

## Table of Contents

Find out method for assessing Software Development infrastructure security .....	2
Methodology of Risk Assessment (Chunlin Liua, 2012) .....	2
a) Identify the assets and people that need to be protected. ....	3
b) Perform a threat assessment to identify and define the threats that could cause harm to the facility and its inhabitants.....	3
c) Identify assets and threats.....	5
d) Conduct a vulnerability assessment to identify weaknesses that might be exploited by a terrorist or aggressor.....	6
e) Compute the risk using the results of the asset value, threat, and vulnerability assessments.....	9
Test maturity models (TMM) (Yuqing Wang, 2019) .....	11
Hardening.....	16
References .....	21

## Find out method for assessing Software Development infrastructure security

### Methodology

#### Methodology of Risk Assessment (Chunlin Liua, 2012)

Risk assessment is an umbrella term for mapping and identifying hazards or risk factors that may cause harm to the system or software and how the organization protect their assets.

This type of assessment analyzes from 2 dimensions which is probability and impact.

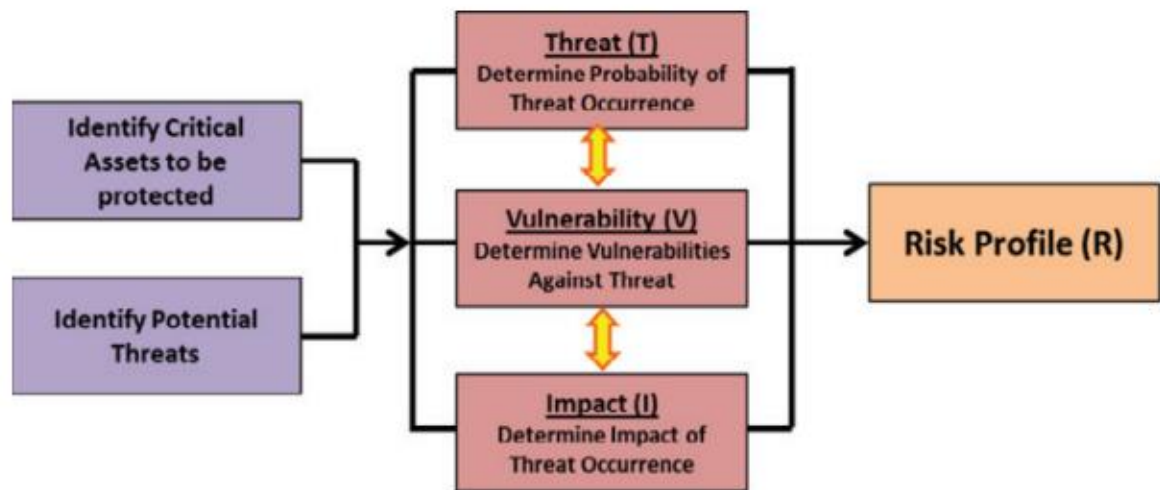


Figure 1: Flow of risk assessment

This risk assessment measured in both quantitative and qualitative factor. Determining what the current level of acceptable risk, measuring the current risk level and determining what can be done solve the issue will be included in the highest level. The result of this implement this methodology is the combination of threat assessment, vulnerability assessment and impact assessment to arrive at a numeric value for the risk to each asset against specific threat in accordance with the risk formula:

$$\text{Risk} = T \times V \times I$$

Where

T = Threat Rating, V = Vulnerability Rating and I = Impact Rating

The entire process of Risk assessment can be summarized as:

a) Identify the assets and people that need to be protected.

Assets is one of the value to the facility and it can be tangible. For example, tenants, activities and equipment. By identifying the facility's critical assets will helping in understanding the core functions and processes. This will also lead to a higher efficient in achieving and maintaining the process. Redundancy and recovery plans need to be included for a clear understanding on the assets.

RefNo	Name of Asset	Description of Asset	Redundancy (Quantity & Readiness)	Recovery Plan (Repair/ Replacement Cost & Time)
ASST01	Asset A	e.g. Production system...	e.g. 100% redundancy, but requires 2 hours lead time to fully activate.	e.g. \$10,000 - \$50,000/ 6 months
ASST02	Asset B	e.g. Emergency power supply	e.g. 1 no 2 cells on hot standby	e.g. < \$200,000 / 3 months
ASST03	...	...	...	...

