How Idax Works

- March 2016 -

www.idaxsoftware.com

CONTENTS

idax

- Overall Approach
- Individual Risk Calculations
- High, Medium, Low – Individual risk
- Risk Weightings for assets
- Risk Calculations in combination
- Role Mining
- Review Generation

OVERALL APPROACH

idax

Idax calculates risk and identifies outliers by combining a number of different techniques:

1. Risk is calculated for a group of individuals that share a common meta-data classification– eg department, role, location.
2. That Risk is measured from 0 to 10 and is the degree to which those individuals differ from the most common set of access rights for individuals in that classification.
3. Risk is calculated across at least two of these classifications – usually department and role. This helps address the issue where a number of individuals in a single department all have similar but inappropriate access.
4. As part of this process, Idax determines the most usual set of access rights for individuals within a classification. These can either be used on their own, in combination with externally defined templates, or exported for validation and external use.
5. Idax also measures the risk for individual assignments in combination with all other access rights across the population. This identifies unusual access even when a number of staff within a classification all have similar access.
6. Idax uses several role mining techniques to identify groups of individuals with similar access, irrespective of meta-data classifications. This addresses the circumstance when several individuals in a single department all have similar but inappropriate access. It also enables automatic role definition where roles have not already been defined.
7. This analytics is achieved through unsupervised machine learning with no additional business context or data required, enabling fast and efficient analysis.

INDIVIDUAL RISK CALCULATIONS

idax

This example shows 6 staff, in a department. This risk calculation has been simplified for clarity, but shows how a template is defined and individuals measured against that to indicate department risk.

	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5	Asset 6	Asset 7	Asset 8	Asset 9	Asset 10	Missing Template Permission	Permission not in Template	Risk Rating (3)
Matthew Williams	Y									Y	3	1	5.0
Timothy Miller	Y	Y	Y	Y	Y	Y					-	2	4.7
Elizabeth Martinez	Y	Y							Y		2	1	3.9
Jeremy Davis	Y	Y	Y					Y			1	1	3.3
Harold Brown	Y	Y	Y	Y			Y				-	1	2.9
Douglas Powell	Y	Y	Y	Y							-	-	0.0
TOTAL (1)	6	5	4	3	1	1	1	1	1	1			
	In Template (2)				Not in Template								
Automatic Asset Wts	1.0	5.0	5.0	5.0	9.0	9.0	9.0	9.0	9.0	9.0			

1. Permissions for staff are aggregated, and based on distribution a department template is created.
2. Based on asset distribution across the organisation, automatic asset weightings are calculated. The more likely, the asset, the lower the weighting. Asset weightings can be uploaded to use external values.
3. Each individual is compared to the template and depending on how many assets they have that match the template, how many are not in the template and asset weights a risk metric is calculated.

HIGH, MEDIUM & LOW RISK

idax

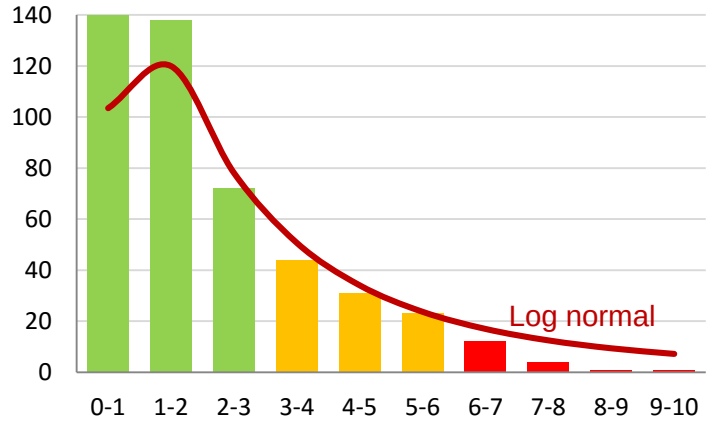
Idax risk for an individual is calculated on a continuous scale from 0 to 10. However, it is often useful to categorise risk into high, medium, and low. Reviews of data sets across multiple clients has indicated that a log normal distribution with mean of 0.8 and standard deviation of 1 is a close approximation to a "good" distribution. This results in:

- Low Risk - 0-3 risk rating, expected 65% of population
- Medium Risk - 3-6 risk rating, expected 25% of population
- High Risk - 6-10 risk rating, expected 10% of population

In the examples below, (a) shows a distribution that is better than log normal, whilst (b) has more high risk individuals than expected, and therefore requires more attention.

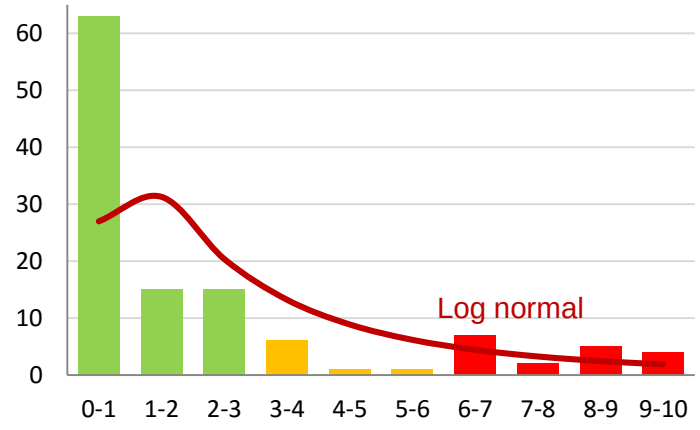
(a)

	Staff	Actual	Expected
Low	350	75%	66%
Medium	98	21%	24%
High	18	4%	10%



(b)

	Staff	Actual	Expected
Low	93	78%	66%
Medium	8	7%	24%
High	18	15%	10%



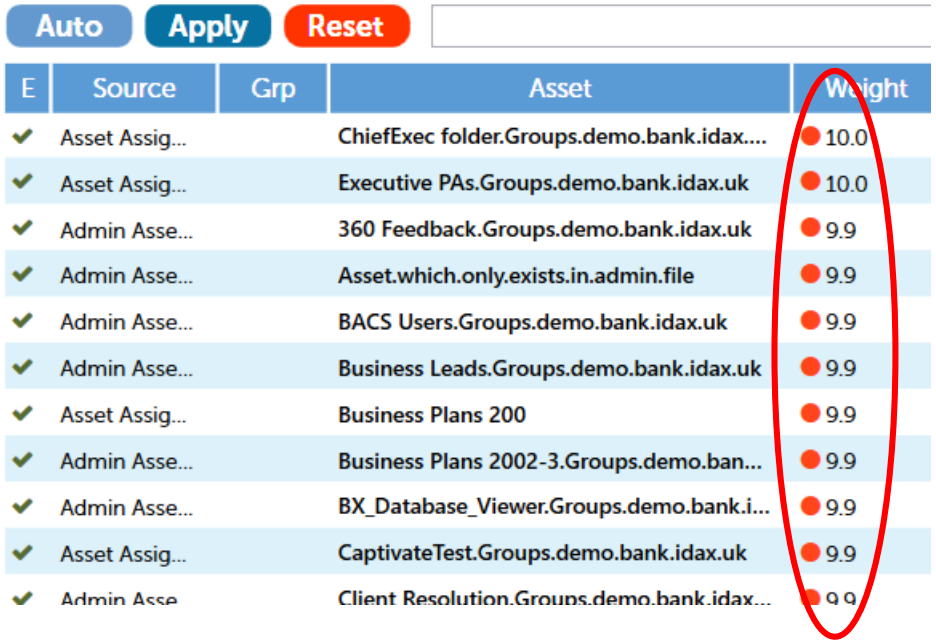
RISK RATINGS FOR ASSETS

idax

An individual "asset" is an entitlement, access right or collection of entitlements and has a weighting from 0 to 10. Weightings can either be automatically calculated by idax, based on distribution, manually uploaded, or a combination of the two.

The expectation is that significant assets, such as SOX have a higher weighting than all other assets. Each weighting can be:

- Provided from an external source
- Manually overridden
- Automatically calculated
- A combination of all methods



AUTOMATIC WEIGHTINGS

The automatic weighting calculation uses the distribution of entitlements to that asset across the whole population to determine the weighting.

If an asset is widely available and those that have it have little else in common, then it has a low weighting. If few people have it but they also have little else in common it is highly weighted.

This is particularly useful in determining the set of assets that are of less concern.

RISK CALCULATIONS IN COMBINATION

In some cases risk measured across only one classification has an inherent weakness. For example, when individuals in a single department all have similar but inappropriate access, or as below, where an individual is the only person in a department.

Idax addresses this by looking at risk across multiple dimensions and for individual access rights within an individuals permissions.

Individuals ☑ Ignore with no Assets

A	Individual	Manager	Role	Department	Role Risk	Dept Risk
	Richard Collins	Lauren Davis	Trade Support Analyst	2 Lawyers	4.0	0.0

Asset	Asset Wt	Ind	Role	Dept	#All	#Role	#Dept
In Role or Dept 9 Assets							
GPN group.Groups.demo.bank.idax.uk	7.7	✔	✖	✔	7	1/4	1/1
Corporate Secretariat.Groups.demo.bank.idax.uk	7.3	✔	✖	✔	14	1/4	1/1
Preference Team.Groups.demo.bank.idax.uk	7.0	✔	✖	✔	14	1/4	1/1
London Office.Groups.demo.bank.idax.uk	6.8	✔	✖	✔	13	1/4	1/1
IDXBNK_TEMPLATES_CRM_ALL_DATA_R.Groups.demo.b...	5.8	✔	✖	✔	28	1/4	1/1
IDXBNK_BMW.Groups.demo.bank.idax.uk	3.4	✔	✖	✔	62	1/4	1/1
All at Fifth Floor.Groups.demo.bank.idax.uk	2.8	✔	✖	✔	60	1/4	1/1
CRM.Groups.demo.bank.idax.uk	1.5	✔	✖	✔	73	1/4	1/1
ActiveSync Users.Groups.demo.bank.idax.uk	1.2	✔	✖	✔	74	1/4	1/1
In Role and Dept 11 Assets							
Analysts Virtual Team2.Groups.demo.bank.idax.uk	6.6	✔	✔	✔	27	2/4	1/1
Analyst Users Group.Groups.demo.bank.idax.uk	6.4	✔	✔	✔	33	2/4	1/1

Richard is the only member of the Lawyers department, so his dept risk is 0, but his Role Risk is 4.0, and should be reviewed.

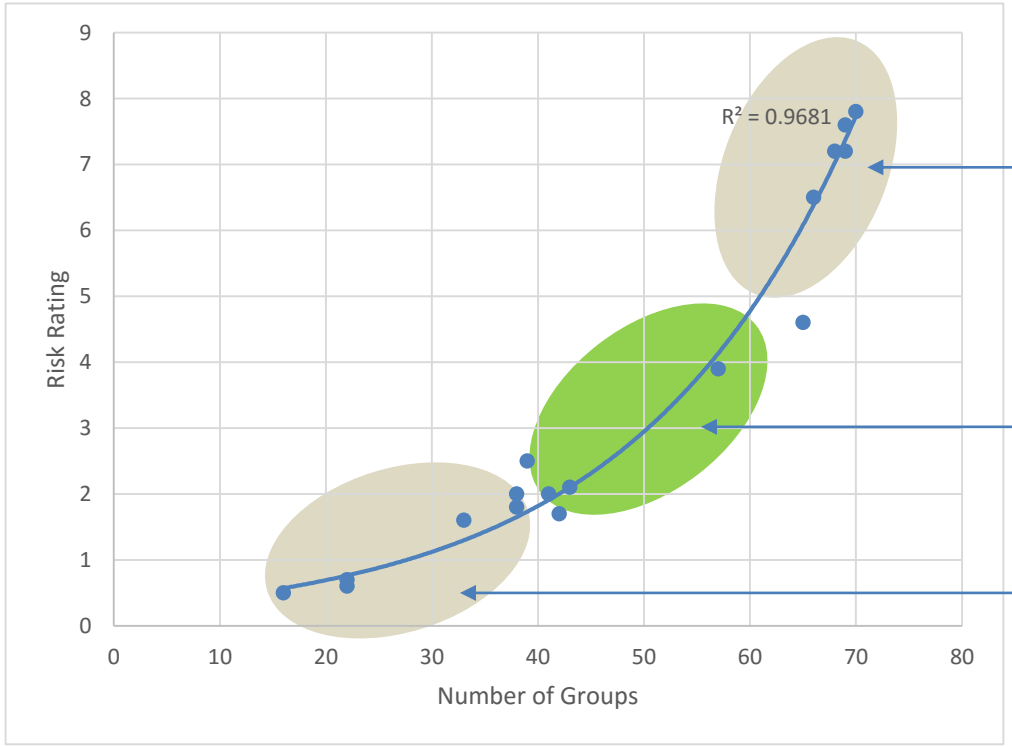
When we look at his detail, we can see that he has a number of rights that are unusual across his role showing as 1 in 4.

ROLE MINING

In addition to comparisons within existing classifications (department, role) Idax has the ability to mine roles within a set of individuals or whole populations. Idax uses a number of techniques to group individuals with similar access and to optimize risk differentiation.

This is particularly useful where roles for Role Based Access have not already been defined, or where roles that have been defined are not optimized for identifying risk.

Idax algorithms identify the optimum groupings to maximise differentiation and identify unusual patterns of access,



Too many high risk

Optimum for differentiating risk

Too many low risk

RISK BASED REVIEWS - 1

The Review recommendation process has a number of steps:

1. A threshold is entered by when the review is set up, above which individuals are reviewed. In the example below, staff above 4.0 are reviewed. The proposal is that 100% of staff are reviewed initially.
2. High/ Medium/ Low thresholds are set manually that drive the decision matrix in the next step. These can be set based on either automatic or manual asset weightings.

RISK BASED REVIEWS - 2

3. Then based on the decision matrix a recommendation is derived. The decision matrix identifies – does an individual have the right; is it in their Department profile and is it in their Role profile
4. Based on the outcome of the decision matrix the recommendation is to either "Allow", "Refer", "Remove" or "Add". All the recommendations are configurable based on how the review is to be set up

Decision Matrix

Individual	Department	Role	High		Medium		Low	
✓	✓	✓	2384	Allow	19047	Allow	19286	Allow
✓	✓	✗	0	Refer	0	Refer	0	Allow
✓	✗	✓	0	Refer	0	Refer	0	Refer
✓	✗	✗	14396	Remove	25791	Remove	11099	Remove
✗	✓	✓	3503	Add	21301	Add	17586	Add
✗	✓	✗	0	-	0	-	0	-
✗	✗	✓	0	-	0	-	0	-
✗	✗	✗	141065	-	201809	-	79655	-

The future of managing identity access risk

www.idaxsoftware.com