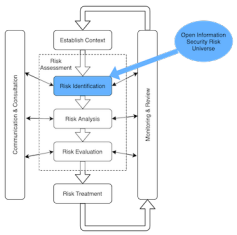
Open Information Security Risk Universe

1 Table of Contents

2 Introduction

A Risk Universe provides a comprehensive view of the possible risks we face. This view is designed to aid in categorisation but also to act as a check on the scope of our risk identification exercises to ensure we don't miss risks that then take us by surprise when they occur.

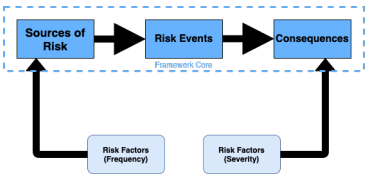


The goal of the Open Information Security Risk Universe (OISRU) is to provide a model and method independent framework and taxonomy for expressing and categorising security risk.

This framework should be complementary to the Basel II operational risk event types, recognising that information security risk permeates operational risk.

2.1 Overview of the Risk Universe

The Open Information Security Risk Universe comprises, at it's core, Sources of Risk Events, Risk Events and Consequences of Risk Events. These are supplemented by Risk Factors that drive the Frequency or Severity of the Risks.



The Open Information Security Risk Universe does not directly address likelihood or controls as these are covered in other relevant analysis and evaluation methods.

2.2 Definitions

Risk: *The effect of uncertainty on objectives. Usually expressed in terms of risk sources, possible events and their consequences and likelihood.* (Source: ISO 31000)

Sources of Risk: *Element which alone or in combination has the potential to give risk to risk.* (Source: ISO 31000)

Risk Event: *Occurence or a change of a particular set of circumstances.* (Source: ISO 31000)

Consequences: *Outcome of an event affecting objectives.* (Source: ISO 31000)

Likelihood: *Chance of something occuring.* (Source: ISO 31000)

Control: *Measure that maintains or modifies risk.* (Source: ISO 31000)

2.3 Other Relevant Standards

- NIST Special Publication 800-30 R1 Guide for conducting risk assessments* has a comprehensive set of threat sources (Risk Sources) in Appendix D, a *very* comprehensive set of threat events (Risk Events) in Appendix E and a list of effects of threat events (Consequences) in Appendix H.
- Octave Allegro has an indicative set of threat trees in Step 5 (Risk Sources) and in Appendix B includes the Impact Areas (Consequences) and in Appendix C includes Threat Scenarios (Risk Events).

Both of these standards are very useful and highly recommended sources but they do tie their taxonomy into specific qualitative methods for risk analysis. The goal of OSIRU is to be independent of any particular analysis model, whether quantitative or qualitative.

- ISO27005 includes a list of consequences in Appendix B.2.3 and Appendix C includes a mixed list of events and sources. Appendix C seems to use the term consequences in a somewhat muddled way.

2.4 Contributors

The following people have contributed to this document:

- Phil Huggins
- Paul De Luca
- Robin Oldham
- Jordan M. Schroeder
- Tony Richards

2.5 License

3 How to use

3.1 Risks

It's key to understand that a risk event alone is not a risk, at it's simplest a risk can be a single risk event and the single consequence of that event.

However, it is likely as we develop our risk scenario that they will consist of the combination or one or more sources, one or more risk events and one or more consequences.

Risk events may lead to other risk events within the scenario. For example a *software exploit* may lead to *unauthorised access to a system* that then causes consequences.

3.2 Risk Scenarios

Risk scenarios are the business-context descriptive narrative form of the risks facing your business. The risk scenarios are useful in communicating with stakeholders about the risk as they feel like real-world stories they recognise from their own experience. Risk scenarios tend to be specific to business functions and their environment.

For example:

Title: *"Accidental Market Sensitive Information Leak."*
Description: *"During the reporting period a member of the accounting team, under time pressure, accidentally sends a draft of the annual report to an employee at our technology outsourcer who has the same name as our Chief Financial Officer as a result of address auto-complete in their email software. If the draft leaks it could lead to market sensitive information being published ahead of the publication of the report which could lead to a regulatory sanction and trigger insider trading*".

