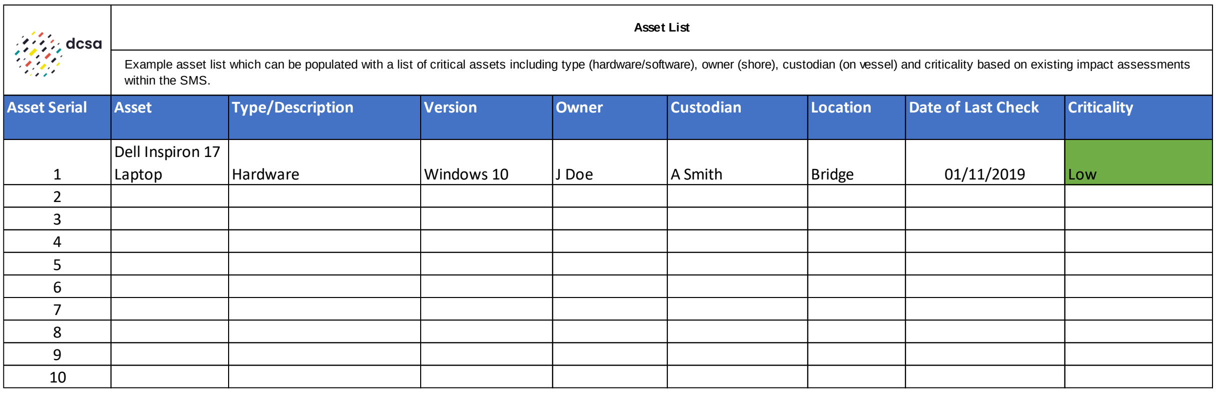
DCSA Templates Reading Guide

1. Asset Management

Before the risk assessment can be planned and conducted, you need to first identify the assets you have in the organisation. The best way to do so, is by creating an asset inventory. The asset inventory should contain all assets that are valuable to the organisation and that contributes to its ability to function. This includes physical devices, systems, software platforms and applications.



Asset List

Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.

Asset Serial	Asset	Type/Description	Version	Owner	Custodian	Location	Date of Last Check	Criticality
1	Dell Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

- The assets should be inserted into an asset list (see example above). When using the asset list, each asset must be assigned a unique serial number. Then the Asset and a description of the asset should be noted, followed by the version.
- Next, there needs to be assigned an owner and custodian to each asset. If there are changes in employees in the organisation, the asset list should be updated to reflect such change.
- Asset owners have a special role, as they can be the best source to identify the potential vulnerabilities and threats towards the asset they are responsible of – and what the likelihood and impact of such vulnerabilities could be.
- The asset owners can end up being the risk owners for the asset, as they are able to take accountability for managing risks, due to their knowledge on the asset.
- The 'location' section in the asset list is referring to where the exact location of the asset is on the vessel, as it is a critical requirement for asset management on-board a vessel and elsewhere to be able to locate the assets.
- The criticality of the asset should also be defined, on a low - medium – high scale.

Measuring Weight of an asset (criticality)		
Weight	**Rate**	**Description**
Low	1	The asset value is low based on low business objectives, and would have little / no critical impact to the organisation if the asset was lost or damaged
Medium	2	The asset value is medium based on business objectives, and would have some critical impact to the organisation if the asset was lost or damaged
High	3	The asset value is high based on business objectives, and would have high critical impact to the organisation if the asset was lost or damaged

The two following examples can be applied to the asset list:

- If the captain has a laptop on the vessel, the location of the device should be defined. This is to ensure you are always able to locate your assets, in case an incident were to occur. Since it is the captain's laptop, he could be the owner of the laptop, or ownership could be retained by group IT with the Captain being an allocated user. Essentially, whoever owns the risk against the asset should be the ultimate owner.
- A PLC (Programmable Logic Controller) on-board as part of an IoT infrastructure. Then it would be important to be able to exactly pinpoint where on the vessel it can be found. The IT responsible on the vessel could be defined as the asset owner, however, asset ownership would vary between different company structures.

Assets should be reviewed on a periodic basis, and be part of an asset lifecycle management process to document: creation, processing, storage, transmission, deletion and destruction activities of assets. The organisation should define the interval by which the asset list should be updated (monthly, quarterly or yearly).

Quantitative Risk Assessment

2.1 Quantitative Risk Assessment

- Risk describes the extent to which an entity is threatened by an event, and is typically a function of severity and likelihood[1]. Risk can be assessed quantitatively, qualitatively or semi-quantitatively. The quantitative risk assessment differs from the two others, as it defines a way to make risks measurable. It is done by developing a risk applicability matrix, where ratings to identified risks can be defined. They are normally defined from a 1-5 scoring.

- Before a risk assessment can be conducted, the organisation needs to identify its critical information assets. When the assets have been identified, the threats and vulnerabilities towards those assets must be identified.

- A threat event is an event that has potential of causing negative consequences or impact to an organisation[2]. The threat agent/ threat source is the method targeted, with the goal of intentionally exploiting a vulnerability[3]. A threat agent can be spyware, organised crime or insiders.

- A vulnerability is a weakness or gap in a security program, internal controls or information systems, which can be exploited by a threat agent[4].

2.2 The 1-5 risk rating

When conducting a quantitative risk assessment, the risks are typically categorised on a 1-5 rating. This rating can be 'viewed' from severity and likelihood.

- In the first table severity and likelihood is described more in detail.

	Severity			Likelihood	
5	Catastrophic	Severe impact to the organisation. Loss of resources and worst case loss of life	5	Almost certain	A threat is very likely to occur. Could be multiple times per week
4	Major	Serious impact to the organisation. Will damage both reputation and compromise of information	4	Likely	Two to three times per month
3	Moderate	Partially damaged image and loss of costumer confidence. Some negative impact to the organisation and its operation	3	Possible	Occurs once per month
2	Minor	Small harm to the organisation.	2	Unlikely	Occurs once or twice a year
1	Negligible	Insignificant impact to organisation and operations.	1	Rare	Few previous incidents: happens once every 10th year

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf page 6

[2] NIST SP 800-12 Rev. 1 (NIST SP 800-30) in https://csrc.nist.gov/glossary/term/Threat-Event

[3] NIST SP 800-53 Rev. 4 under Threat Source (FIPS 200) in https://csrc.nist.gov/glossary/term/threat-source

[4] NIST SP 800-37 Rev. 1 under Vulnerability (CNSSI 4009) in https://csrc.nist.gov/glossary/term/vulnerability

It is important to describe in depth the definitions of the risk rating levels, as this helps to ensure a consistent assessments of risks across the organisation. Once the definitions of severity and likelihood have been defined, they should be inserted into a risk matrix.

- In the second table severity and likelihood has been inserted in a risk matrix, showing the 1-5 scores.

Catastrophic	5	10	15	20	25
Major	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Negligible	1	2	3	4	5
	Rare	*Unlikely*	*Possible*	*Likely*	*Almost certain*

If both severity and likelihood have a score of 5, the negative consequences towards the organisation will be high. It is thus up to the organisation to define what risk acceptance level they are willing to accept. If they set their risk acceptance to '16', it means that all risks scoring a higher number than 16 should be mitigated. This is why the risk matrix above has the number '16' marked with red.

2.3 How to Apply CIAS to Quantitative Risk Assessments

The security term CIAS stands for Confidentiality, Integrity, Availability and Safety.

- Confidentiality refers to the ability to protect data, so that only those users with appropriate permission levels are authorised to view data. It could also assess the protections to be applied to data classified as confidential. This can be ensured by using Access Control Lists (ACL), but also through encryption.

- Integrity refers to the reliability of data stored recorded by and stored within an organisation. If there is a high risk of data being altered during an incident, the score for integrity will be high. Data encryption or hashing are useful tools to ensure a high level of integrity.

- Availability refers to the lack of availability of systems. If an incident were to occur, where the systems would be down for 15 minutes, the availability score would be 1. Redundancy or RAID can be used to mitigate incidents from happening[5].

- Safety is also important to incorporate in the risk assessment, as it focuses on people. If the score is 1, there is a hazard identified, but no one's safety is at risk. If the score is at 5, which is the worst case scenario, an incident would have led to loss of life.

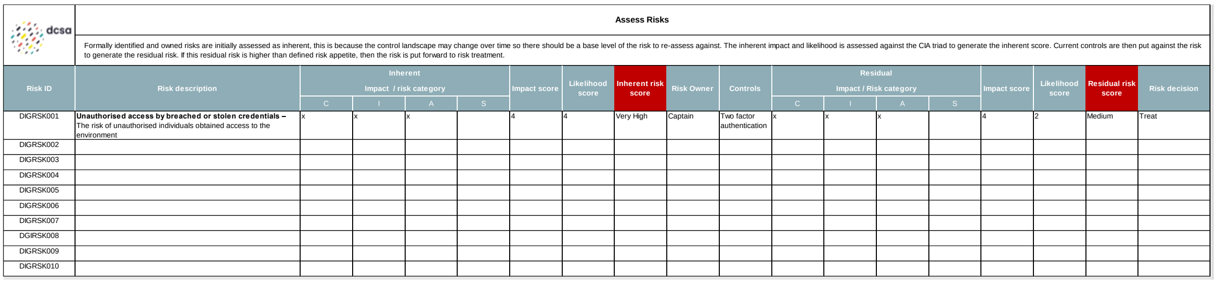
[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf page 2-4

Confidentiality, integrity, availability and safety can be conceptualised the following way, based on the 1-5 risk rating.

	Confidentiality	Integrity	Availability	Safety
1	Negligible	No noticeable change	15min	Hazard identified
2	PD/IP	Smaller change, data or system still usable.	1 hour	Hazard occurs, but no injury (near miss)
3	Data breach	Noticeable change, diminishes usability of data or system.	6 hour	Minor injury – requires treatment but able to continue working.
4	Large data breach	Significant changes to data or settings, requires significant effort to recover.	One day	Major injury – unable to continue working/evacuation from ship.
5	Data breach detrimental to the organisation	Data or settings are fatally corrupted.	One week	Loss of life.

2.4 Example of the Information Security Risk Assessment

When assessing risks, there are two central risk categories to take into consideration: *Inherent-* and *residual risk.*



Assess Risks

Formally identified and owned risks are initially assessed as inherent, this is because the control landscape may change over time so there should be a base level of the risk to re-assess against. The inherent impact and likelihood is assessed against the CIA triad to generate the inherent score. Current controls are then put against the risk to generate the residual risk. If this residual risk is higher than defined risk appetite, then the risk is put forward to risk treatment.

Risk ID	Risk description	Inherent Impact / risk category				Impact score	Likelihood score	Inherent risk score	Risk Owner	Controls	Residual Impact / Risk category				Impact score	Likelihood score	Residual risk score	Risk decision
		C	I	A	S						C	I	A	S				
DIGRSK001	**Unauthorised access by breached or stolen credentials –** The risk of unauthorised individuals obtained access to the environment	x	x	x		4	4	Very High	Captain	Two factor authentication	x	x	x		4	2	Medium	Treat
DIGRSK002																		
DIGRSK003																		
DIGRSK004																		
DIGRSK005																		
DIGRSK006																		
DIGRSK007																		
DGIRSK008																		
DIGRSK009																		
DIGRSK010																		

- *Inherent risk* covers what the risk for the company actually is, if there are no controls in place to treat the risk.
- *Residual risk* differs from inherent risk, by covering what the risk for the company is, with the controls in place to mitigate the risk[6].

When working with residual risks, the organisation needs to define its risk appetite: how high is an acceptable risk level? This will vary between organisations, as the risk appetite will be determined at the highest levels.

[6] NIST SP 800-30 Rev. 1 under Residual Risk (CNSSI 4009). https://csrc.nist.gov/glossary/term/residual-risk

Here is an example of applying the risk template, looking at the inherent risk of malware:

Risk description	Inherent Impact / Risk category				Likelihood	Impact score
	C	I	A	S		
Malware propagation	5	5	5	3	5	25

With no controls in place to mitigate the risk (malware), the score on CIA is 5, giving us an impact score of 25 (Severity x Likelihood). The impact score describes the amount of harm that can be expected as a result of the risk materialising.

If there were controls in place to mitigate the risk, it would be expected that the risk categories (CIAS) would have a lower score than five, meaning the impact score would be reduced.

To illustrate with an example, a control to lower the risk of malware propagation could be Antivirus software.

Control(s)	Risk description	Residual risk Impact / Risk category				Likelihood	Impact score
		C	I	A	S		
Antivirus	Malware propagation	3	3	3	3	5	15

The risk catalogue needs to be reviewed on a regular basis, which could be every quarter. Reviews should happen at regular intervals, as there is a risk of a control becoming outdated. With the example provided, the antivirus solution could become end of life, leading to no protection against malware.

When applying the risk rating levels to a risk, the organisation should base the categorisation on historical data. E.g. if a phishing attack has previously occurred - it could help indicate the likelihood of how often the risk occurs. If there is no historical data on a risk, it does not automatically mean the likelihood of it occurring is low, but rather that it is a risk which is yet to be detected within the organisation.