

OCIO

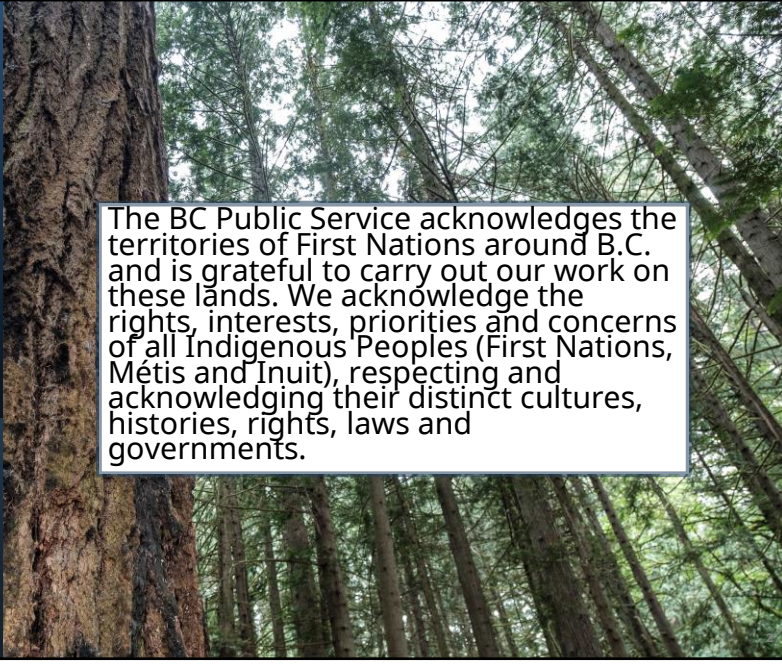
Office of the
Chief Information Officer

Security Threat and Risk Assessment 101



Ministry of
Citizens' Services

Territorial Acknowledgement



The BC Public Service acknowledges the territories of First Nations around B.C. and is grateful to carry out our work on these lands. We acknowledge the rights, interests, priorities and concerns of all Indigenous Peoples (First Nations, Métis and Inuit), respecting and acknowledging their distinct cultures, histories, rights, laws and governments.

Image Source:

Province of British Columbia (Government of BC) – Flickr

<https://www.flickr.com/photos/bcgovphotos/48308844876/in/album-72157686474934255/>

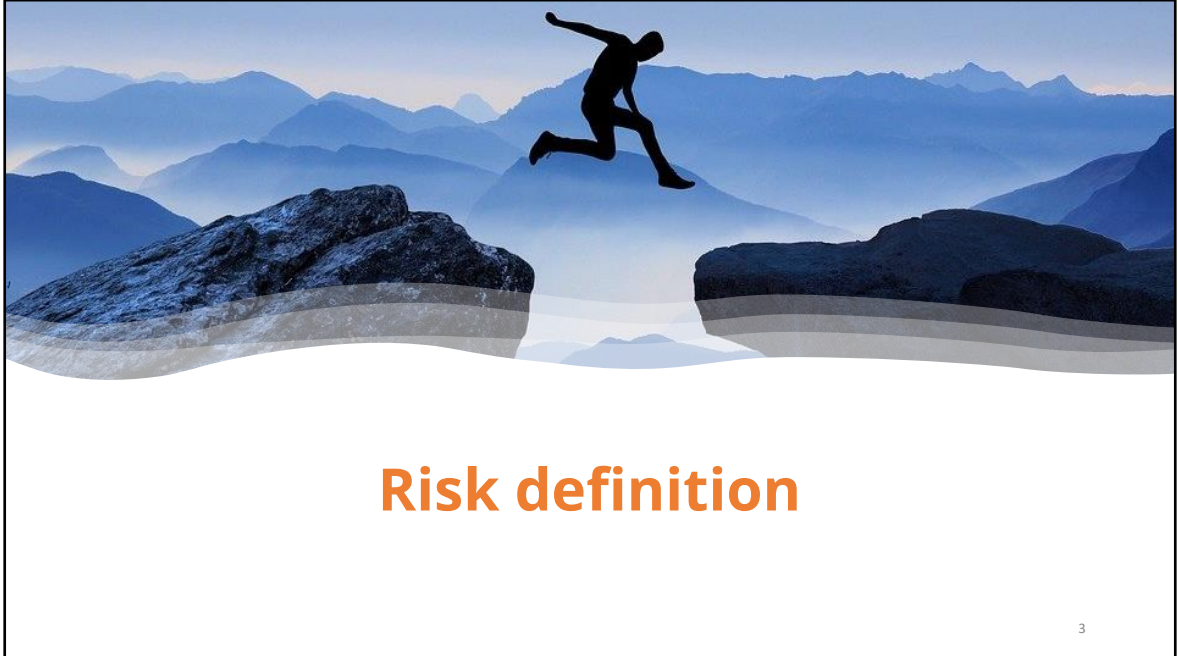
https://live.staticflickr.com/65535/48308844876_d71ac6635b_o_d.jpg

This file is licensed under the

<https://creativecommons.org/licenses/by-nc-nd/2.0/>

Free to:

- **Share** — copy and redistribute the material in any medium or format



Here are some definitions:

The effect of uncertainty on objectives.

Risk is the possibility that something could occur which might have an impact.

An acknowledgment of how likely a threat is to leverage a vulnerability, what the potential impacts could be, and what it means to the organization

Image source:

<https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment/concepts>
<https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/glossary>



Speaker: Mack

We care because of the potential for negative impacts to:

- confidentiality, availability, integrity
- systems, services, or products
- information
- organization
- clients
- other stakeholders
- and more

We care because, if risks are not treated costs can be unpredictable and possibly significant if security incidents and breaches occur.

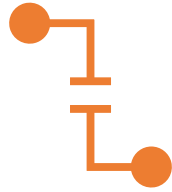
With risk management costs become more predictable and services more reliable.

We also care about risk relative to our organizations risk appetite and tolerance.

Image source:

<https://pixabay.com/photos/teds-couple-love-together-cute-1808323/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

What is a Security Threat and Risk Assessment (STRA)?



~
The process of assessing
information security risk
to a system at a point in
time.
~

What results from the STRA process?

The primary and final artefact which results from the STRA process is a Statement of Acceptable Risks (SoAR).

The SoAR artefact contains:

Meta information about the system and risk assessment

The risks to the system

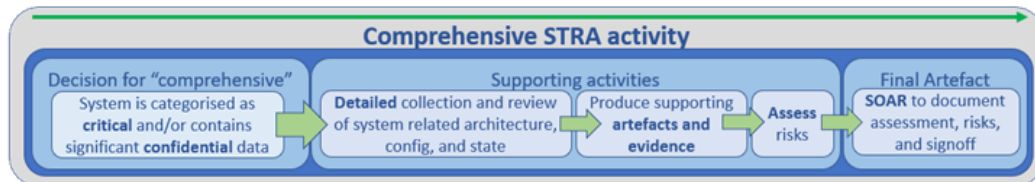
Approval of the documented SoAR by an accountable individual

Do I ever need additional documentation to support an STRA?

The primary risk evaluator may decide to produce other supporting documents, and/or collect evidence in certain circumstances.