When writing relevant risk scenarios the analyst should consider:

- **Context** - *'Who'* - Groups, Individuals, Organisations
- **Triggers** - *'Why'*, - Motivations, Goals
- **Event** - *'What, How'* - Activities, Objectives, Targets
- **Timelines** - *'When, How long'* - Triggering Events, Opportunity
- **Location** - *'Where*' - Geography, Networks
- **Responses** - *'So what'* - Harms, Likely following events

While the description of the risk scenario under consideration can be tailored to use language appropriate to the organisation in scope and the stakeholders or experts that must consider it the underlying statement of the risk that scenario represents can, and should, be standardised using the Open Information Security Risk Universe.

3.3 Risk Statements

At it's simplest a risk scenario can be translated into a risk statement using the following structure:

There is a risk that <**source**> causes <**event**> occurs leading to <**outcome**> that causes <**consequence**>.

An example of a minimal risk statement structured as above is:

"*There is a risk that an employee accidentally emails data to an external recipient leading to an information breach that causes an accidental market sensitive information leak which results in regulatory fines.*"

"*There is a risk that an* ***employee accidentally*** *(<source>)* ***emails data to an external recipient*** *(<event>) leading to an* ***information breach*** *(<event>) that causes an* ***accidental market sensitive information leak*** *(<outcome>) which results in* ***regulatory fines*** *(<consequence>).*"

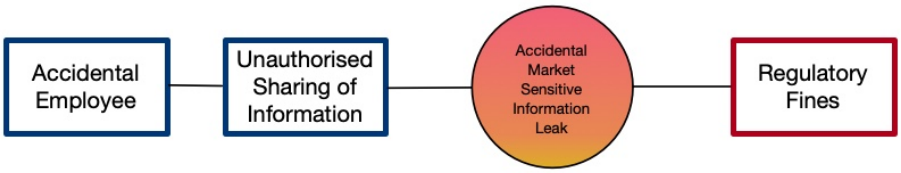
By ensuring that every risk scenario is also formally stated as a risk statement it allows comparison between scenarios as well as identifying what coverage of the OSIRU is currently being considered by the organisation and whether that is appropriate.

3.4 Bow-Tie Diagrams

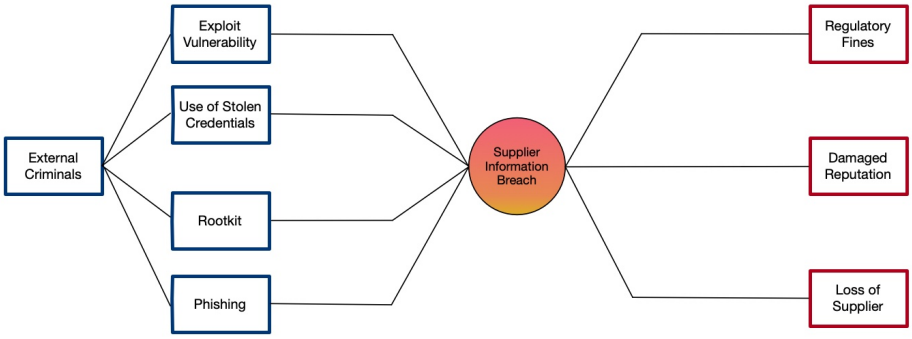
Bow-Tie diagrams can be a very useful way to visualise the components of a risk. A bow-tie diagram uses the risk as the 'knot' of the tie with two trees either side, the left hand tree is a fault tree showing the causal relationships that cause the risk and the right hand tree is an event tree showing the consequences of the risk.

A simple risk such as the example given above can be represented as follows:

<source> -> <event> -> <outcome> -> <consequence>

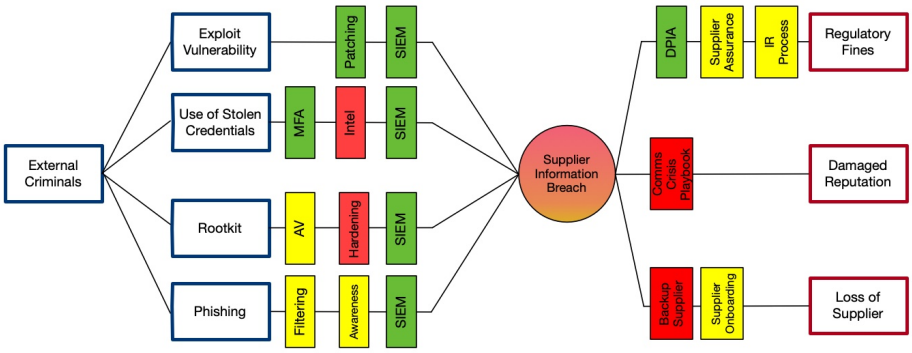


This is much simpler than most bow-tie diagrams, a more complicated example includes the following that shows many events and consequences:



The real value of a bow-tie diagram is in evaluating the available controls and mitigations. In this contect a control is a limiting factor that influences the fault tree on the left hand side whereas a mitigation is a limiting factor that influences the event tree on the right hand side.

