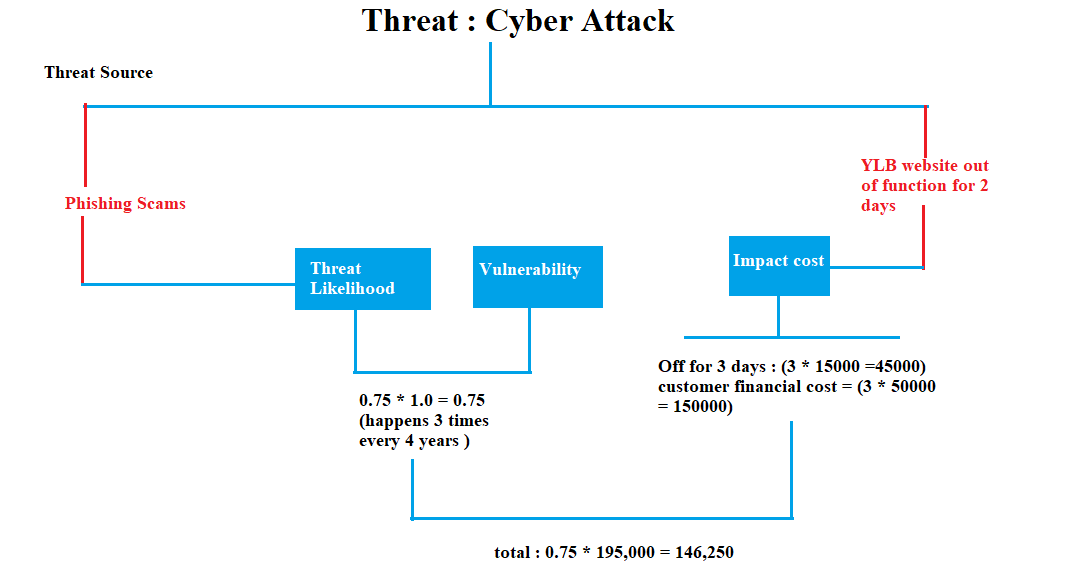
1. YLB could be vulnerable to natural disasters like earthquakes, floods, and hurricanes, which have the potential to disrupt its operations and harm its physical infrastructure. For instance, a flood could ruin computer systems or paper documents, and an earthquake could harm the bank's building. To address this risk, YLB should have a detailed disaster recovery plan that includes backup systems and a plan for moving employees and operations if necessary.
2. Political instability and conflict in the region could pose a threat to the bank's operations and the safety of its employees. If the political situation in the country deteriorates, it could lead to protests, riots, or other forms of civil unrest that could disrupt the bank's operations and put employees at risk. To address this risk, YLB may need to implement security measures such as hiring additional security personnel or implementing emergency protocols for employees to follow in the event of a crisis.
3. Economic instability and currency fluctuations could impact the bank's financial performance. If the country experiences economic downturns or currency devaluation, it could lead to reduced demand for the bank's services and impact the bank's ability to generate revenue. To mitigate this risk, YLB should diversify its sources of funding and have contingency plans in place to address potential economic challenges.
4. There is a risk that human error or malicious insiders could compromise the security and integrity of YLB's data and operations. This could occur if an employee accidentally deletes important data or reveals sensitive information to unauthorized individuals, or if an employee with malicious intent intentionally disrupts the bank's systems or steals customer data. To mitigate this risk, YLB should implement strong security protocols to prevent unauthorized access to sensitive information and provide regular training to employees on data security best practices.
5. Cyber-attacks, like phishing scams and ransomware, could put YLB's online systems and customer data at risk. Hackers could use these tactics to gain access to the bank's systems and steal sensitive information, or they could hold the bank's data hostage until a ransom is paid. To address this risk, YLB should invest in robust cybersecurity measures such as firewalls, antivirus software, and employee training on how to identify and prevent cyber threats.
6. Physical theft of assets or data could occur at the bank's branches or offices. For example, criminals could break into the bank's premises and steal physical assets such as cash or computer equipment, or they could attempt to steal data by accessing the bank's computer systems. To prevent this risk, YLB should have robust security measures in place such as surveillance cameras, alarms, and security personnel.
7. Supply chain disruptions could affect the bank's ability to access necessary goods or services. For example, if the bank's main supplier of computer hardware experiences delays or disruptions, it could impact the bank's ability to operate smoothly. To mitigate this risk, YLB should diversify its suppliers and have contingency plans in place to address potential supply chain disruptions.
8. Infrastructure failure such as power outages or communication breakdowns could disrupt the bank's operations. If the bank's systems go down, it could impact the bank's ability to serve its customers and conduct business as usual. To prevent this risk, YLB should invest in redundant systems and have a plan in place to quickly recover from any infrastructure failures.