This is often in cases where:

- a system is classified as "Critical", and/or
- where there is a level of complexity to a system, and/or
- where a significant amount of confidential information is involved.



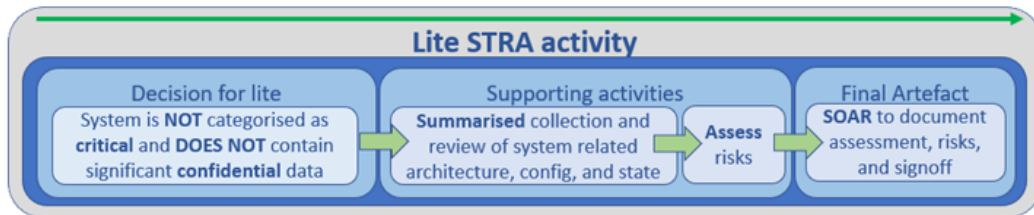
What is a comprehensive STRA?

- Any STRA where additional supporting artefacts are also supplied beyond just the SoAR.
- The SoAR is always the final artefact and is used to document the risks and handle approvals.

8

Based on the criteria of this being a critical system and handling confidential information, and with the added knowledge that this is a complex system – it would be reasonable to approach this as a COMPREHENSIVE STRA activity.

How this differs from a LITE STRA activity is that with a COMPREHENSIVE you will do some more detailed collection and review of system related architecture, config, state and so forth. You may also complete some additional documentation artifacts prior to completing the final artifact with the risks, this being the Statement of Acceptable Risks (SoAR).



What is a lite (fast tracked) STRA?

- This is any STRA where the SOAR is the only artefact resulting from the STRA process.

9

We call this a LITE STRA.

A LITE STRA is where the Primary Risk Evaluator makes a decision to only complete the SOAR artifact without any other artifacts prior. Typically the decision is made if a system is not critical and if it does not contain significant confidential data. There are also typically not very complex systems.

The assessment should be commensurate to what you are assessing. E.g. you would not put the same degree of effort into assessing a simple web form as you would a complex service involving multiple interconnected technologies.

Modality is important.

Adapt the effort you put into the assessment to match what it is you are assessing.

Is there any example / reference STRA process, more detailed, to help guide us through implementation?

Yes, there is a reference STRA process available which can help provide you with this guidance.

See:

<https://www2.gov.bc.ca/gov/content?id=31BECBD755944429B194E5780A3097DF>

Difference between compliance and risk management?

Compliance



Risk Management



A compliance assessment typically is an assessment against predefined controls to see if your organization is following and meeting standards, policies, regulation, or legislation. This is typically a yes / no, check list type activity often conducted by auditors. Usually after a compliance audit there are recommendations on how to make improvements, within the context of the assessed controls. A control is a statement of how something should be, to be in a *proper compliant state*.

Risk management is less focused on the compliance aspect, and in the context of security is more focused on the likelihood and potential impact levers related to how likely a threat might act on a vulnerability, the potential impact, and what it might mean to the organization; and any treatments to help address this. It is about reducing risk and improving and securing systems because of the intrinsic merit of this.

Image source:

<https://pixabay.com/illustrations/rule-hook-check-mark-custom-1752622/>

[Pixabay License](https://pixabay.com/service/license-summary/) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://pixabay.com/vectors/falling-hazard-warning-caution-24031/>
[Pixabay License](https://pixabay.com/service/license-summary/) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Does a risk assessment ever use controls?



12

When a security professional is conducting a risk assessment, they can identify risks a few different ways.

One way is to use an approach called threat modeling. With threat modeling you look at the systems architecture, interconnections, configuration, protocols used, software, scan results, and any other relevant information you have available to you to try to identify weaknesses with exposures which could be acted on by known threats. There are a few different threat modeling methodologies which sometimes get used; STRIDE is one example. As you find risks from the threat modeling exercise you look to see how likely the threat is to act on the vulnerability, the potential impact, and what it would mean to the organization.

Another approach is to use a pre-canned set of controls; these could be from a standard, policy, regulation, legislation, or contract. We call this a “control driven” approach. What makes this different from a compliance assessment is, you are using the controls simply to find and identify risks. As you go through the controls you are looking for weaknesses with exposures that could be acted on by known threats; versus looking to see if you are following a rule. As you find risks from the controls you look to

see how likely the threat is to act on the vulnerability, the potential impact, and what it would mean to the organization.

A third way is to use a blended hybrid approach doing some threat modeling where you need to dig deeper, but using control sets as a general guide to help you think about and keep you on track with discovering risks. This approach is balanced and can optimize efficiency in a risk assessment as it prevents you from getting stuck in the weeds, but also helps you to be able to go deep if there is a good reason to.

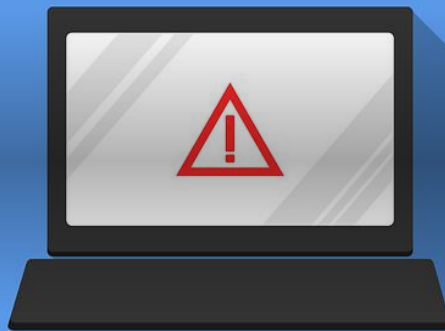
Image source:

<https://pixabay.com/vectors/man-doll-puppet-controlled-master-6853954/>

[Pixabay License](#) Free for commercial use. No attribution required.

<https://pixabay.com/service/license-summary/>

What is a “vulnerability”?



13

A weakness of an asset, system, or control that can be exploited by one or more threats.

Another way of saying this is: A vulnerability is a weakness which has an exposure which could be acted on by a threat.

Managing vulnerabilities is important as this is one part of the information security risk equation which we can make a big difference on.

Unless you are law enforcement it is often challenging to eliminate or reduce a “threat”; however, vulnerabilities (weaknesses with exposures) are within our control to patch and implement mitigating controls for.

This is why we have a vulnerability management program; because we recognize how a concerted focus on reducing vulnerabilities also reduces overall risk.

When considering risk you need to consider how likely it is that a threat might act on a vulnerability and the resulting potential impact. So – you are not just considering one

element, the threat OR the vulnerability; rather you are considering the threat AND the vulnerability.

Image source:

<https://pixabay.com/illustrations/cyber-security-internet-security-1923446/>

[Pixabay License](#) Free for commercial use. No attribution required.