The diagram below shows some example controls but the OSIRU is independent of control frameworks and as such to draw a bow-tie diagram such as this you would need to use both the OSIRU and your choice of control framework.



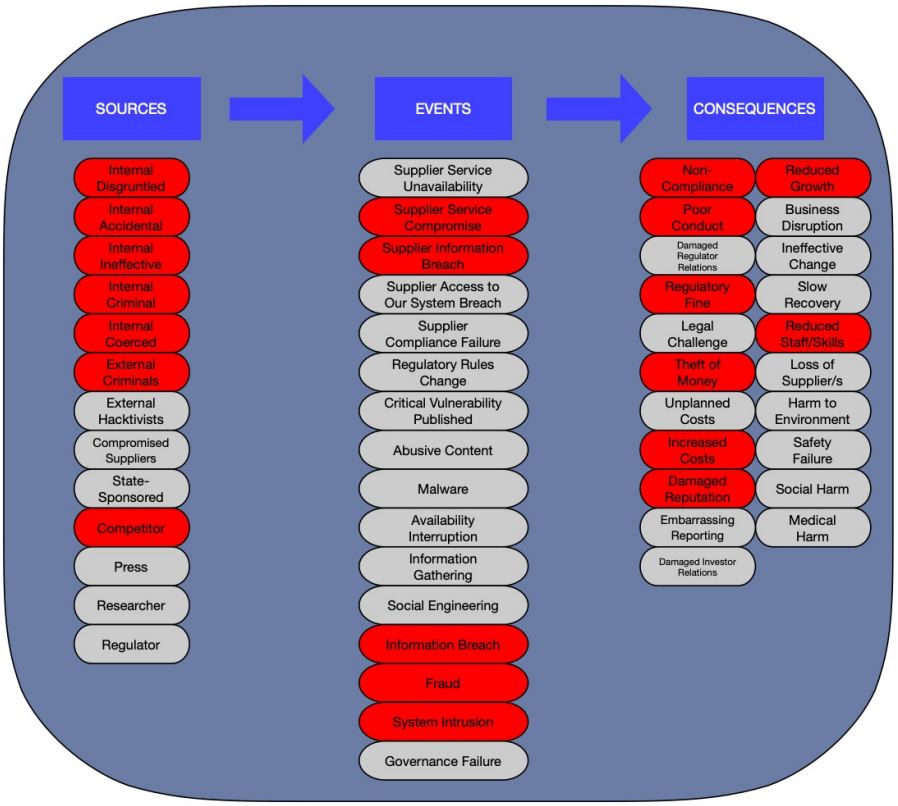
A bow-tie can be extended with concepts of frequency/likelihood, control/mitigation effectiveness and quantified consequences but these are beyond the scope of the OSIRU.

3.5 Risk Coverage

A key use of the OISRU is to check the coverage of existing identified risks to identify any gaps. It does not take long to translate an existing risk register into the OISRU taxonomy of
<source> -> <event> -> <consequence>
This then allows the contents of a risk register to be easily compared to the OISRU to see gaps.

Below is an example of translating the top ten security risks for a firm into the universe. Red components were referenced in an existing risk, grey components

were not referenced in an existing risk.



This allowed the CISO to confirm if he was comfortable with his choice of his top ten risks. In this example the CISO walked through the gaps and identified the lack of hacktivists as a source of risk and the lack of malware, especially ransomware, as a risk event both worthy of generating new risk scenarios, new risk statements and performing the analysis of their expected outcomes.

This sort of comparison is also useful for IT Auditors when they provide oversight of security risk processes and security risk registers as it provides a basis for challenge and communication with the security management team.

4 Sources of Risk

These are the various sources that cause a risk event to occur.

4.1 Internal vs External Sources

Internal sources are within the trust and control boundary of the organisation whereas External sources exist outside the trust and control boundary of the organisation.

4.2 Malicious vs Non-Malicious

Malicious sources are those with intent to cause harm whereas Non-Malicious sources do not have intent to cause harm.

Source	Internal/External	Malicious/Non-Malicious
Disgruntled	Internal	Malicious
Accidental	Internal	Non-Malicious
Ineffective	Internal	Non-Malicious
Criminal	Internal	Malicious
Coerced	Internal	Malicious
Criminals	External	Malicious
Hacktivists	External	Malicious
Compromised suppliers	External	Non-Malicious
State-Sponsored	External	Malicious
Competitor	External	Malicious
Press	External	Non-Malicious
Researcher	External	Non-Malicious
Regulator	External	Non-Malicious

4.3 Characteristics

It can be useful to consider characteristics of each source when analysing risks, the following charcteristics can be useful to bear in mind:

- **Goals** (Curiosity, Personal Fame, Personal Gain, National Interests, Revenge, etc)
- **Skills** (No technical skills, End user, Power user, Developer, Researcher)
- **Knowledge** (External to organisation, Ex-Organisation insider, Organisation partner, Customer, Employee, Other insider)
- **Opportunity** (Connected to Internet, Physically nearby, Access to connected partner, Access to organisation, Access to specific network / system)
- **Deterrability** (Unconcerned criminal, Careful criminal, Careless law-abiding, Careful law-abiding)

5 Frequency Risk Factors

Risk Factors are estimable values that are correlational but may not be directly causal to the risk. An increase in a risk factor may not directly drive an increase in the risk but is indicative of an increase of the risk and will be useful for better informing expert estimation of the overall risk. A positively correlated risk factor increases as the risk increases.

Frequency risk factors are relevant to the estimation of the frequency, or likelihood, by which a risk is expected to occur.

5.1 External Frequency Risk Factors

External Frequency Risk Factors are risk factors that are outside of your scope of control that may affect frequency of the risks you manage.

These are stated as questions to ask yourself or your organisation. The ability to estimate or measure these risk factors will vary between organisations.

- Will an attacker attack us?
- Will an attacker attack our supplier/s?
- Does an attacker have the ability to attack us?
- Are there any hacking campaigns targeting our sector?
- Are there any hacking campaigns targeting our geography?
- Are the tools / knowledge required to attack us readily available?
- Has there been any change in staff stressors (financial, emotional, medical, etc)?
- Have any of the suppliers we trust been compromised?
- How easy is it to impersonate our suppliers' staff or company?
- How aware of security are our suplliers' staff?
- How quickly do our suppliers patch their systems?
- Do our suppliers have effective governance of security?

5.2 Internal Frequency Risk Factors

Internal Frequency Risk Factors are risk factors that are within your scope of control and that may affect the frequency of the risks you manage. These are factors that can be subject to an internal control.

- Will an attacker be successful a exploiting a vulnerability?
- How many software or architecture flaws do we have in our code or systems?
- How many unpatched and unmitigated vulnerabilities are there in third-party software we rely upon?
- How quickly can we patch software flaws in our systems?
- How many unsupported systems do we operate?
- How many suppliers do we trust?
- How exposed are our systems to exploitation?

- How quickly does our movers and leavers processes, for our Identity & Access Management, operate?
- How aware of security are our staff?
- How easy is it to impersonate our staff or our company?
- How often do we assure the effectiveness of our security controls and processes?
- Can we detect changes in staff stressors (financial, emotional, medical etc) and intervene effectively?
- Do our security staff have appropriate training and skills?
- Do we have enough security staff to meet our needs?

6 Risk Events

Risk events are events that can occur and may cause consequences.

Risk events may lead to other risk events. For example a *software exploit* may lead to *unauthorised access to a system*.

We use a simple hierarchy to provide convenient groupings of events. We recommend using the framework at the appropriate level of granularity with regards to the risk scenarios being considered.

Indicative impacts on the information security goals of Confidentiality, Integrity and Availability have been added where appropriate.

6.1 External Risk Events

External Risk Events are events that may occur outside your scope of control but may still cause consequences for your organisation or it's stakeholders.

Level 1	Level2	CIA
Supplier	Service Unavailability	Availability
	Service Compromise	Confidentiality, Integrity
	Information Breach	Confidentiality
	Access to Our System Breach	Confidentiality, Integrity
	Compliance Failure	
Regulatory	Rules Change	
Research	Critical Vulnerability Published	

6.2 Internal Risk Events

Internal Risk Events are events that may occur within your scope of control and cause consequences for your organisation or it's stakeholders.