**2-2) Risk Assessment using Qualitative or Quantitative methodology:**

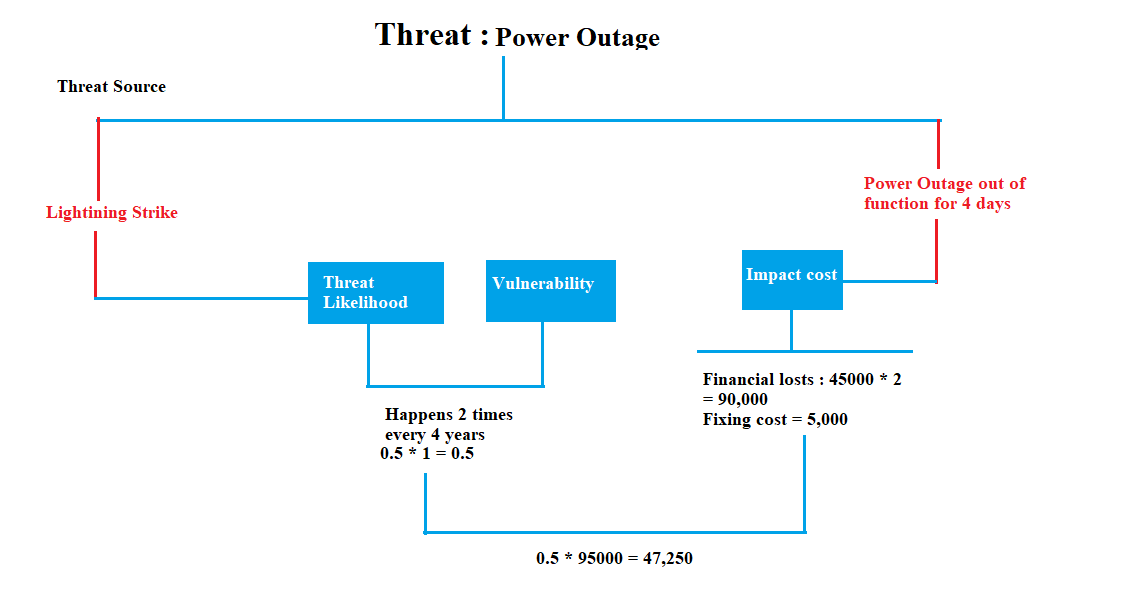
1. The possibility of cyber-attacks, such as phishing scams and ransomware, could pose a major threat to the bank's online systems and customer data. In order to assess the risk of this threat, we can use a qualitative methodology that takes into account a variety of factors. One such factor is the extent to which the bank relies on its online systems. If the bank is heavily dependent on these systems, the risk of a cyber-attack could be even greater. Another factor to consider is the potential impact of a cyber-attack. This could include financial loss and damage to the bank's reputation. It's also important to consider the likelihood of a cyber-attack occurring. By evaluating these and other factors, we can get a sense of how high the risk of a cyber-attack is. Based on this assessment, it may be determined that investing in strong cybersecurity measures is a top priority in order to mitigate the risk of a cyber-attack.
2. Infrastructure failure, such as power outages or communication breakdowns, could potentially disrupt the bank's operations and impact its ability to serve customers and conduct business as usual. To evaluate the risk of this threat, we can use a qualitative methodology that takes into account various factors. One such factor is the extent to which the bank relies on its infrastructure. If the bank is heavily reliant on its infrastructure, the risk of an infrastructure failure could be greater. Another factor to consider is the potential impact of an infrastructure failure. This could include lost revenue and damage to the bank's reputation. It's also important to consider the likelihood of an infrastructure failure occurring. By considering these and other factors, we can determine the level of risk associated with an infrastructure failure. Based on this assessment, it may be concluded that the risk of an infrastructure failure is moderate and that YLB should invest in redundant systems and have a plan in place to quickly recover from any failures in order to mitigate this risk. Human-error or malicious insiders could compromise the bank's data or operations. To assess the risk of this threat using a quantitative methodology, we could gather data on the frequency and severity of incidents involving human error or malicious insiders at the bank and use this data to calculate the expected loss from this threat. For example, if the bank estimates that such incidents occur once every year and that the average loss from each incident is $100,000, the annualized risk from this threat would be $100,000.