*Figure 2: Sample of facilities for assessment*

b) Perform a threat assessment to identify and define the threats that could cause harm to the facility and its inhabitants.

The preliminary phase in the risk assessment process is to refer the facility under review to a list of threats and determine the applicability and likelihood of such threats to the facility based on the geopolitical situation, current events and historical data applicable to the facility within the region. Some of the threats are limited to particular security environment while some may exist any time under any environment. To identify different environments within different levels of threats, Peacetime (PT) and Heightened Security (HS) periods will be take place.

- Peace Time (PT) - Time whereby the prevalent security situation is normal both at the national level and the facility level. High-level security threats are not expected to occur.
- Heightened Security (HS) – A period of heightened state of alert as a result of present and lurking aggression from known criminal or terrorist organizations. Heightened Security situation may also be declared when intelligence from government agencies indicates a high risk of terrorist attacks. During Heightened Security period, security measures are expected to be strengthened whilst maintaining general daily routines.

S/No	Threat	Description	Possible Mode of Attack	Applicable During
T1	Theft / Burglary	Unlawful removal of property from the facility during and/or after business hours committed by lone motivated individuals (insiders/outside rs) or organized syndicates.	Unauthorized access with or without the use of special tools and equipment, including theft of Intellectual Property by Industrial Espionage.	PT HS
T2	Robbery	Removal of valuables by force or threat of force or by fear. May occur during and/or after business hours and may be committed by motivated individual(s) or organized syndicates.	Use of physical force, threat of bodily harm or intimidation of visitors and staff with or without use of weapons (either lethal or non-lethal weapons).	PT HS

*Figure 3: Sample of conventional threat scenarios*

c) Identify assets and threats.

A list of criteria is designed to assess or determine the specific threats that exist. The scores from 1 to 5 (5 being the greatest threat) for each criteria that described in the table below. The average score of the sum of all the seven threat factors will derive the Threat Assessment Rating. While the vulnerability and analysis of the scenario will be rating and describe in the Threat Assessment Work Sheet.

- Threat Assessment factor matrix

Threat Assessment Factors Matrix							
Score	Access to Resources	Knowledge/ Expertise	History of Threats	Asset Visibility/ Symbolic Value	Asset Accessibility	Site Population	Collateral Damage
5	Readily available	Basic knowledge/ open source	Local incident, occurred less than a year; caused great damage; building functions and occupants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	Less than 1000	Beyond 1km radius
4	Easy to produce or acquire	Bachelor's degree or technical school/open scientific or technical literature	Regional/ local incident; occurred between 1 and 5 years ago; caused substantial damage; building functions and occupants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	Less than 500	Within 751m to 1km radius
3	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	International incident; occurred between 6 and 10 years; caused moderate damage; building functions and occupants were one of the primary targets	Existence publish/well-known	Controlled access, protected entry	Less than 200	Within 501m to 750m radius
2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident; occurred between 11 and 15 years ago; caused localized damage; building functions and occupants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	Less than 100	Within 251m to 500m radius.
1	Extremely difficult to produce or acquire	Advanced degree or advance training/ classified information and vast experiences	International incident; occurred between 16 and 20 years ago; caused localized damage; building functions and occupants were not the primary targets	Unaware of existence	Remote location, precipitous terrain, secured perimeter, armed guards, tightly controlled access	Less than 50	Within immediate area to 250m in radius.

Figure 4: List of threat assessment criteria

- Benchmark of threat rating

Threat Rating		
Very High	5	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	4	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	3	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Low	2	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Figure 5: Benchmark of threat rating

- Threat Assessment Work Sheet

S/no.	Threats	Threat Period / Rating	
		PT	HS
T1	Theft / Burglary	----	----
		----	----
T2	Robbery	Rating – e.g. 2 (Low)	Rating
		Explanation – e.g. The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.	Explanation
T3	Public Incidents	Order	----
		----	----






 Rating 5 (Very High)
 Rating 4 (High)
 Rating 3 (Medium)
 Rating 2 (Low)
 Rating 1 (Very Low)

Figure 6: Benchmark of threat assessment

- d) Conduct a vulnerability assessment to identify weaknesses that might be exploited by a terrorist or aggressor.

