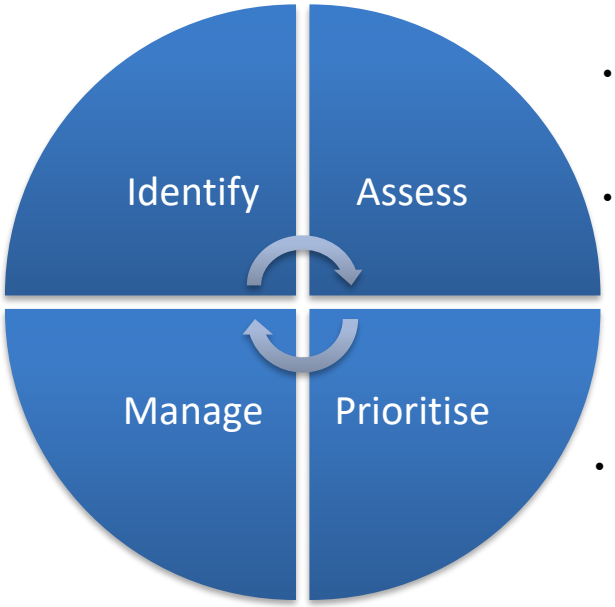
Risk analysis and assessment with RiskTree®

2T Security has developed RiskTree as a structured approach for risk analysis and assessment. Based around the well-established concept of attack trees, RiskTree provides a systematic way of capturing and prioritising the risks to your business and systems. It presents the results in an easy-to-understand format that integrates well with existing business processes, and facilitates effective risk management processes.

RiskTree is a business process that is supported by on-line, cloud-hosted software-as-a-service. This software allows the risks to be described and related in an attack tree structure and saved using a standard format. It then performs the risk analysis and prioritisation, and generates a sorted risk table for review. Countermeasures (also known as controls) can then be applied, and their effects viewed on both the tree and the risk table. For those organisations who need to transfer their risks into other software, data can be exported.

- *Facilitated workshops build RiskTrees, targeting particular types of attack.*



- *Business and technical staff assess factors relating to the risks.*
- *Threat information can be included in the assessment*
- *A risk assessment report is automatically created by the RiskTree software, including charts and tables of data. Recommendations can be embedded and the report customised to meet your requirements.*
- *The RiskTree software calculates the level for each risk and returns a prioritised list.*

RiskTree is being used by both the public and private sector, and is a tried and trusted method for information risk management. 2T Security provide training in both the process and the software, with the intent to leave our clients with the skills to manage their risks in-house, using the software.

A typical engagement will involve a few days of consultancy time (not necessarily in a single block), during which we will understand your requirements and train your staff in the process and the use of the software. This will involve 'train the trainer' style sessions, initially with us facilitating risk identification workshops. We will then hand over to your staff, and help them process the output into intelligible business information. We can continue to provide help and support if required after the end of the initial consultancy time.

Alternatively, we can provide the risk assessments as a service, in which we will facilitate the workshops with your staff, create the RiskTrees and run the assessments, and deliver a risk assessment report that provides a prioritised list of risks, cross-referenced with relevant countermeasures and if necessary, recommendations for work to mitigate the risks.

Key benefits

- Experienced consultants to train your staff in the process
- Workshop-based approach identifies risks using business language
- Saves time and money over other risk assessment approaches
- Browser-based software, with no plug-ins or browser extensions required
- Data can be exported in different formats, such as JSON, XML, and CSV
- Works effectively with agile methods for project delivery
- Strong security model means that no sensitive data are sent outside your network
- Link your Splunk environment with RiskTree for real-time reporting of risk levels directly into RiskTree using data from Splunk
- Map your countermeasures into built-in control sets, including ISO27001, MITRE® ATT&CK®, NIST 800-53, and the NCSC Cloud Security Principles and Cyber Assessment Framework (CAF).

Tried and trusted

RiskTree has been deployed by clients in both the public and private sectors. One client replaced their previous information risk management processes completely, and is already seeing the benefits of the RiskTree approach from better business engagement, end-to-end lifecycle support for security from projects, and more comprehensive risk registers – all leading to better assurance. The Cabinet Office has used RiskTree since 2017 to support the accreditation of the ResilienceDirect portal for the blue-light emergency services. The Home Office used RiskTree to assess the risk of transitioning a Police database from an on-premise Data Centre into a cloud-hosted platform.

Process overview

The RiskTree process starts with Risk Discovery Workshops. In these, system owners and technical staff describe the system and bad outcomes are identified – these are the aims of potential attackers, such as stealing data, committing fraud, or damaging the system. For each bad outcome, a RiskTree is built. This can be performed using the RiskTree software, in real time, or using a whiteboard or other mind-mapping software. The software allows evidence and justifications for the assessments to be captured to support the business decisions that need to be made, making it easy to revisit an assessment and understand the reasoning behind it. As well as considering malicious attacks, RiskTree also looks at accidents and natural hazards (e.g., flooding, fires, etc.).

Once the tree is complete, the workshop assesses each identified risk using a range of values. Any countermeasures that are in place are also factored in at this stage. The data are then compiled into the RiskTree software, and this creates a prioritised list of the risks. The list can be made for intrinsic risks (without any countermeasures), residual risks (with countermeasures in place), and for target risk reduction (which shows planned countermeasures, but also allows ‘what-if’ analysis of possible future

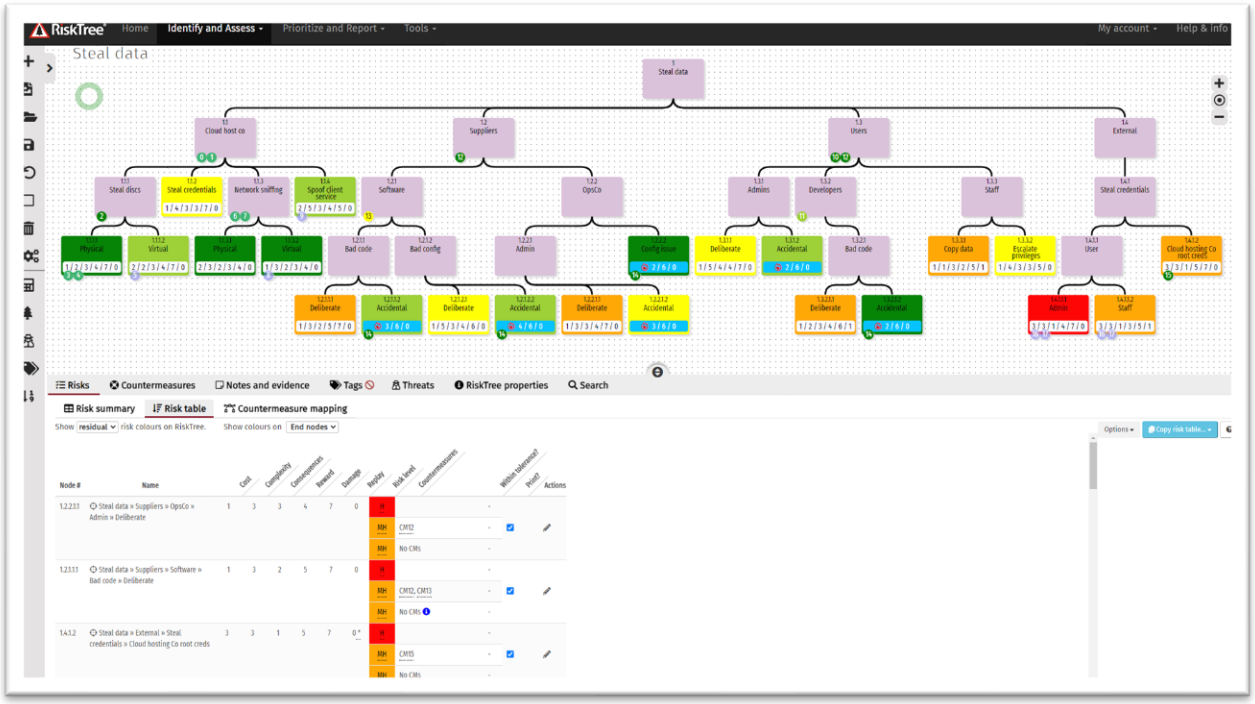
countermeasures). These views can make it easy to demonstrate the value that the countermeasures bring to the business.

One or more trees can be blended together to create a risk report. These can therefore show the risk across a complete system, or even across multiple systems. The reports include visualisations that allow the overall risk profile to be quickly assimilated.

Software

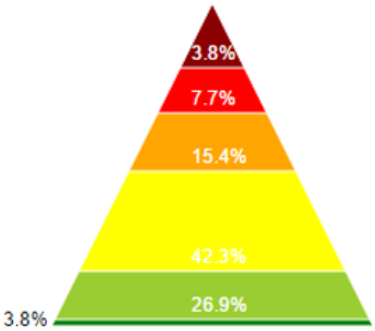
The RiskTree Designer software allows creation of the trees within the browser environment. This can be done during the workshops, or as a data-capture exercise afterwards. The tree is built quickly and efficiently, and can then be submitted to the on-line service for secure assessment.