3. Natural disasters, such as earthquakes, floods, and hurricanes, could disrupt the bank's operations and potentially cause damage to physical infrastructure. In order to assess the risk of this threat, we can use a qualitative methodology that takes into account a range of factors. One such factor is the bank's location and its susceptibility to natural disasters. If the bank is located in an area that is prone to natural disasters, the risk could be higher. Another factor to consider is the potential impact of a natural disaster. This could include financial loss and damage to the bank's reputation. It's also important to consider the likelihood of a natural disaster occurring. By evaluating these and other factors, we can determine the level of risk associated with natural disasters. Based on this assessment, it may be concluded that the risk of a natural disaster is high, and that YLB should prioritize having a comprehensive disaster recovery plan in place to mitigate this risk. This plan should outline steps to be taken in the event of a natural disaster in order to minimize disruption and protect the bank's operations and infrastructure.
4. Supply chain disruptions can have a major impact on the bank's ability to access necessary goods or services. These disruptions can occur for a variety of reasons, including natural disasters, transportation issues, and problems with suppliers. To properly assess the risk of this threat, it's helpful to use a quantitative methodology that takes into account data on the frequency and severity of supply chain disruptions experienced by the bank. By gathering this data, it's possible to calculate the expected loss from this threat. For example, if the bank estimates that supply chain disruptions occur once every two years and that the average loss from each disruption is $200,000, the annualized risk from this threat would be $100,000. This information can be used to help the bank prioritize risk mitigation efforts and make informed decisions about how to best protect against supply chain disruptions. It may be necessary to invest in backup suppliers, diversify the bank's supply chain, or implement other strategies to reduce the risk of disruption. By taking these and other steps, the bank can better protect itself against supply chain disruptions and minimize the impact on its operations.