Vulnerability assessment is an in-depth study of building structures, systems and site features to determine building vulnerabilities, adequacy of current protection measures (if any), lack of reliability and time of operational recovery from attack. There are 5 criteria to be measured in this phase (rating of 1 to 5 will be apply; 5 is the highest score):

- Susceptibility

It concerns the issue of how vulnerable the asset is to the danger because of its attractiveness in terms of its physical and symbolic characteristics, and the exposure level that leads to the overall vulnerabilities of the asset. The weakness will be identified according to the environment, architecture and structural features, security measures and processes.

- A minor weakness is one that vulnerability is not obvious and even if it is discovered by a perpetrator, it is not easily overcome without the perpetrator being detected.
  - A weakness means that the vulnerability is obvious but not easily overcome by perpetrator without being detected.
  - A major weakness means that the vulnerability is exposed to perpetrator and it is easily overcome without being detected.
- Adequacy of Security  
The adequacy of current protections is evaluated in relation to the particular risks that relate to the asset(s).
  - Redundancy  
The evaluation reflects the geographical distribution and interdependencies of the primary service components and their backups within the institution, as well as the availability of alternative work locations or recovery sites for primary service or processes.
  - Recovery Periods  
Recovery period refers to the time after an incident or attack occurs to the time when usual / core operations are restored whether at alternate site or alternative business mode.

Rating	Susceptibility	Security Measures	Redundancy	Recovery Period
5	One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor.	Lacks security measures	Lacks redundancies.	Entire facility functional again after 1 month after an attack.
4	One or more major weaknesses have been identified that make the asset Highly susceptible to an aggressor.	Poor security measures	Poor redundancies. 25% of the facility's function can be restored.	Most parts of the facility would be functional again within a month after an attack.
3	A weakness has been identified that makes the asset moderately susceptible to an aggressor	Moderate security measures	Moderate redundancies. 50% of the facility's function can be restored.	Most part of the facility would be functional again within a week after an attack.
2	A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor	Good security measures	Good redundancies. 75% of the facility's function can be restored.	The facility would be operational within a day after an attack.
1	Very low susceptibility of the asset to an aggressor.	Excellent security measures	Excellent redundancies. 100% of the facility's function can be restored.	The facility would be operational immediately after an attack.

*Figure 7: Benchmark and sample of vulnerability assessment criteria*

### Qualification of Criteria

An impact assessment took place in order to assess the impact of probable occurrence of the various identified threats against the facility under assessment. The assessment criteria are including Loss of Life, Injuries, Loss or damage of building / assets, Loss of primary service (importance / duration), and Impact on economic and/or socio-political well-being of the country / nation.

Criteria	0	1	2	3	4	5
Loss of life	No Loss of Life	Less than 1% of population	1% to 2% of population	More than 2% but less than 3% of population	3% to 4% of population	More than 4% of population
Injuries	No Injury	Less than 10% of population	10% to 20% of population	More than 20% but less than 30% of population	30% to 40% of population	More than 40% of population
Loss due to damages to building/ asset	No Impact	Less than 1% of Overall Construction Cost	1% to 2% of Overall Construction Cost	More than 2% but less than 3% of Overall Construction Cost	3% to 4% of Overall Construction Cost	More than 4% of Overall Construction Cost
Loss of primary services	No Loss	Less than 1 day	1 day to 1 week	More than 1 week but less than 1 month	1 month to 6 months	More than 6 month
Impact on national economic/ socio-political wellbeing	No Impact	Insignificant	Minor	Moderate	Major	Catastrophic

*Figure 8: Criteria and benchmark of the impact assessment*



Impact Rating		
Very High	5	Loss or damage of assets has exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions; property damage; and a catastrophic impact on economic and political well-being of the nation.
High	4	Loss or damage of assets has grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time; and functions; property damage; and a major impact on economic and political well-being of the nation.
Medium	3	Loss or damage of assets have moderate to serious consequences, such as injuries or impairment of core functions and processes; and functions; property damage; and a moderate impact on economic and political well-being of the nation.
Low	2	Loss or damage of assets have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time; and functions; property damage; and a minor impact on economic and political well-being of the nation.
Very Low	1	Loss or damage of assets have negligible consequences or impact; and functions; property damage; and an insignificant impact on economic and political well-being of the nation.