The Internal Risk Events are largely derived from this ENISA [PDF] review of CSIRT incident taxonomies across Europe.

Level 1	Level 2	CIA
Abusive Content	Harmful Speech	
	Child / Sexual / Violent Content	
	Harassment	
Malware	Ransomware	Availability
	Worm	Confidentiality, Integrity, Availability
	Spyware	Confidentiality

Level 1	Level 2	CIA
	Rootkit	Confidentiality, Integrity, Availability
	Dialler	
Availability Interruption	Distributed / Denial of Service	Availability
	Sabotage	Integrity, Availability
Information Gathering	Open Source Intelligence Analysis	Confidentiality
	Network Scanning	
	Network Sniffing	Confidentiality
Social Engineering	Lies	Confidentiality, Integrity
	Threats	Confidentiality, Integrity
	Phishing	Confidentiality, Integrity
	Bribes	Confidentiality, Integrity
Information Breach	Unathorised access to system / component	Confidentiality, Integrity
	Unauthorised access to information	Confidentiality
	Unauthorised sharing of information	Confidentiality
	Unauthorised modification of information	Integrity
	Unauthorised deletion of information	Integrity, Availability
Fraud	Misappropriation / misuse of resources	
	False representation	
	Theft of money	
System Intrusion	Software Exploit	Confidentiality, Integrity
	SQL injection	Confidentiality, Integrity
	Cross-site scripting (XSS)	Confidentiality, Integrity
	File Inclusion	Confidentiality, Integrity

Level 1	Level 2	CIA
	Control System Bypass	Confidentiality, Integrity
	Use of stolen credentials	Confidentiality, Integrity
	Password brute force	Confidentiality, Integrity
Governance Failure	Process failure	Confidentiality, Integrity
	Audit Failure	Confidentiality, Integrity

7 Severity Risk Factors

Severity risk factors are relevant to the estimation of therange and severity of consequences that a risk event may cause to occur.

7.1 External Severity Risk Factors

External Severity Risk Factors are risk factors that are outside of your scope of control that may affect the consequences of the risks you manage.

These are stated as questions to ask yourself or your organisation. The ability to estimate or measure these risk factors will vary between organisations.

- How much is the business worth?
- How many customers does the business have?
- What could be the level of fines we must pay?
- How much money will an attacker steal?
- What will be the cost for adverse legal action for negligence or liability?
- What would be the cost of reduced growth?
- What would be the cost of increased regulatory scrutiny?
- How much would customer notification cost?
- How much would customer rectification cost?
- Does our supplier have a documented & practised security incident response procedure?
- Does our supplier have a robust BC/DR capability?
- Does our supplier encrypt our data?

7.2 Internal Severity Risk Factors

Internal Severity Risk Factors are risk factors that are within your scope of control and that may affect the consequences of the risks you manage. These are factors that can be subject to an internal control.

- How long does it take us to detect financial crime?
- How long does it take us to detect security incidents from the initial attack stage?
- How long does it take us to resolve security incidents once detected?
- How much does it cost us to resolve security incidents?
- How often do we practice resolving breach scenarios?
- How many data records do we store?
- How long do we store data records for?
- How much money do we hold in our accounts?
- How much money can we access in our customers accounts?
- How many privileged user accounts do we operate?
- How much cyber insurance cover do we have?
- How long does our BC/DR process take to resume and restore normal operations following a crisis?
- Do we encrypt our data?

- How long does it take us to onboard or switch suppliers?

8 Consequences

Consequences are the possible harm resulting from a risk event occurring including loss, injury, or other adverse or unwelcome circumstance.

The use of Level 1 consequences is just a convenient grouping.

Level 1 Consequences	Level 2 Consequences
Operations	Reduced growth
	Business Disruption
	Ineffective Change
	Slow recovery
	Reduced access to staff / skills
	Loss of suppliers
	Environmental harm
	Safety failure
	Social harm
	Medical harm
Compliance	Non-compliance
	Poor conduct / integrity
	Damaged regulator relations
	Regulatory fines
	Legal challenge
Financial	Theft of money
	Unplanned costs
	increased costs / inefficiency
Strategic	Damaged reputation
	Embarrassing reporting
	Damaged investor relations