**2-3 ) The Diagram :**

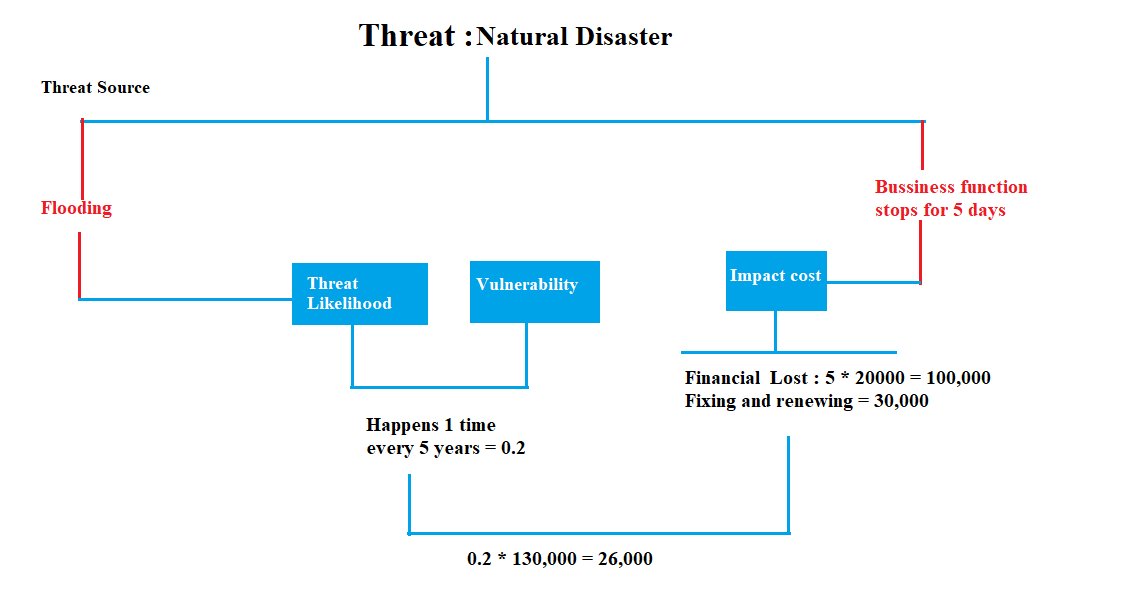
**Cyber Attack:**

****

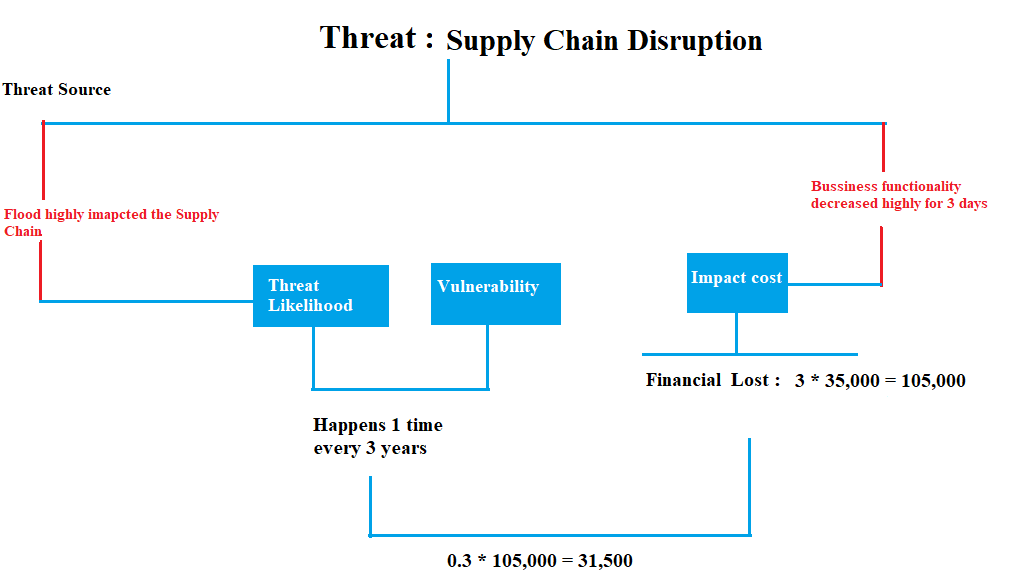
**Infrastructure Failure:**



**Natural Disaster :**

****

**Supply Chain :**



**2-4) Risk Mitigation Strategies for each Risk :**

1. For Cyber Attacks: There are a number of steps that YLB can take to mitigate the risk of cyber attacks. One of the most effective strategies is to invest in strong cybersecurity measures. This could include things like firewalls, antivirus software, and employee training on how to recognize and prevent cyber threats. By taking these steps, the bank can significantly reduce the risk of a cyber attack occurring. Another option is to transfer the risk through the use of insurance. For example, the bank could purchase cyber liability insurance to cover the costs of a data breach. This can provide an additional layer of protection in the event that a cyber attack does occur. It's also important for the bank to have a comprehensive plan in place for responding to and recovering from a cyber attack. This could include steps such as isolating affected systems, restoring data from backups, and communicating with customers and stakeholders. By taking these and other precautions, YLB can effectively mitigate the risk of cyber attacks and protect its online systems and customer data.
2. For infrastructure failure: Infrastructure failure can pose a significant risk to the bank's operations and can disrupt its ability to serve customers and conduct business as usual. To mitigate this risk, it's important for the bank to have a robust plan in place to address infrastructure failures and minimize disruption. One effective strategy is to invest in redundant systems. By having backup systems in place, the bank can continue to operate even if one system goes down. Another important aspect of this plan is to have a process in place to quickly recover from any failures. This might include steps such as isolating affected systems, restoring data from backups, and communicating with customers and stakeholders. Another option is to transfer the risk through the use of insurance. For example, the bank could purchase business interruption insurance to cover the costs of lost revenue resulting from an infrastructure failure. This can provide an additional layer of protection in the event of a failure. By taking these and other precautions, YLB can effectively mitigate the risk of infrastructure failure and protect its operations.
3. For Natural Disaster: There are a number of strategies that YLB can consider to mitigate the risk of natural disasters. One effective approach is to transfer the risk through the use of insurance. For example, the bank could purchase insurance to cover the costs of damages or lost revenue resulting from a natural disaster. This can provide an important layer of protection in the event of a disaster. Another strategy is to reduce the risk by implementing a comprehensive disaster recovery plan. This plan should include measures such as backup systems and a plan for relocating employees and operations if necessary. By having these measures in place, the bank can minimize disruption and protect its operations in the event of a natural disaster. It's also important for the bank to regularly review and update its disaster recovery plan to ensure that it remains effective in addressing the changing landscape of risks and threats. By taking these and other precautions, YLB can effectively mitigate the risk of natural disasters and protect its operations.