The RiskTree Processor analyses the risk data and generates a prioritised table of risks. The default is that this is sorted on a traditional six-point scale (Very High – Very Low), but a configuration tool allows this to be customised.

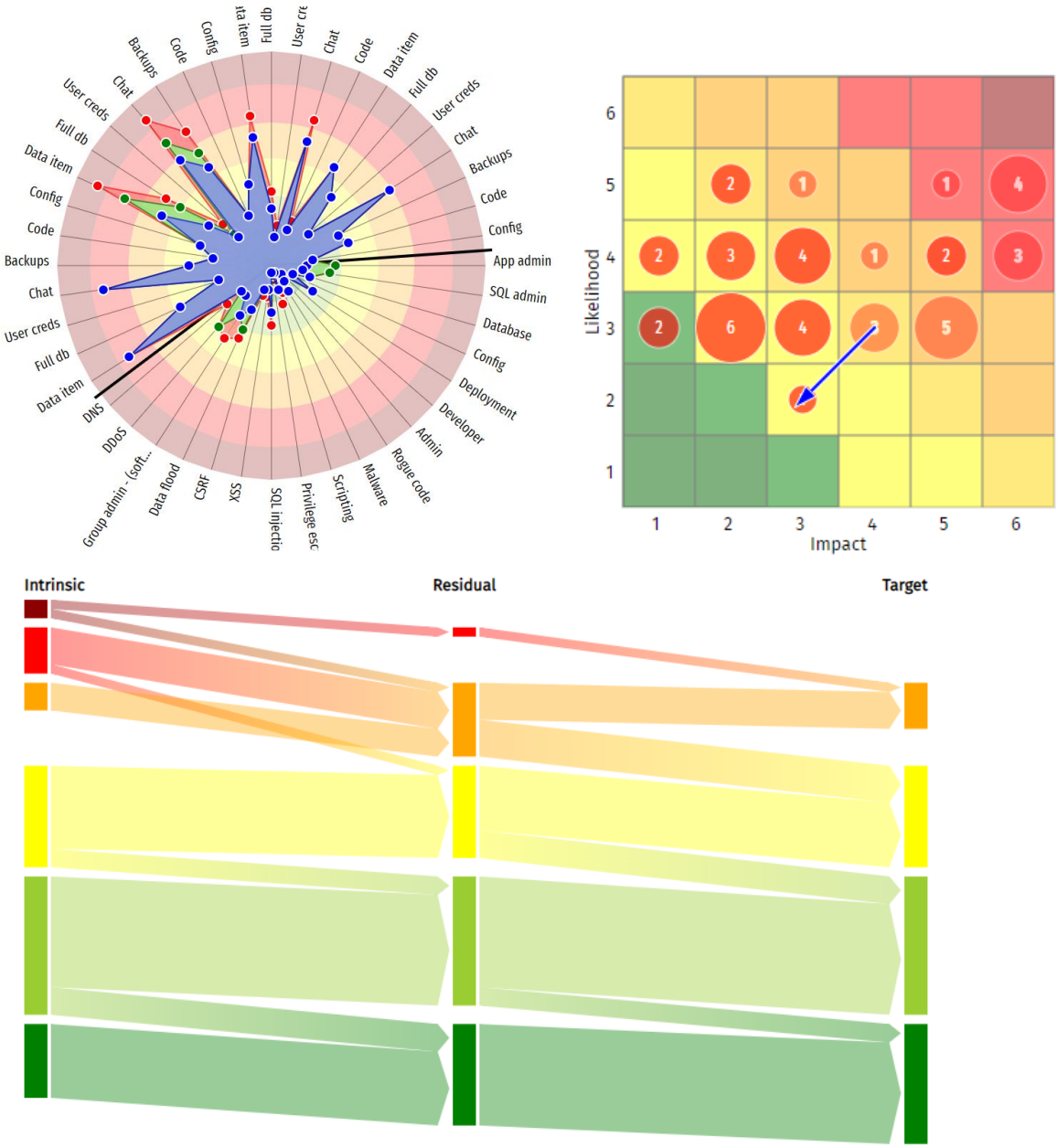


Name	Cost	Complexity	Consequences	Reward	Damage	Replay	Risk	Countermeasures
ALH - break system » External » DDoS	3	3	1	1	4	0	MH	
							MH	
ALH - break system » User » Data flood	1	1	3 (1)	1	1	2	MH	
							M	CM2
ALH - break system » Supplier staff » Delete » Data » App admin	1	1	4	1	3	0	M	
							M	
ALH - break system » Supplier staff » Delete » Data » SQL admin	1	3	3	1	3	0	M	
							M	

Notes and evidence for the assessment values can be captured during the workshops, and can easily be navigated through the RiskTree and data tables. Countermeasures can be added to the RiskTree, and their effect on risk mitigation assessed. Tags can also be added to the risks and countermeasures, allowing additional layers of metadata to be used. These have various applications, such as linking risks with tags for assets, tagging risks with their owners, or linking countermeasures with controls from control sets such as ISO27001.



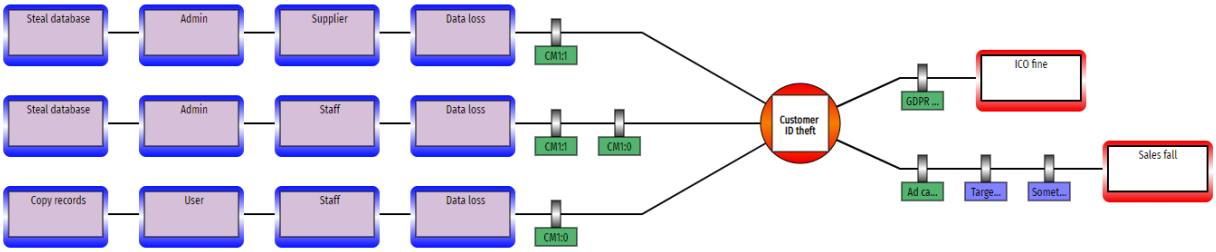
Charts showing risk levels are automatically created by the RiskTree Processor, and spider charts and Sankey diagrams give an immediate view of the level of risk reduction being provided by the countermeasures.



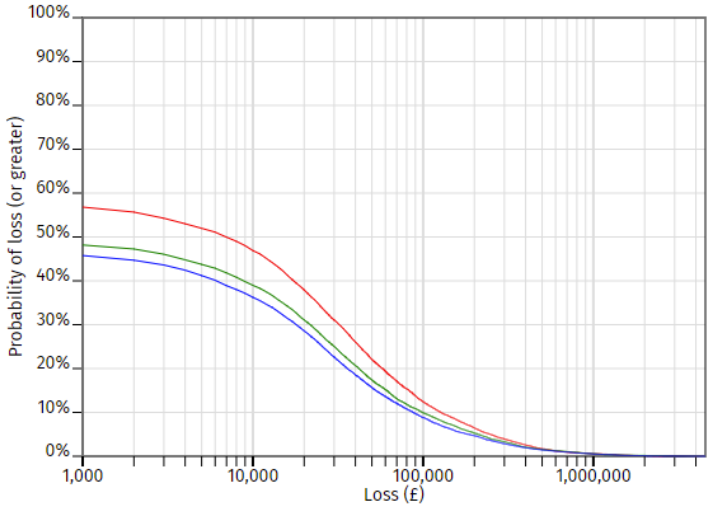
RiskTree Viewer accounts can be created for read-only access to RiskTrees, allowing the trees to be drawn and the risks and countermeasures examined, but without being able to edit or recalculate. These let the recipient examine RiskTrees in a more intuitive manner than a static report, but without incurring the cost of another user account. Viewer accounts are provided free to users of client organisations. This allows them to explore all of the information using the intuitive RiskTree interface, rather than struggling to cross-reference data in a static document.

Beyond attack trees

Once a RiskTree assessment report has been created, the data can be used to build bow-tie models. Unlike other bow-tie software, these can use the risk evaluation data to assess each bow-tie outcome in an intuitive and user-friendly view within the report.



RiskTree also supports quantitative risk analysis. Any or all risks can have quantitative information added, which are then used by a Monte Carlo simulation to produce a set of loss exceedance curves on a chart. These charts can be drawn for an individual risk, all risks within a bow-tie diagram, or all risks.



Requirements

The RiskTree software works on Chrome, Firefox, Safari, and Microsoft Edge browsers. JavaScript must be enabled, but no plug-ins or extensions are needed. It can be used on tablets, but some features will not work as well as on a conventional computer. It does not currently support smartphone use.

Assured Service Provider

in association with National Cyber Security Centre

Consultancy: Risk Management

NCSC Assured Service Provider

HM Government

Cyber Security Supplier to HM Government