Figure 9: Benchmark of impact rating

S/no.	Threats	Threat Period / Rating	
		PT	HS
C1	Theft / Burglary	Rating - e.g. 1 (Very Low)	Rating - e.g. 1 (Very Low)
		Explanation - e.g. Loss or damage of assets have negligible consequences or impact; and functions; property damage; and a very low impact on economic and political well-being of the nation.	Explanation - e.g. Loss or damage of assets have negligible consequences or impact; and functions; property damage; and a very low impact on economic and political well-being of the nation.
C2	Robbery	Rating	Rating
		Explanation	Explanation
C3	Public Order Incidents	----	----
		----	----






	Rating 5 (Very High)		Rating 4 (High)		Rating 3 (Medium)		Rating 2 (Low)		Rating 1 (Very Low)
---	----------------------	---	-----------------	---	-------------------	---	----------------	---	---------------------

Figure 10: Impact Assessment Work Sheet

e) Compute the risk using the results of the asset value, threat, and vulnerability assessments. In order to perform a proficiency decision-making process in selecting and prioritizing risk management strategy, the ranking of the threats according to the respective risk profile is applicable. For threats of Medium risk profile, mitigation measures should be considered based on the principle of “ALARP” (as low as reasonably practicable). As for threats that are of Low and Very Low risk profile, it is recommended that facility owners and the security designers should evaluate the Residual Risk before accepting them.

S/no.	Threats Scenarios	PT					HS				
		T	V	I	Risk Rating (T x V x I)	Risk Profile	T	V	I	Risk Rating (T x V x I)	Risk Profile
R2	Robbery	---	---	---	---	---	---	---	---	---	---
R3	Public Order Incidents	e.g. 2	e.g. 3	e.g. 3	18	Medium	e.g. 4	e.g. 5	e.g. 3	60	High
R4	Sabotage / Mischief	e.g. 3	e.g. 4	e.g. 4	48	High	e.g. 3	e.g. 4	e.g. 4	48	High
R5	Stand-off Attack with Hand Thrown Devices	---	---	---	---	---	---	---	---	---	---
	Rating 5 (Very High)		Rating 4 (High)		Rating 3 (Medium)		Rating 2 (Low)			Rating 1 (Very Low)	

Figure 11: Sample of risk assessment work sheet

Index	Threats	Risk Ranking		Risk Management Strategy
		PT	HS	
e.g. R9a	Attack by a vehicle carrying improvised explosive devices (VBIED) in Adjacent Area	High	Very High	To Mitigate the Risk
e.g. R9c	Attack by a vehicle carrying improvised explosive devices (VBIED) - Forced Entry	Medium	High	To Mitigate the Risk
e.g. R10	Attack with Chemical / Biological / Radiological Agents	Medium	Medium	To Consider Mitigation (ALARP)
e.g. R11	Commando-style attack	Low	Medium	To Consider Mitigation (ALARP)
e.g. R1	Theft / Burglary	Low	Low	To Evaluate Residual Risk before Acceptance
e.g. R2	Robbery	Low	Very Low	To Evaluate Residual Risk before Acceptance
e.g. R3	Public Order Incidents	Very Low	Very Low	To Evaluate Residual Risk before Acceptance

Figure 12: Example of risk ranking

### Test maturity models (TMM) (Yuqing Wang, 2019)

Test Maturity Model is based on the Capability Maturity Model (CMM) which used to develop and refine the process of an organization's software development and specifies an increasing series of levels of a software development organization. TMM is a detailed model for test process improvement, thus, the higher the level, the better the software development process. Basically, TMM is synthesize what an organization should focus to assess its test automation processes and develop a self-assessment instrument for assessing test automation processes and scientifically evaluate it.