4. For the Supply Chain: Supply chain disruptions can pose a significant risk to the bank's operations and can affect its ability to access necessary goods or services. To mitigate this risk, it's important for the bank to have strategies in place to address potential supply chain disruptions. One effective approach is to diversify the bank's suppliers. By relying on a range of suppliers, the bank can reduce the risk of disruption if one supplier experiences problems. It's also important to have contingency plans in place to address potential supply chain disruptions. This might include steps such as identifying alternative sources of goods or services, or implementing other measures to minimize disruption. Another option is to transfer the risk through the use of insurance. For example, the bank could purchase business interruption insurance to cover the costs of lost revenue resulting from a supply chain disruption. This can provide an additional layer of protection in the event of a disruption. By taking these and other precautions, YLB can effectively mitigate the risk of supply chain disruptions and protect its operations.
5. **) Business Impact Analysis:**
   1. **) Six Disaster Scenarios:**
6. A major earthquake of catastrophic proportions has struck the city where YLB is located, causing extensive damage to the bank's building and severely disrupting its operations. The bank's building had been severely damaged, and it was unclear when, or even if, it would be able to reopen. In the meantime, the bank's employees were forced to work from temporary locations.
7. A ransomware attack succeeds in encrypting YLB's data, rendering it inaccessible unless a ransom is paid, or a cyber attack using a zero-day exploit succeeds in bypassing the bank's security measures and stealing sensitive customer data.
8. A major supply chain disruption, caused by a natural disaster in a distant country, has had a significant impact on the bank's ability to access the goods and services it needs to operate effectively. The bank has had to turn to alternative sources, which often come with a higher price tag, and has had to pay premium prices to expedite shipments. These added expenses have put a strain on the bank's budget and have eaten into its profits. The supply chain disruption has also had a knock-on effect on the bank's operations, causing disruptions and delays that have frustrated customers and led to a decline in satisfaction. The bank has had to work hard to mitigate these negative impacts, finding creative solutions and working closely with suppliers and partners to overcome the challenges posed by the natural disaster.
9. A devastating fire has ripped through the bank's main data center, causing extensive damage to the server room and destroying vital equipment. The loss of the data center and the equipment it contained was a major blow to the bank, and it was faced with the difficult task of rebuilding and replacing what had been lost. The process of rebuilding the data center was complex and time-consuming, and it required the bank to invest significant resources in order to get back up and running. The bank also had to deal with the added stress of ensuring the safety and security of its data, as well as the well-being of its employees, who were shaken by the disaster.
10. A terrorist attack targeting the bank's main branch has resulted in the death of several employees and caused significant damage to the property. The bank was left to deal with the aftermath of the attack, including the loss of life, the injuries sustained by its employees, and the extensive damage to its property.
11. A government-imposed lockdown in response to a major health crisis has forced the bank to close its branches and shift to a remote work model, resulting in significant disruptions to its operations. The sudden shift to remote work was not without its difficulties, and the bank struggled to adapt to the new reality. Communication and collaboration maybe more difficult, as employees will no longer physically present in the same location.