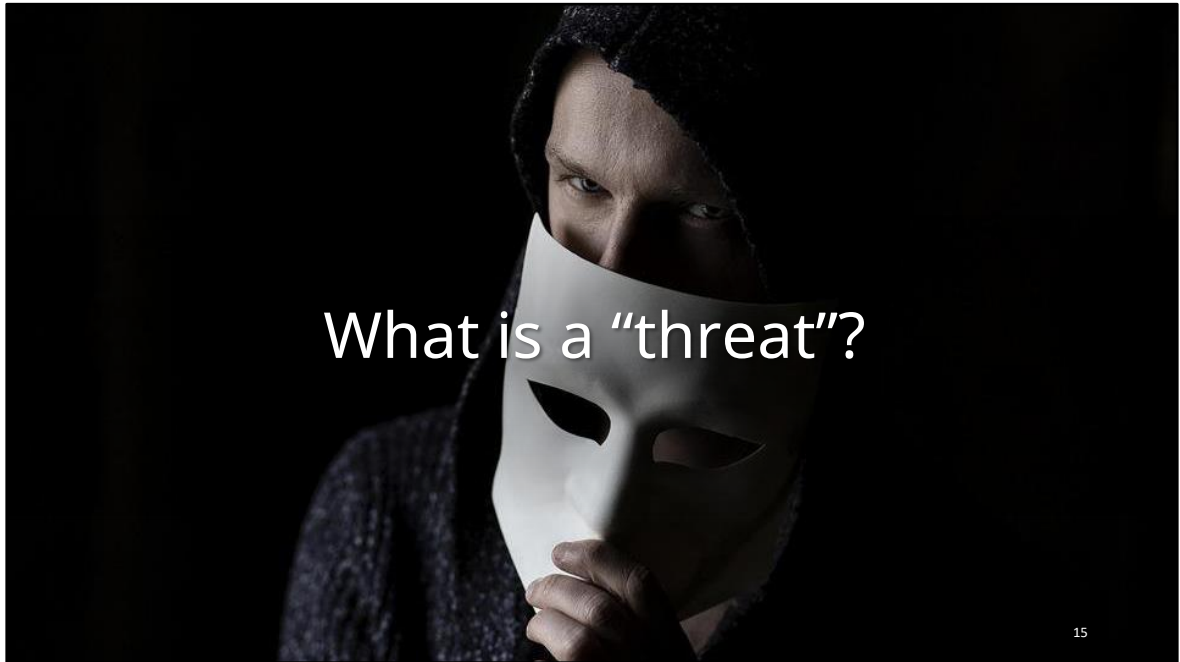
<https://pixabay.com/service/license-summary/>

Do I need to perform a vulnerability scan or penetration test every time I complete an STRA?

The short answer is NO.

In special circumstances, if a system is critical, or highly complex, the primary risk evaluator may deem it appropriate and worthwhile to conduct a vulnerability scan or penetration test to help inform an STRA.

It is advisable that the primary risk evaluator of an STRA be empowered to make this decision where possible.



A "threat" is a potential cause of an unwanted incident, which may result in harm to a system or organization.

A "threat" is any thing which can leverage (make use of) a vulnerability (weakness with exposure) to cause a harm.

The key word is "cause".

This can be a: Person, group, process or technology

Examples of threats can include:

- Juvenile
- Insider
- Hacktivist
- Organized Crime / Criminal
- Nation State

- Cyber Terrorist
- Malicious software

But... A threat can be any “THING” which can act on a vulnerability to cause an impact.

Image source:

<https://pixabay.com/photos/scam-hacker-security-virus-fraud-4126798/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Remember, risk is how likely a threat is to leverage a vulnerability, and what the potential impacts could be.



Image source:

<https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://pixabay.com/photos/mountain-leap-high-rock-boy-2699809/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment/concepts>
<https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/glossary>

How is a risk rating determined?

**LIKELIHOOD X POTENTIAL IMPACT =
RISK RATING**



Critical
Rating: 17 to 25

High
Score: 15 to 16

Medium
Score: 8 to 14

Low
Score: 2 to 7

Very Low
Score: 1

To determine a risk rating you first need to determine a numerical rating for the likelihood and for the potential impact. You then multiply these values together. The numerical risk rating which results can then be cross-referenced to determine the risk rating in plain language.

Let's talk about the risk ratings a bit more:

“Critical” Risk —> Rating = 17 to 25

Unacceptable risk which cannot be justified except in very special circumstances. Resources to treat should be made available immediately with little resistance or barriers. Treatment of critical risks should receive priority attention.

“High” Risk —> Rating = 15 to 16

Risk should be reduced but may be tolerated for a short period if the cost is prohibitive or the identified treatment would result in other adverse impacts.

“Medium” Risk → Rating = 8 to 14

Risk should be reduced but may be tolerated if the treatment cost exceeds the cost of the risk’s potential impact.

“Low” Risk → Rating = 2 to 7

Risk exists and is tolerable. It should be controlled, and treatment efforts should be maintained. The risk state may take a long period of time to improve. These risks do not receive priority attention.

“Very Low” Risk → Rating = 1

Risk exists and is tolerable. It should be controlled, and minimal treatment efforts should be maintained. The risk state may not improve over time. These risks do not receive priority attention.

Image source:

<https://pixabay.com/illustrations/rating-star-five-application-4068907/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

How can I determine likelihood for a risk?



Almost certain (>90-100%)
Score: 5

Likely (>50-90%)
Score: 4

Possible (>25-50%)
Score: 3

Unlikely (>10-25%)
Score: 2

Rare (0-10%)
Score: 1

Likelihood is the possibility or probability that a threat might act on a vulnerability to cause an impact.

Understanding and factoring in likelihood is part of the risk equation.

Don't forget to consider likelihood. If you only consider impact and not likelihood too, you are not really assessing RISK.

We can try to consider likelihood first by looking at what we know.

If we know that threats have acted on a particular type of vulnerability a certain number of times over the last year, the year before, and so forth with our organization or similar organizations, we may be able to reasonably predict the likelihood of occurrences this year. This is called the Annual Rate of Occurrence. This is a reasonable quantitative approach to likelihood.

It is important to understand that when you are dealing with possibilities and probability that it is still a guess, however educated you are trying to be. Better data

just means you have a better chance of getting it right. With experience gut feel on likelihood can sometimes be just as effective as taking a quantitative approach. A lot depends if you have a point of comparison, context, and similar past experiences to draw on. With experience comes confidence on this.

Sometimes we don't have a detailed level of information to work with. In this case the application of likelihood in your risk assessment will need to be a gut feel. This is a qualitative assessment.

An aspect to consider is that other factors can also influence likelihood. For example, past occurrences alone while they are quantitative, don't consider factors such as world events, shifts in threats, newly discovered aspects to a vulnerability, or exposure of weaknesses. So, in many ways a qualitative review and assessment of likelihood where many factors are looked at and considered together can result in a better, more thoughtful, and more accurate determination of likelihood. Many of the mentioned factors are hard to quantify.

You should also try to consider these aspects when thinking about likelihood.

Image source:

<https://pixabay.com/vectors/bayesian-statistics-bell-curve-2889576/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

How can I determine impact for a risk?



**Catastrophic
Score: 5**

**Major Impact
Score: 4**

**Moderate Impact
Score: 3**

**Minor Impact
Score: 2**

**Negligible Impact
Score: 1**

Different sources of training will use slightly different words for this term which are all driving at the same thing.

You may hear the following words used interchangeably with “impact”, including: Harm, and Consequence

An impact in information security is usually the potential of something negative happening related to confidentiality, availability or integrity.

Downstream the impacts can further manifest as reputational harm, financial harm, economic harm, physical harm, psychological harm, social harm, and more. Understanding this helps us understand the meaning to the organization.

Always think about what the impacts might mean to your organization, clients, and stakeholders.

When we consider and express impact in any of the previously mentioned contexts and at that level, the assessment of impact is qualitative.

When we go another layer deep, however, this then makes the assessment quantitative.

Let's dig into this further with some examples:

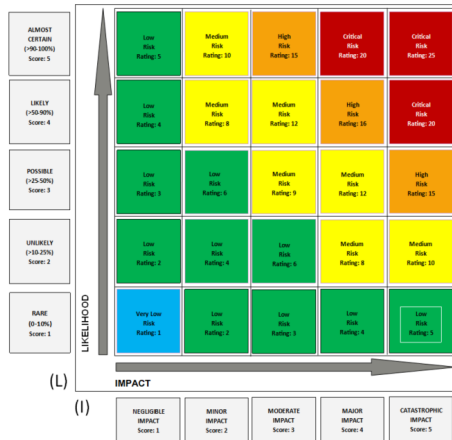
If I say an impact is to availability, this might mean a reputational and financial harm. If I left my impact statement at that level and moved directly to assign an impact rating, this would be an example of a qualitative assessment of impact.

If I went on to say that the reputational impact could cause citizens to not trust the service, and the reduction in use could necessitate the shutdown of the service – what if this service was a profit centre for the organization? This could mean for example that the organization might lose 2 million dollars of potential profit annually. This would be an example of a quantitative assessment because I have followed a logical path to determine an impact which has been defined numerically with quantities defined. I can then use this information to assign an impact rating.

Image source:

<https://pixabay.com/photos/asteroid-comet-meteorite-3628185/>
[Pixabay License](https://pixabay.com/service/license-summary/) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

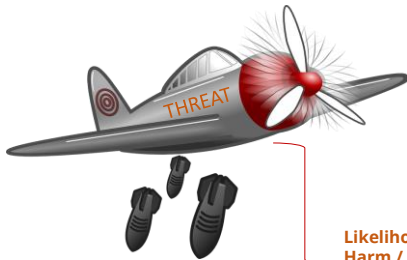
Make rating risk easy. Use a matrix.



See:

<https://www2.gov.bc.ca/gov/content?id=BA0689FE831E4C719D4BA54690D6C5DF>

Let's bring it all together



Vulnerability
(Exposed Weakness)
(OPEN HATCH)



Likelihood that a
Harm / impact will
occur =
Almost Certain
(MUNITION IS FALLING
DIRECTLY ABOVE TANK)

Potential impact =
Catastrophic
(TANK IS NO MORE)



What does it mean to the organization?
(Loss of life, loss of equipment, and loss of battle.)

21

Scenario:

Let's pretend there is a war. In this scenario, the aggressor (threat) is using an air raid to attack.

What was the likelihood of this occurring?

Almost certain because the plane which is the threat is right over top of a tank which has its hatch wide open. The hatch is a weak point on the tank, and with the hatch wide open there is a clear exposure related to this weakness.

What was the potential impact?

Catastrophic because a downward bomb attack from the plane could make the tank no more. Beyond a loss of equipment this could mean a loss of life. If this occurs to enough tanks, it could mean a loss of the battle.

What would the risk rating have been?

Critical. If we use the risk matrix we can at a glance see that the risk rating would be "Critical" for this risk.

What are some mitigating controls which could have been put in place and would have reduced the risk?

- Keep the hatch closed when it doesn't absolutely need to be open.
- Invest in faster tanks.
- Invest in air-defence systems.

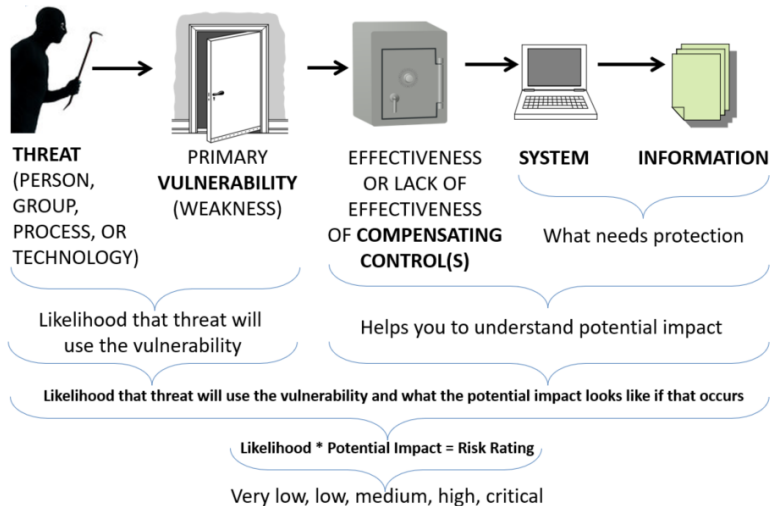
Image source:

<https://pixabay.com/vectors/air-raid-bombing-raid-bomber-bomb-148909/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://pixabay.com/vectors/tank-cannon-weapons-t-34-war-6898680/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://pixabay.com/vectors/explosion-detonation-blast-burst-147909/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Let's bring it all together



Scenario:

Lets pretend a thief is in the neighbourhood. You are aware that homes close by have been broken into. Despite this you are a very trusting person. You go out to the store and leave your front door wide open. This is a weakness because the lock is not engaged and there is an exposure as the door is wide open for the thief to see and walk through. The thief does spot this and enters your home while you are aware. You have tried to be secure by storing your most valuable possessions, including your laptop in a safe. This compensating control unfortunately is ineffective as the safe is not very heavy and you did not bolt it to the floor. You telework. You have confidential information on your laptop which is very important to your organization. Your laptop is not encrypted. The thief picks up the safe and walks off with it. Once the thief gets home he takes a crow bar to the safe and opens it. He finds your laptop and is able to extract the confidential information from it. He then used the information to hold your organization ransom for 1 million dollars.

What was the likelihood of this occurring?

Almost certain because the thief was already known to be in the neighbourhood.

What was the potential impact?

Major impact because of the level of potential harm to your organization.

What would the risk rating have been?

If we use the risk matrix we can at a glance see that the risk rating would be **“Critical”** for this risk.

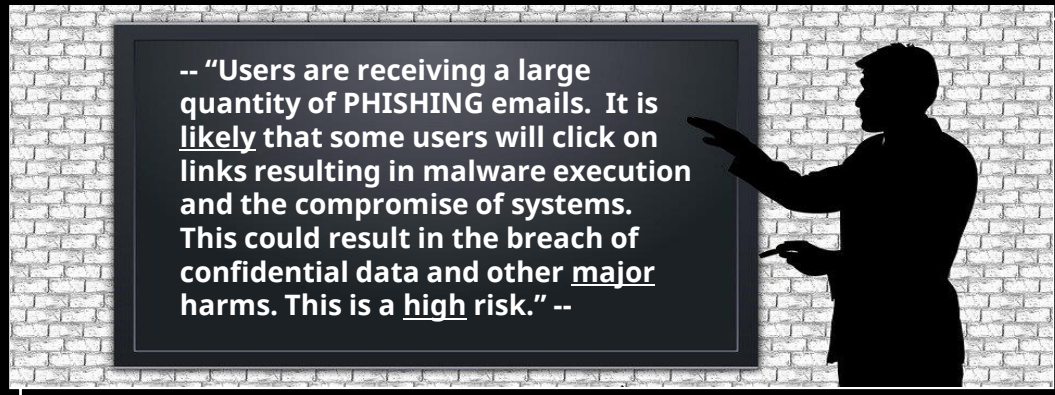
What are some mitigating controls which could have been put in place and would have reduced the risk?

- Lock the door
- Mount the safe to the floor
- Have a home security / alarm system in place



Writing a risk statement / description

EXAMPLE



This is a good example because it captures the elements of a risk. The exposure is acknowledged: e.g. "Users are receiving a large quantity of PHISHING emails" The weakness is acknowledged: e.g. "

Image source:

<https://pixabay.com/illustrations/smartboard-monitor-training-school-1523538/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Responsible VS Accountable

1

Responsible
means you have
an obligation to
perform a task.

2

Accountable
means you must
answer for the
overall outcome.

24

When conducting a Security Threat and Risk Assessment it is important to understand these two terms, “Responsible” vs “Accountable”.

Responsible means you have an obligation to perform a task. Accountable means you must answer for the overall outcome.

What do you do once you know you have a risk?

Treat it



or

Consciously Accept it



Don't ignore it



Treatments can include:

- Remediate (fix)

- Mitigate (reduce)

- Transfer (shift liability to someone else – e.g. insurance)

- Avoid (change circumstance so that the risk no longer applies)

If you aren't going to treat a risk, this should mean that the accountable individual is satisfied that the risk is within an acceptable level consistent with their risk appetite. (i.e. they have accepted it)

You shouldn't ignore the risk, leaving it without a treatment or acceptance.

Image source:

#1

<https://pixabay.com/photos/auto-repair-oil-change-oil-auto-3691962/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

#2

<https://pixabay.com/illustrations/thumbs-up-good-great-like-thumb-4423320/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

#3

<https://pixabay.com/photos/man-head-scared-cover-emotion-314481/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Treating risk



26

Let's think further about the risk statement we talked about a moment ago.

What are some potential treatments?

Avoid – You could avoid the risk by shutting down email as a service and instructing business areas to find other ways to communicate. This isn't a very feasible or realistic treatment.

****** Mitigate (Recommended) ****** – You could put in place safeguard controls such as SPAM filters and training / awareness in place to reduce the risk to an acceptable level.

Transfer – You could purchase cyber breach insurance in case an attack is successful.

Remediate – You could try to find a way to completely fix the risk. In this case it is unlikely.

Accept – If you are an accountable individual, you could decide that the risk level is within your risk appetite and tolerance. By accepting you would also be acknowledging that you have the financial capacity to handle any harms which could occur should the risk play out.

Image source:

#1

<https://pixabay.com/vectors/worker-craft-tools-craftsmen-6351121/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

#2

<https://pixabay.com/vectors/woman-business-point-hand-up-1453935/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

#3

<https://pixabay.com/illustrations/man-manager-employer-office-banker-5583395/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

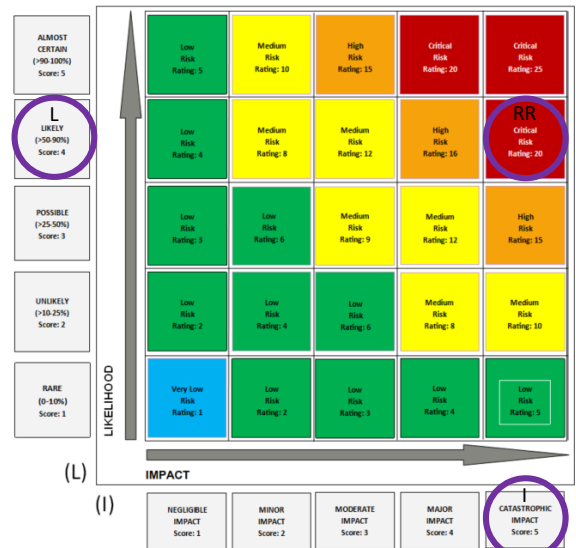
#4

<https://pixabay.com/vectors/africa-african-comic-characters-2027628/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

#5

<https://pixabay.com/vectors/woman-engineer-work-worker-lady-1455991/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Example Risk: Risk to house by tree



$$\text{Likelihood (L)} * \text{Impact (I)} = \text{Risk Rating (RR)}$$

OCIO

OCIO
CIRMO

OCIO
CONN

OCIO
DPD

OCIO
ES

SBC

GDX

RPD

PSD

CSD

Asset at risk = House

Threat = Large, old, rotten Fir tree close to house with lots of wind. Large branches hang over top of the roof. Main trunk of the tree leans significantly over the house. Tree roots also threatens house.

Vulnerability = Exposure – No way to protect roof from falling branches or tree. Holes in perimeter drain tubing may allow roots into the system. Weaknesses – Old roof tiles and boards. Perimeter drains are close to the root system from the tree and the tubing is old and brittle.

Likelihood = Likely.

Potential impact = Catastrophic impact. If tree or large branch falls the roof, and/or building structure could be damaged. This could be costly to repair and may or may not be covered by insurance. Could result in bankruptcy. Injury to people or animals could occur, up to and including death. Infiltrated perimeter drains could result in basement flooding resulting in flooding and damage to property.

Overall risk rating = Critical

Treatment =

- 1) Transfer - Make municipality aware of the concern to transfer liability to them if they do not approve work to be done on tree.

and

2) Mitigate – Significantly prune the tree to take weight off it.

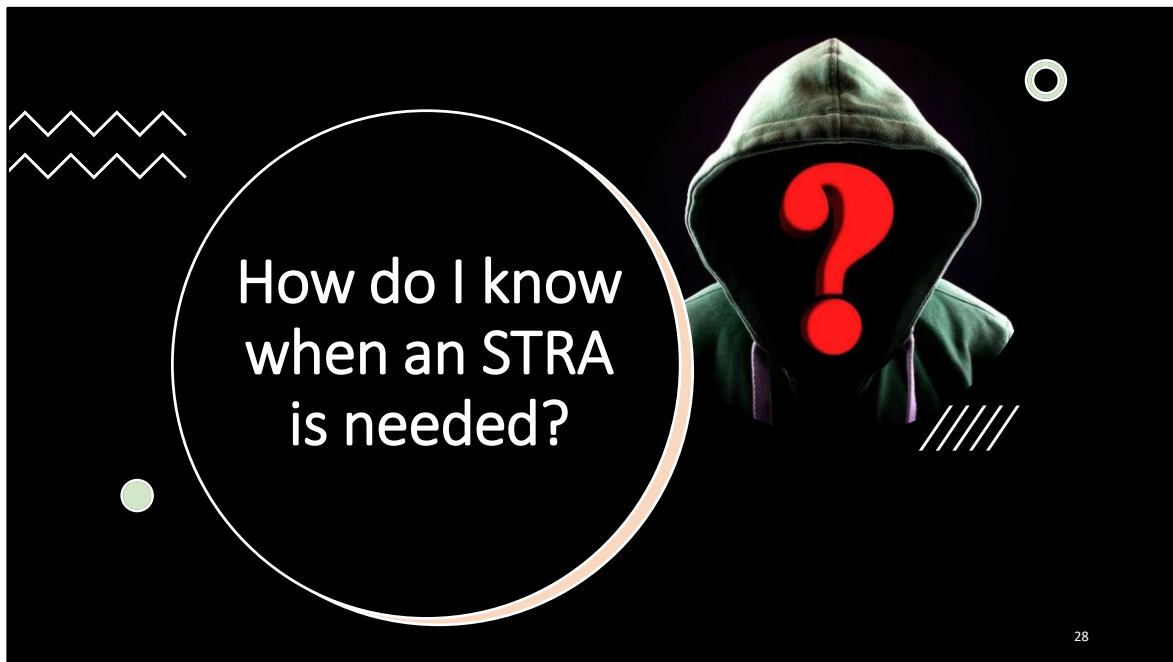
or

3) Remediate - Request permit from municipality to cut down rotten portions of tree. Cut down or prune the tree as approved.

Image source:

<https://pixabay.com/photos/house-architecture-front-yard-1836070/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

<https://pixabay.com/vectors/tree-grenn-fruits-trunk-falling-158522/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>



STRAs are conducted for new information systems and for contracting arrangements.

Information Owners and Information Custodians of a new or significantly modified information system must conduct a Security Threat and Risk Assessment.

STRAs must also be conducted for all information systems during planning, development and implementation.

A review and updated STRA must be conducted throughout the life of an existing information system for any significant or material change(s) and must also consider any previously identified risks.

Information Owners must ensure Security Threat and Risk Assessments are performed regularly to identify and minimize the risks to information and information systems they own.

For projects, an information Security Threat and Risk Assessment is conducted at an early stage of the project to identify necessary controls.

Prior to constructing any new information processing facilities, Information Owners and Information Custodians must conduct a Security Threat and Risk Assessment.

The head of the government organization is accountable for ensuring that appropriate and reasonable support and resources are provided for this to occur.

Image source:

<https://pixabay.com/photos/hacker-question-mark-hoodie-attack-2883630/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

Sources:

https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/01_-_information_security_standard_v20.pdf
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/stra_standard_v30.pdf

**Example of how to
complete a SoAR for an
STRA**

29

Example of how to complete a SoAR for an STRA

FICTIONAL EXAMPLE

SECTION A – TRACKING INFORMATION

Assessment Reference Number: <u>REF1234</u>	Type: <u>COMPREHENSIVE</u>
System Name: <u>Payroll123</u>	Primary Risk Evaluator: <u>Mr Danger</u>
Division: <u>Head Office, Municipality of Adanac</u>	Owner: <u>John Joe</u>
Branch: <u>Information Technology Branch</u>	SoAR is confidential: ☐
System stores or handles confidential information: ☒	STRA is shareable: ☒
Critical System: ☒	Scope: <u>BRANCH</u>
Short Description :	
The new "Payroll123" system is a Software as a Service (SaaS) cloud application offered by Payroll Corp. They use an AWS backend to host the SaaS application. The SaaS application runs from AWS systems in the United Kingdom. This new system is required to replace a previous system which was using old technology, and which was not meeting business needs. For this Security Threat and Risk Assessment a threat modeling approach has been taken to assess the risks to the system. A supporting document is also attached which supplies evidence for the risks, along with configuration, and system architecture details. If the noted risks are treated, then use of the system for it's intended purpose with Protected B data appears to be appropriate and reasonable.	

Example of how to complete a SoAR for an STRA

FICTIONAL EXAMPLE

SECTION B – RISK ASSESSMENT TABLE

If more rows are needed please copy from an existing row to keep the drop-downs available. If no risks are identified in the SoAR provide a justification in the description box in Section A.

RISK REF #	RISK NAME	PRIMARY RISK TYPE	RISK RATING	TREATMENT PLAN	SHORT DESCRIPTION
1	Potential for interception of data which could represent a confidentiality harm as it relates to personal information. This could negatively impact staff.	Confidentiality	Medium	Plan - Treat: Mitigate (reduce) risk	Many network hops to get to the service where it is hosted in the United Kingdom means increased opportunities for threat actors to potentially try to intercept network traffic related to the service. This means the likelihood of such an attack is increased. The risk level remains at "Medium", however, as other compensating controls include strong encryption in transit and at rest, the use of multi-factor authentication, and access control lists which only allow connection to the site instance for those coming in from authorized IP addresses helps to balance the risk. Discussions could occur with the company Payroll Corp to see if the service could be hosted in North America or Canada.

And more risks...

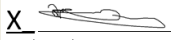
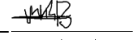
31

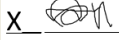
Example of
how to
complete a
SoAR for an
STRA

FICTIONAL EXAMPLE

SECTION C – ACCEPTANCE

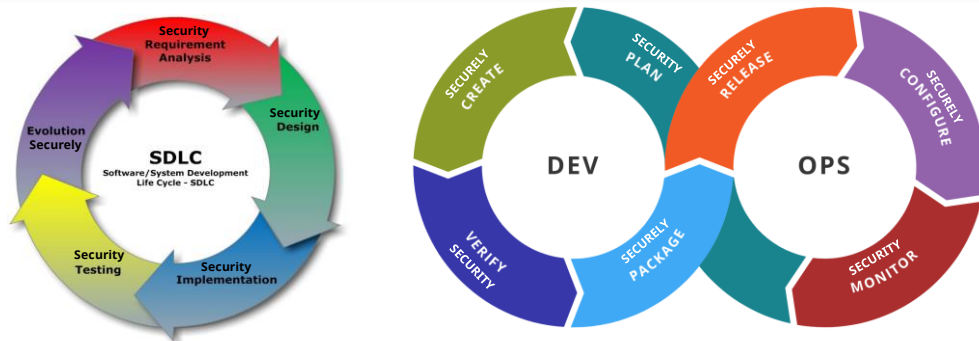
Please do not remove or change the signature blocks marked "required". You may add as many additional signature fields as needed by your ministry. Digital or printed signatures are acceptable. If electronic signatures are attached please note in the signature fields.

Signing below constitutes your recommendation of this SoAR to the accountable individual.	
Signature	X  Owner (If <u>required</u>) X  Information Security Officer (Required)
Name & Title	John Joe Mr. Danger
Date	7/21/2023 7/21/2023

Signing below constitutes acceptance by the accountable individual of the risks documented in Section 8, their ratings, and treatment plans.	Submission Instructions
President, CEO, CIO, or delegate signature	Submit this signed form to the appropriate location or email as an attachment to: security@Municipality-of-Adenac.ca
Name & Title	Any questions regarding this form can also be directed to this email.
Date	
X  Accountable Individual (Required) Joe Smith 7/24/2023	

CISO RECEIPT OF SOAR - FOR OFFICE USE ONLY	
Signing below acknowledges receipt of the SOAR by the CISO. This marks the completion of the risk assessment. SOARs which are obviously incomplete or inaccurate will not receive a signature.	
CISO, or delegate signature	X  Chief Information Security Officer (Required) Name: Mary Lerkins
	Date 7/25/2023

Software / System Development Life Cycle (SDLC) and DevOps



Even when we don't make changes, legacy and unpatched software can be at risk for vulnerabilities as they are discovered in the industry. As threat actors become aware they then look for opportunities to attack those with the vulnerabilities (weaknesses with exposures). This puts our organization at increased risk.

Don't secure just once and walk away. Whether leveraging traditional lifecycles or leveraging DevOps, keep security as a discussion and activity at every stage.

Throughout system and software lifecycles security risk needs to be consideration and part of work plans.

Involve security professionals at each stage.

Security is not the blocker to a product's launch. Recognize that feedback and recommendations related to security are provided to help ensure the success and enablement of the product and is intended to help reduce the chance of unpredictable blockers.

By making security part of every stage, we can avoid significant technical security debt which later can be impactful to a product when it needs to be corrected.

If we consider security at every stage our systems, services, and products will be more resilient.

Security Threat and Risk Assessments (STRA) help us to identify and analyze risk for new and significantly / materially changed systems. They help in assessing risk at points in time through the life of a system. STRAs help us to not forget to assess security risk.

Image source:

#1

https://commons.wikimedia.org/wiki/File:SDLC_-_Software_Development_Life_Cycle.jpg

This file is licensed under the [Creative Commons Attribution-Share Alike 3.0 Unported](https://creativecommons.org/licenses/by-sa/3.0/) license.

<https://creativecommons.org/licenses/by-sa/3.0/>

Free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material for any purpose, even commercially

#2

<https://commons.wikimedia.org/wiki/File:Devops-toolchain.svg>

This file is licensed under the [Creative Commons Attribution-Share Alike 4.0 International](https://creativecommons.org/licenses/by-sa/4.0/) license.

<https://creativecommons.org/licenses/by-sa/4.0/>

Free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material for any purpose, even commercially



**Why considering
security risks at
every stage is
advisable**

Image source:

Attribution: Judy Baxter

<https://www.flickr.com/photos/judybaxter/281024071>

https://live.staticflickr.com/87/281024071_d4fec7a1ec_o_d.jpg

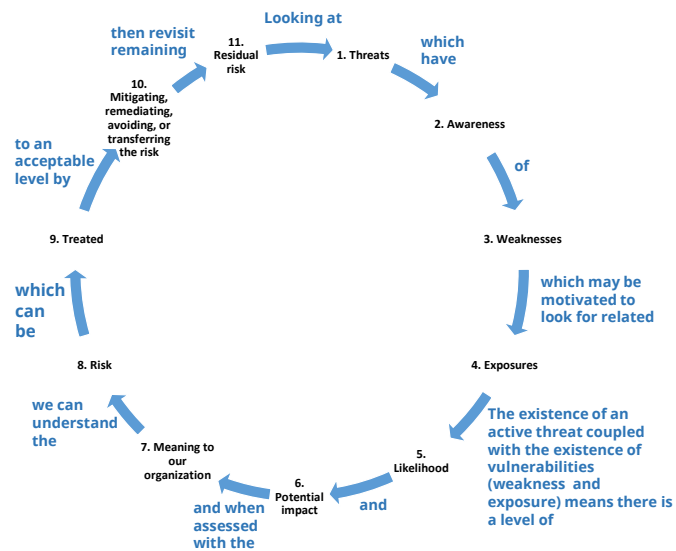
License: Creative Commons [Attribution-NonCommercial-ShareAlike \(CC BY-NC-SA 2.0\)](https://creativecommons.org/licenses/by-nc-sa/2.0)

<https://creativecommons.org/licenses/by-nc-sa/2.0>

Free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material

The information security risk lifecycle



35

When looking at “6. Potential impact” and “7. Meaning to our organization” think of an asteroid hitting earth. The initial “Potential impact” is that an asteroid hits the ocean causing an impact of Tsunamis world-wide which can lead to further destruction / harm. When you assess the scope of the potential impact further by considering the size of the asteroid and speed you can then, through inference and logic determine what the impact would mean to civilization, in this case – e.g. the end of civilization, or near to that. By thinking through the meaning of an impact we can better understand the risk.

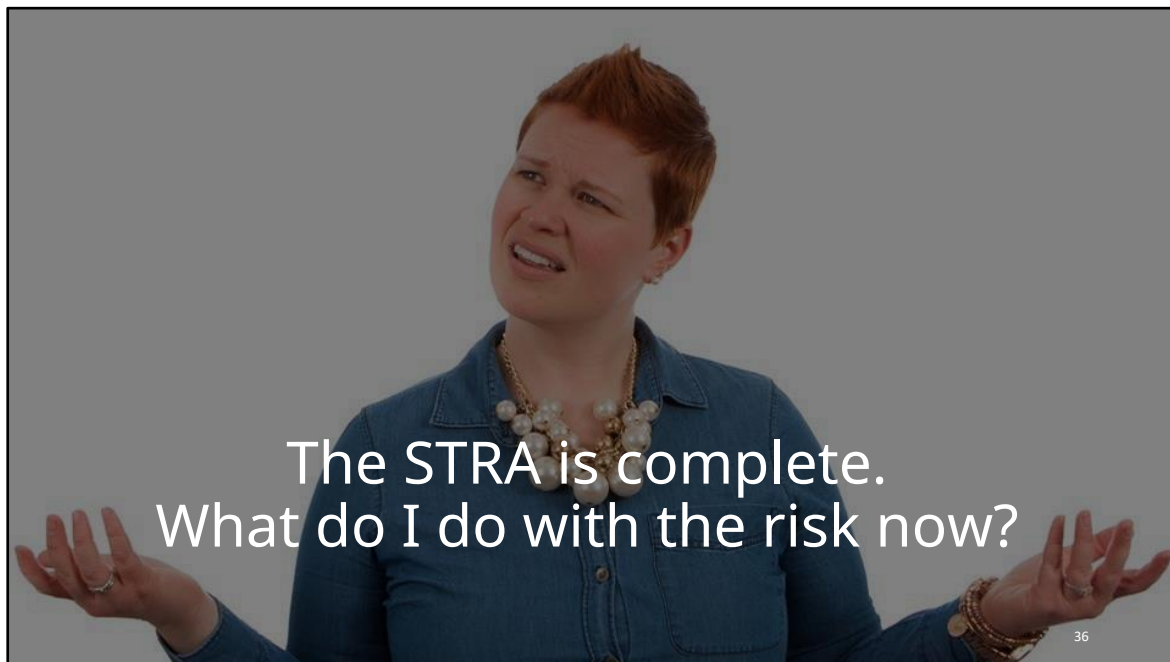
Apply the same concept to information technology now. Imagine your email server is hacked and confidential emails are breached. This on its own is an impact, however, as you investigate the impact further you can start to determine the meaning of the impact to your organization. For example, maybe the breach creates a situation where public confidence is lost in the service. Maybe this means a decision is made to stop offering a service. In this case, the meaning of what has occurred extends beyond the initial impact that a server was breached, and some data was stolen.

Always think about what the risk will mean.

Have an inquisitive mind when identifying and assessing risk.

Don't be afraid to ask questions.

Don't fear monger. Follow logical steps as shown in the risk lifecycle.



Don't just call it done and put it on a shelf.

Any residual risks which still require a treatment action should be prioritized, tracked, and followed-up on from a risk register.

The key is – risks should be followed-up on. Risk assessment does not have a functional purpose if follow-up does not occur.

Risk registers are a tool to facilitate identified risks not getting lost and treatments happening.

Image source:

<https://pixabay.com/photos/poses-female-education-posing-1367416/>
[Pixabay License](#) Free for commercial use. No attribution required.
<https://pixabay.com/service/license-summary/>

What can a risk register look like?

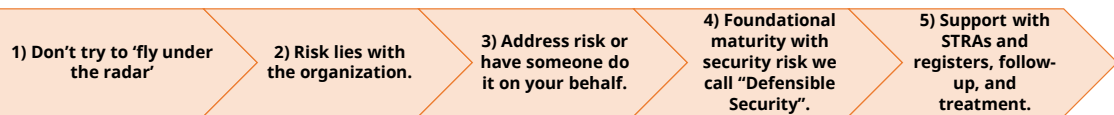
 BRITISH COLUMBIA Risk Register																
Risk ID	Risk Category	Risk Name	System or asset which is the subject of the risk?	Describe the threat (thing) which could act on the vulnerability	Describe the vulnerability which could be leveraged (exposure and weakness)	Likelihood Rating	Likelihood Rating # (Calculated)	Potential Impact Rating	Potential Impact Rating # (Calculated)	Describe the Potential Impact (what would it mean to the organization?)	Risk Rating #	Risk Rating	Planned Treatment?	Treatment assigned to (person)	Treatment target date?	Treatment complete?
1						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
2						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
3						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
4						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
5						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
6						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
7						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
8						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
9						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
10						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
11						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
12						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
13						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
14						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
15						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
16						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No

https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/vulnerability-risk-management/risk_register_template.xlsx

EXAMPLE

Risk ID	Risk Category	Risk Name	System or asset which is the subject of the risk?	Describe the threat (thing) which could act on the vulnerability	Describe the vulnerability which could be leveraged (exposure and weakness)	Likelihood Rating	Likelihood Rating # (Calculated)	Potential Impact Rating	Potential Impact Rating # (Calculated)	Describe the Potential Impact (what would it mean to the organization?)	Risk Rating #	Risk Rating	Planned Treatment?	Treatment assigned to (person)	Treatment target date?	Treatment complete?
1	Network and Device Security	Users are receiving a large quantity of PHISHING emails which are likely to result in harms to systems.	Workstations and other connected systems	Malicious actor using a phishing email to infect system with malware.	Users who are not adequately trained or aware of how to handle Phishing emails. Systems which are not sufficiently hardened with anti-malware software.	Likely	4	Major	4	Systems infected by a successful Phishing attack could result in a ransom situation or further lateral attacks by malware to other network devices. This could cause harms to confidentiality, availability, or integrity. Downstream this could cause reputational and financial harm.	16	HIGH	Mitigate	JOHN DOE	2122-01-01	No

Key take aways



38

1. Ignoring risk or trying to 'fly under the radar' and go unnoticed is not being risk-based.
2. Risk always lies with the organization.
3. Organizations must address risk or have someone do it on their behalf.
4. There is a foundational maturity that must be achieved to address information security risk; we call this "Defensible Security".
5. All of this should be guided and supported by Security Threat and Risk Assessments, and a Risk Register for residual risks which require tracking, follow-up, and treatment.

Where can I
find more
on how to
complete
an STRA?

**Government of B.C.
STRA site**

<https://www2.gov.bc.ca/gov/content?id=7175C19B66564EA3A343AB8B668BEFC2>

39

•Security Threat and Risk Assessment

- [Concepts](#)
- [Approach](#)
- [Assessment Process](#)
- [Outputs](#)
- [Tools and Templates](#)

Where can I
find more on
Information
Security
Risk
Management
?

**Government of B.C.
Professional Development site**

<https://www2.gov.bc.ca/gov/content?id=56FE9F38FC2749B286B59C6D04D30A22>



Thank you for joining us today. We are happy to now take questions.

Image Sources

Pixabay License

(<https://pixabay.com/service/license-summary/>)
Free for commercial use. No attribution required.

- <https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/>
- <https://pixabay.com/photos/teds-couple-love-together-cute-1808323/>
- <https://pixabay.com/illustrations/rule-hook-check-mark-custom-1752622/>
- <https://pixabay.com/vectors/falling-hazard-warning-caution-24031/>
- <https://pixabay.com/vectors/man-doll-puppet-controlled-master-6853954/>
- <https://pixabay.com/illustrations/cyber-security-internet-security-1923446/>
- <https://pixabay.com/photos/scam-hacker-security-virus-fraud-4126798/>
- <https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/>
- <https://pixabay.com/photos/mountain-leap-high-rock-boy-2699809/>
- <https://pixabay.com/illustrations/rating-star-five-application-4068907/>
- <https://pixabay.com/vectors/bayesian-statistics-bell-curve-2889576/>
- <https://pixabay.com/photos/asteroid-comet-meteorite-3628185/>
- <https://pixabay.com/vectors/air-raid-bombing-raid-bomber-bomb-148909/>
- <https://pixabay.com/vectors/tank-cannon-weapons-t-34-war-6898680/>
- <https://pixabay.com/vectors/explosion-detonation-blast-burst-147909/>
- <https://pixabay.com/illustrations/smartboard-monitor-training-school-1523538/>
- <https://pixabay.com/photos/auto-repair-oil-change-oil-auto-3691962/>
- <https://pixabay.com/illustrations/thumbs-up-good-great-like-thumb-4423320/>
- <https://pixabay.com/photos/man-head-scared-cover-emotion-3114481/>
- <https://pixabay.com/vectors/worker-craft-tools-craftsmen-6351121/>
- <https://pixabay.com/vectors/woman-business-point-hand-up-1453935/>
- <https://pixabay.com/illustrations/man-manager-employer-office-banker-5583395/>
- <https://pixabay.com/vectors/africa-african-comic-characters-2027628/>
- <https://pixabay.com/vectors/woman-engineer-work-worker-lady-1455991/>
- <https://pixabay.com/photos/house-architecture-front-yard-1836070/>
- <https://pixabay.com/vectors/tree-grenn-fruits-trunk-falling-158522/>
- <https://pixabay.com/photos/hacker-question-mark-hoodie-attack-2883630/>
- <https://pixabay.com/photos/poses-female-education-posing-1367416/>

Creative Commons Attribution-Share Alike 3.0 Unported license.

(<https://creativecommons.org/licenses/by-sa/3.0/>)

Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material for any purpose, even commercially.

- https://commons.wikimedia.org/wiki/File:SDLC_-_Software_Development_Life_Cycle.jpg

Creative Commons Attribution-Share Alike 4.0 International license.

(<https://creativecommons.org/licenses/by-sa/4.0/>)

Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material for any purpose, even commercially.

- <https://commons.wikimedia.org/wiki/File:Devops-toolchain.svg>

Creative Commons Attribution-NonCommercial-ShareAlike (CC BY-NC-SA 2.0).

(<https://creativecommons.org/licenses/by-nc-sa/2.0/>) Attribution: Judy Baxter

Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material.

- <https://www.flickr.com/photos/judybaxter/281024071>
- https://live.staticflickr.com/87/281024071_d4fec7a1ec_o_d.jpg