### Capability Maturity Model (CMM)

#### Characteristics of the Maturity levels

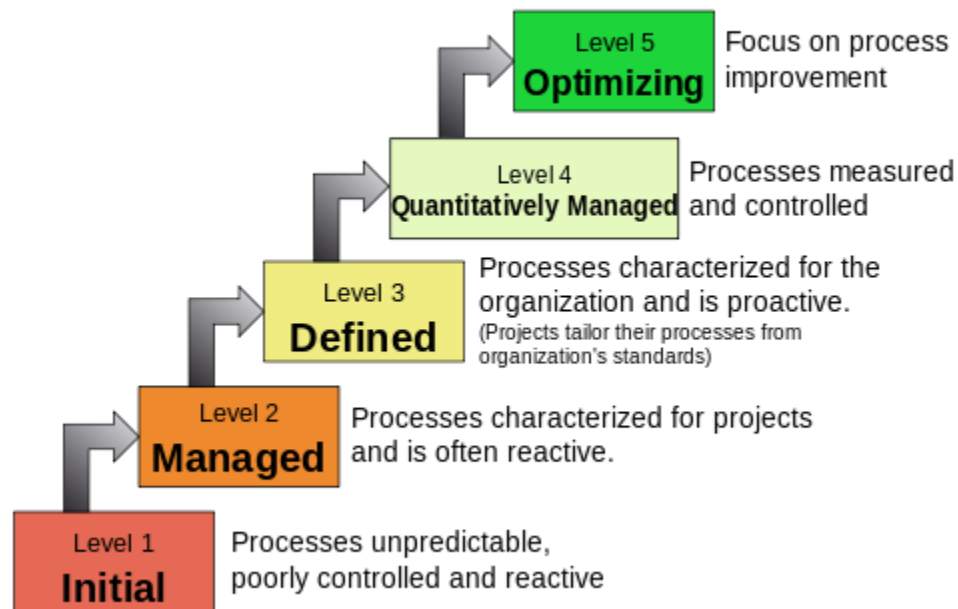


Figure 13: Levels of CMM

### Test maturity models (TMM)

Test maturity models define key areas (KAs) which is the objectives that indicate where an organization should focus to assess its test process. It is very important in order to mature the process by following the checklist. There are many test maturity models widely used in the market area. However, some test maturity models which has self-assessment instruments for organizations is high recommended to implement. Hence, it is easier to enable data collection, assist the

assessment process, and conduct these self-assessment at different stages of the test process and therefore make it possible for the progress tracking and the identification of improvement steps. For instant, TPI provides a Test Maturity Matrix, TMap provides Checklists, TOM provides Test Organization Maturity Questionnaire. All these assessments items are used to assess the maturity state of the test process.

### **Test Process Improvement (TPI)**

TPI model able to determine the strong and weak points of the current test process and formulating specific and realistic improvement actions for this test process.

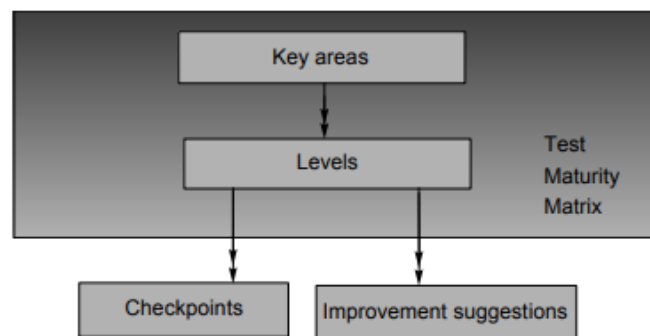


Figure 14: TPI model

TMM Levels	Level 1 : Initial
Goals	Software should run successfully
Objective of TMM levels	<ul style="list-style-type: none"> <li>• At this level, no process areas are identified</li> <li>• An objective of testing is to ensure that software is working fine</li> <li>• This level lacks resources, tools, and trained staff</li> <li>• No Quality Assurance checks before software delivery</li> </ul>

TMM Levels	Level 2: Defined
Goals	Develop testing and debugging goals and policies

Objective of TMM levels	<ul style="list-style-type: none"> <li>• This level distinguish testing from debugging &amp; they are considered distinct activities</li> <li>• Testing phase comes after coding</li> <li>• A primary goal of testing is to show software meets specification</li> <li>• Basic testing methods and techniques are in place</li> </ul>
-------------------------	---

TMM Levels	Level 3: Integrated
Goals	Integration of testing into the software lifecycle
Objective of TMM levels	<ul style="list-style-type: none"> <li>• Testing gets integrated into an entire life cycle</li> <li>• Based on requirements test objectives are defined</li> <li>• Test organization exists</li> <li>• Testing recognized as a professional activity</li> </ul>

TMM Levels	Level 4: Management and Measurement
Goals	Establish a test measurement program
Objective of TMM levels	<ul style="list-style-type: none"> <li>• Testing is a measured and quantified process</li> <li>• Review at all development phases are recognized as tests</li> <li>• For reuse and Regression Testing, test cases are gathered and recorded in a test database</li> <li>• Defects are logged and given severity levels</li> </ul>

TMM Levels	Level 5: Optimized
Goals	Test process optimization
Objective of TMM levels	<ul style="list-style-type: none"> <li>• Testing is managed and defined</li> <li>• Testing effectiveness and costs can be monitored</li> <li>• Testing can be fine-tuned and continuously improved</li> </ul>



### **Test Management approach (TMap)**

TMap help in delivering complex and high-quality software more quickly while saving the time and costs of the organizations. TMap offers a toolbox for setting and conducting tests in combination with manuals and instructions. The example of assessment items according to the checklist of TMap Test Environment is stated as below:

#### **(1) Environmental data**

- Are standard test data sets available?
- Do agreements about the test data exist with the test data owners?
- Does the system data need to be adapted?
- Is it possible to test with test accounts or with production profiles?

#### **(2) Maintenance tools / processes**

- Does one single point of contact exist for test environment maintenance?
- Are agreements reached about the readiness and quality of the test environment?
- Is the maintenance of the test environment supported by maintenance tools?

## Hardening

Hardens are typically the method of protecting a system by which its vulnerability surface, which is stronger as a system performs more functions; in general, a single-function system is better than a multipurpose system. By implementing hardening in software or server, it will boost the protections. As most of the environments or applications are not focus on the security, hence, the information assets will expose in high security risks without implement hardening. There are 4 hardening infrastructure layers which are:

- Server hardening

Server hardening is a method to improve server security by using viable, efficient means.

It is recommended that the CIS benchmarks be used as a guide to harden benchmarks.

Items	Notes
implement a "least functionality" approach. for example: Do not install the IIS server on a domain controller	
Create a secure remote administration for the server	
Consider using the server local firewall. Windows- Windows firewall, Linux- IPtables, AppArmor	
When hosting multiple applications, make sure that each has their own accounts separate from the others.	

*Table 1: Example checklist of server hardening*



- Application hardening

Application hardening is the method of protecting apps from threats locally and on the Internet. Application hardening can be carried out by eliminating the functions or components you don't need.

Items	Notes
For securing an IIS, the first step is to remove all sample files. To help the user in the setting of sample files, which can be used by the user to examine and as a reference when constructing their web sites. But these sample files are full of vulnerabilities and holes, so they should never be present on a production web server.	
Sample files are stored in virtual and physical directories, so to remove IIS sample application, remove the virtual and physical directories. For example, IIS samples are present in the Virtual Directory of \IIS samples and its location is C:\Inetpub\IISsample.	
The next step in securing IIS is to set up the appropriate permissions for the web server's file and directories this is possible using Access Control Lists (ACLs).	
Install SSL Architecture	

Table 2: Example checklist of application hardening



- Database hardening

As the database is confidential and sensitive data, hence, the incorrect or leakage of data will affect the organization or business operations.

Items	Notes
Having a TNS Listener Password (encrypted) to prevent unauthorized administration of the Listener	
Turning on Admin Restrictions to ensure certain commands cannot be called remotely	
Locking and Expiring Unused Accounts	
Defining user account naming standards	

*Table 3: Example checklist of database hardening*

- Operating System hardening

Items	Notes
Install the latest Service Pack for the operating systems used	
Do not create more than two accounts in the Administrators group	
File and File System Encryption – All disk partitions are formatted with a file system type with encryption features (NTFS in the case of Windows)	
Remove unnecessary drivers	

*Table 4: Example checklist of operating system hardening*



## References

Chunlin Liua, C.-K. T. Y.-S. F., 2012. The Security Risk Assessment Methodology. *International Symposium on Safety Science and Engineering in China, 2012*, p. 601.

Yuqing Wang, M. M. E., 2019. A Self-assessment Instrument for Assessing Test Automation. *Proceedings of the Evaluation and Assessment on Software Engineering*, p. 145.