**3-2) BIA Report/Table:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Function** | **Process** | **Criticality** | **RTO** | **RPO** | **WRT** | **MTD** |
| **Marketing** | 1. Developing marketing campaigns 2. Conducting Market Research 3. Advertising and Promotion 4. Customer Segmentation and Targeting | Some processes can be Mission critical and other are Important | 12 hours to 24 hours | 12 hours | Up to 48 hours | Up to 72 hours (3 days) |
| **Data Storage** | 1. Data-Replication: Real-time Synchronisation 2. Data-Backup: Creating copies of data and storing them in separate locations 3. Data-Recovery: Restoring data from backups in the event of data loss or corruption 4. Data-archiving: Storing Historical data in a separate location for long-term retention and access | Mission Critical, The bank's data is essential to its operations and must be stored and protected securely. | Up to 4 hours | 1 hour | Up to 8 hours | 12 hours |
| **Finance** | 1. Financial Planning and Budgeting 2. Financial Reporting and analysis 3. Risk Management 4. Investment Management | Most times , it is mission critical and Important missions , due to budgeting and auditing and risk management | Up to 4 hours | Up to 2 hours | Up to 8 hours | Up to 12 hours |
| **Disaster Recovery** | 1. Site Failover; Switching to the backup disaster recovery site in the event of a disaster or outage at the main location 2. Data Restoration: Restoring data from backups in the event of data loss or corruption 3. Business Continuity Planning: Developing plans to ensure the bank can continue operating during and after a disaster | Mission Critical, Ensuring the bank can continue operating during and after a disaster is critical to its survival. | Up to 24 hours | Up to 12 hours | Up to 48 hours | Up to 72 hours |
| **Customer Service** | 1. Handling customer inquiries and complaints 2. Developing customer loyalty programs 3. Resolving customer disputes and complaints 4. Providing technical support and assistance | It is mission critical on responding to the customer need, and important mission when gathering feedback from customers can be useful | Up to 2 hours | Up to 1 hour | Up to 4 hours | Up to 6 hours |

**4.1.1 - Company’s infrastructure:**

YLB has implemented disaster recovery technologies and utilizes the Azure cloud for data storage in order to ensure continuity of operations in the event of any disruptions. It is also aware of the potential for political and economic instability in the region, as well as the risk of cyber-attacks.

**4.1.1 - Backup**

As we said before YLB uses backup by tapes method. We can say it uses father and grandfather backup. Where tapes are moved to a secondary location to Jbeil and a second copy of tape is stored in a floor inside the building where no staff allowed to enter since keys are shared with the top manager and the administrator of the backup team.

**4.1.2- Cloud Services:**

All backup and all mission critical applications are on a cloud using PAAS. IT Team installs the updates and other applications are installed by them.

**4.1.3 - Power**

YLB is safe when it comes to power, it has a well performing backup UPS which get maintenance every month, and it has a backup generator which goes on instantly when power go off but all servers stay alive all that time.

**4.1.4 - Redundancy**

ISP company is obliged to have a redundancy plan because the internet is going to people via routing so if a router is down YLB must in maximum timeslot of 15 min deliver the internet via alternate route to the people the internet will go slower but the important in this procedure is to preserve availability and connectivity to people.

**4.1.5 - Operating systems**

YLB was using windows XP on all workstations but they upgraded all their workstations to windows 10 x64 and they use windows server 1008 R1 and windows server for active directory and database.

**4.1.6 - Servers and Switches**

YLB uses Cisco equipment for networking and Huawei for the server’s infrastructure.

**4.1.7- Virtualization**

Virtualization is the process of creating a virtual version of something like computer hardware. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. The organization uses VMs for redundancy and to support the fast incident healing and data recovery. Live migration of VMs occurs through HYPER-V.

Type-1, or bare-metal hypervisors, are installed directly onto the physical hardware. As such, they must contain their own operating systems for booting, running the hardware, and connecting to the network. Popular Type-1 hypervisors include Microsoft Hyper-V and VMware ESXi.

Type-1, or hosted hypervisors, run on an operating system that is directly installed on the hardware. In this case, a copy of Windows, or a Unix-based system must be installed to boot the system and access the hardware. Once the operating system is running, the hosted hypervisor can launch.

Type-1 hypervisors are often used to run multiple operating systems on a single machine, rather than to emulate numerous running systems on the hardware. Popular Type-1 hypervisors include VMware Workstation, VirtualBox, and Parallels that emulates a Windows operating system while running on a Mac-based computer. The purpose of the hypervisor is to manage each virtual machine and provide it with the resources it needs to run.

**4.1.8 – Security**

Security is an important term when it comes to YLB because it is protected against attacks from inside and from outside too. Since from active directory and Oracle database they gave privilege to the employees according for their jobs and USBs are not allowed and it’s stopped by active directory. Doors are closed when company closes; finger prints are checked in and out. Security guards are available 14/7. Each workstation has its antivirus system, all of them are managed from a single server.

**4.1.9 – Recovery**

The RTO is 1-hour minimum for critical situations but other simple issues are done with a short period time. If a network problem occurs in a specific redundant switches and access points are available to be spare network components. are available in the building.

**4.1.10 - Database**

YLB uses SQL server 1008 R1 and SQL server 1011 all the databases are backed up on and stored on the physical hard drives and tapes the company replicate its databases to a secondary location. Moreover, copy of the DBs are stored on the VM that is related to it.

**4.2. The diagram represents the process:**

a) The main location in DT and the backup location in Jbeil are connected using two redundant WAN links. Replicated traffic between the two locations is optimized and encrypted.

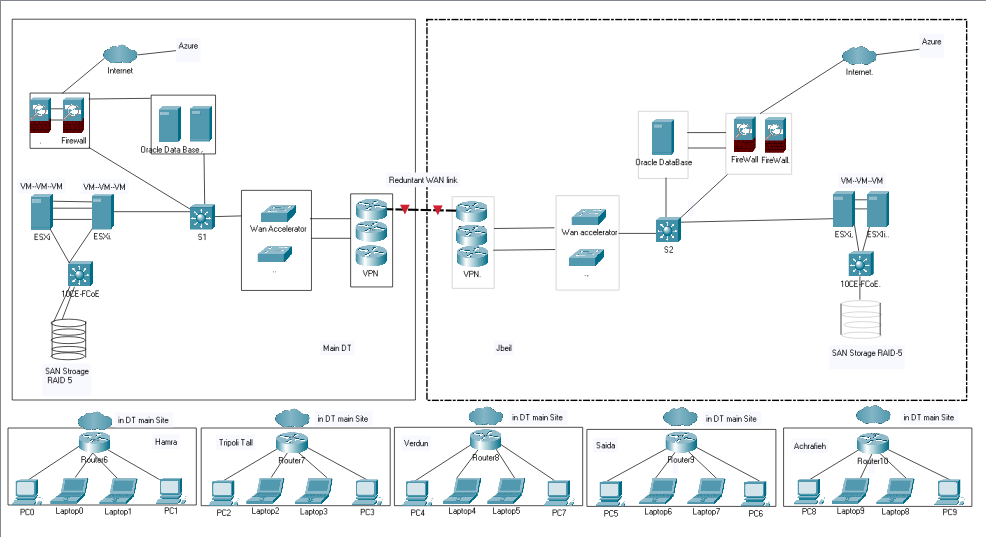
b) The three branches are connected to the main location in DT and the backup location in Jbeil using one WAN link each (no link redundancy).

c) The two Head offices are connected to the main location in DT using redundant WAN links, and they are connected to the backup location in Jbeil using one WAN link each (no link redundancy).

d) The main location in DT has two VMWare Hypervisors with VMs, and the backup location in Jbeil has one VMWare Hypervisor with VMs. Replication between the VMWare hypervisors occur through the use of VMWare vMotion, which allows live migration of VMs from one hypervisor to another without downtime.

e) The main location in DT has two Oracle Databases, and the backup location in Jbeil has one Oracle Database. Replication between the Oracle databases occurs through the use of Oracle Data Guard, which allows for the creation of a standby database that is continuously updated with changes made to the primary database.

f) The main location in DT has two SAN storages, which are connected to the core switch. The cloud location has one SAN storage. Replication between the SAN storages occur through the use of data replication software, which copies data from one storage system to another in real-time or at scheduled intervals.



**5) Conclusion:**

YLB is a big business that may be vulnerable for several types of threats, on its several functions keys and their process that their failure might be risky to the whole operation the bank, so several Risk mitigation strategies must be used to mitigate the risk with different types of mitigation strategies and different types of implementations, also these should be counted even using qualitative or quantitative methodologies to assess the risk.

**6) REFERENCES:**

* Business Continuity and Disaster Recovery Planning for IT Professionals.
* [http://www.gartner.com/smarterwithgart ner/disaster-preparedness-enablebusiness-continuity-via-a-business-impactanalysis/.
* <http://www.dbpmanagement.com/15/5-ways-to-manage-risk>.
* https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems/engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitorin