GETVISIBILITY

Data Risk Score Assessment & Control

A unified view of your data landscape;

Knowing your organisation's data, understanding your organisation's risk, and measuring how risk changes over time is the foundation to any effective security strategy

Empowering
Data Risk Visibility

- Getvisibility's risk measurement framework helps to unify the organisation with multi-layer reporting, appropriate to each user using a risk score

- Getvisibility has created a risk score to empower everybody in the organisation through comprehensive, actionable reports

- The Getvisibility risk score enables key decision makers to quickly make informed budgeting and strategic decisions. This allows for the effective measurement of these decisions and policies while informing long term strategic goals

What is Data at Risk

The Data Challenge

Organisations have enormous quantities of data stored in diverse locations. Almost every organisation has files that contain sensitive or regulated data.

Most organisations have no idea what their data footprint looks like and are creating significantly more data and risk on a daily basis.

Active Directory

48% of employees have access to more company data than they need to perform their jobs

Sensitive & Regulated

61% of companies have over 5,000 stale sensitive files

ROT & Duplicate Data

85% of companies have over 100,000 folders containing stale data

Data Risk Factors

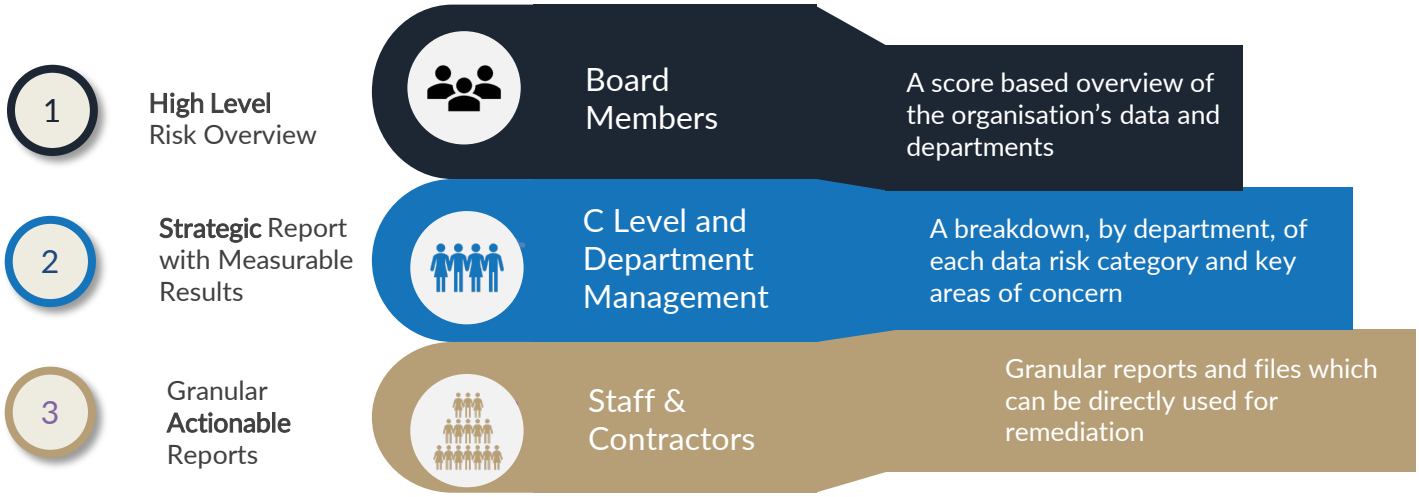
Organisations struggle to comply with strict data regulations and are under growing pressure due to a sharp rise in cyber attacks and data breaches.
The three main data risk factors for organisations are:

- Active Directory- Maintaining strict access control measures is difficult and without data classification, its extremely difficult to enforce
- Sensitive and Regulated Data –With new data protection laws, many organisations are struggling to grasp what regulated information they contain, and how to manage this information
- ROT and Duplicate Data – The more data stored, the higher the vulnerability to hacks, insider threat, and human error. Maintaining control over unnecessary data is imperative for reducing data security risks

GETVISIBILITY

Multi-Layer Reporting

The Getvisibility risk score enables key decision makers to quickly make informed budgeting, operational, tactical, and strategic decisions. It also allows key decision makers to measure the effectiveness of their teams and budgetary decisions, providing a framework for continuous learning and improvement.



The risk score is a powerful tool for risk and security practitioners. CISOs, DPOs, and security experts now have a bench-marked mechanism for demonstrating good practice, as well as the consequences of under investment.

The Getvisibility remediation tools provide the solutions for managing and improving the data risk scores.

Data Risk Assessment and Scoring

Getvisibility's Data Risk Assessment Report takes a holistic approach when assessing your organisations data vulnerabilities.

This risk score measures your data protection posture by taking into account: data type, location, context, who has access, protections in place, relevant regulations, and company processes. You will be given an overall risk score, as well as broken down scores per department and vulnerability type, allowing for clear and immediate remediation.

Information Stored

Getvisibility will give a clear view of what information is stored, where it is located, and how sensitive the data is.

Users and Permissions

A risk score based on the correlation between: access rights, data sensitivity level, volume, and context. organisations will be enabled to take immediate action to reduce this risk through permission changes, group deletion, and stale account deletion.

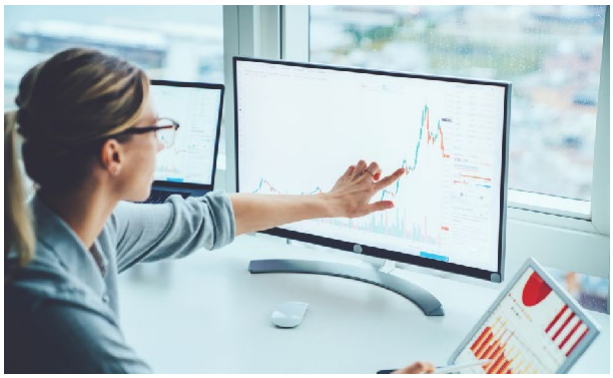
Laws, Regulations, Standards

A risk score assesses how the current data protection posture aligns to the relevant industry laws, regulations and standards.

Protections and Processes

A risk score for processes in place when creating, storing, and sharing sensitive data. Measures the implementation effectiveness of theses processes.

Data Risk Scoring Explained



Aggregated Risk Score

The Getvisibility Scan and Data Risk Assessment compiles the information from various sources and arrives at an aggregated overall risk score, giving an overview of the current data risk posture. The lower the score the lower the risk, the higher the score the higher the risk. An overview report is generated giving a high level view of the current risk status in key categories.

Actionable Results

Strategic Reporting

For key stakeholders and management to aid in strategic decision making and budget allocation. The reports contain key risk factors, broken down by department / location and arranged by risk category giving detailed information on what the high and low risk areas are and where to allocate remediation resources.

Tactical Reporting

A key component of the Data Risk Assessment as they allow for action and remediation. These reports give granular details, exportable CSVs etc to allow for quick and accurate remediation.

0-3

Low Risk – Low level of vulnerability, maintenance of current measures recommended

4-6

Medium Risk – Elevated risk, remediation action recommended

7-10

High Risk – Critical risk level, urgent action recommended

GETVISIBILITY

Understanding Your Scores

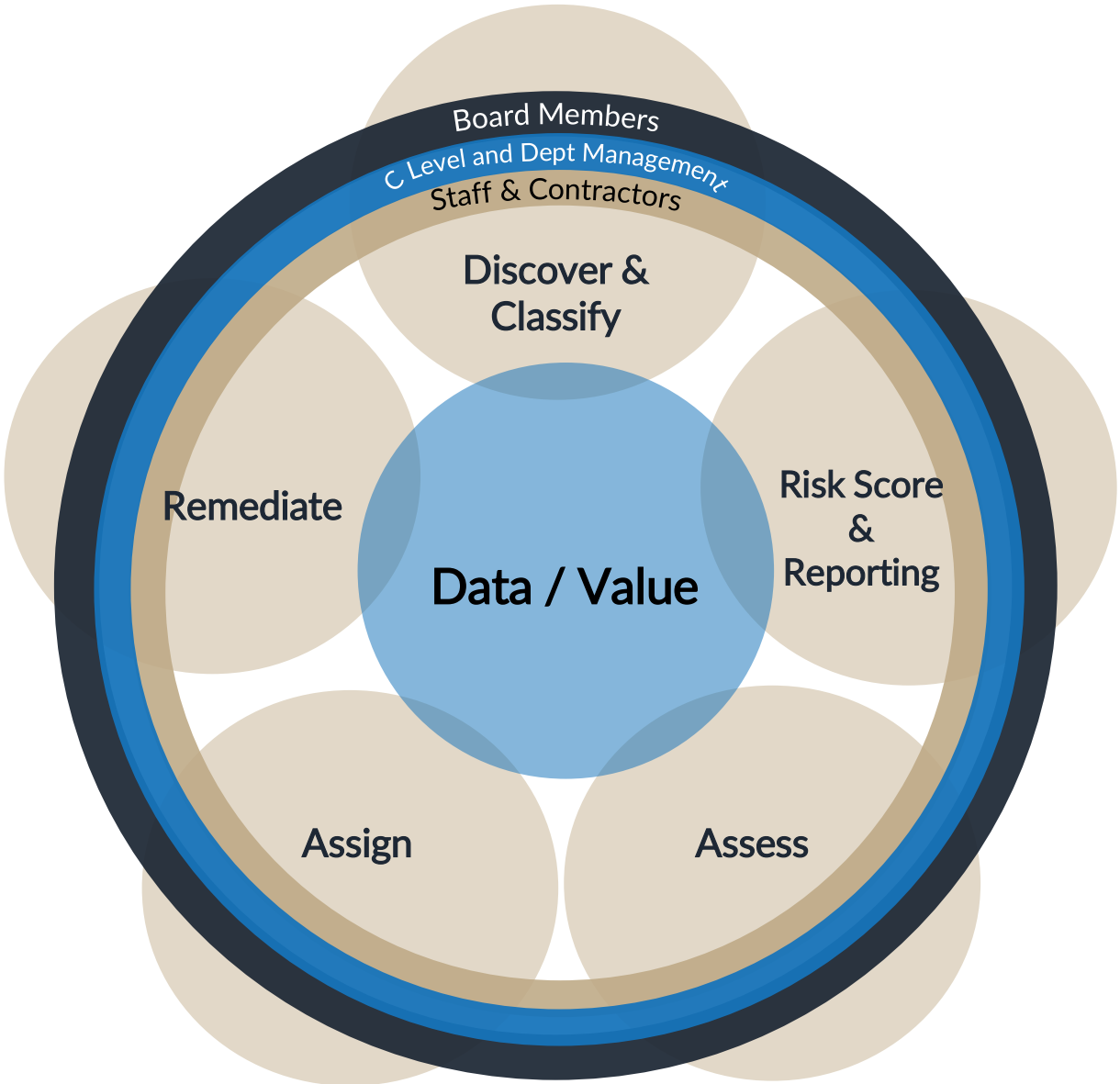
Data Risk Score	This measures the likelihood of a data breach and the relative damage to a company's reputation, finances, and legal standing were such an event to occur
Content Risk Score	Measures the amount of critical information contained in the company's files and its vulnerability to exposure
Dynamic Risk Score	Measures the rate of change in the creation of sensitive and regulated data over time
Endpoint Risk Score	Measures the distribution of sensitive and regulated data between devices and shares on a network
Access Risk Score	Measures the vulnerability of sensitive and regulated data to unauthorised access
Audit Risk Score	Measures the attack surface of a company's system. Based on the results of consultation with Getvisibility

GETVISIBILITY

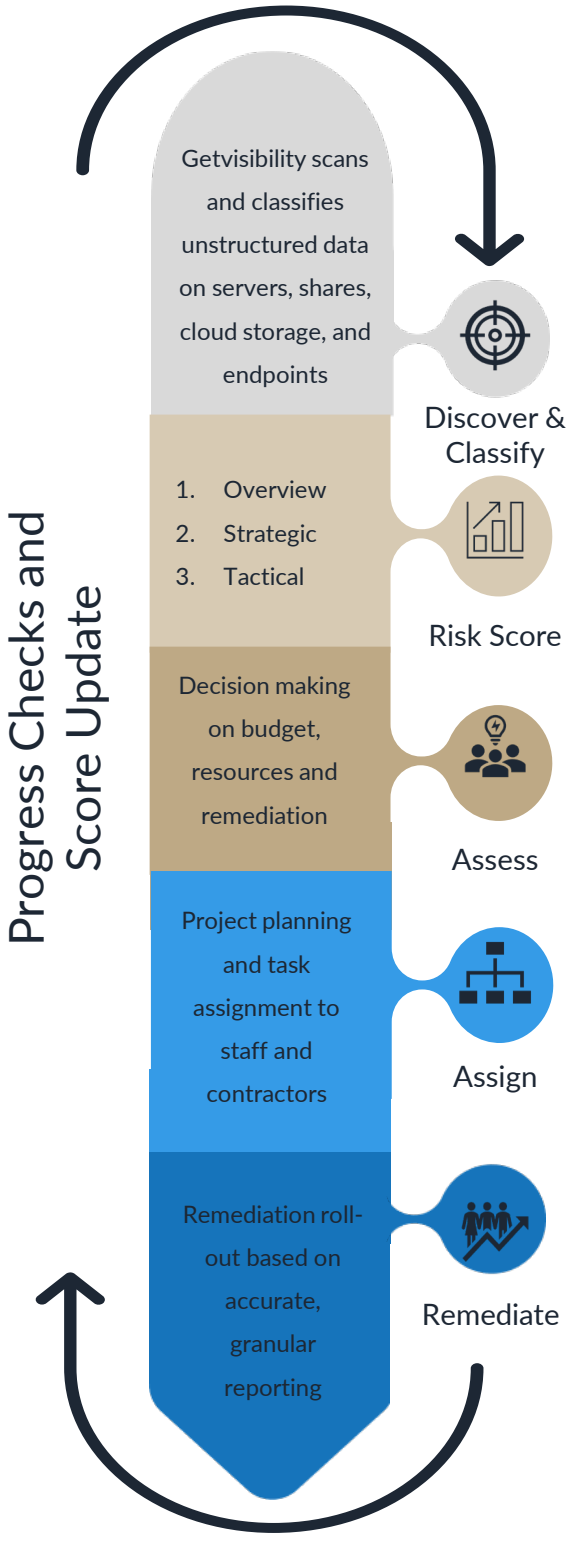
Data Protection and Score Review

A Key Business Process

Recurring Data Risk Assessment Reporting allows organisations to measure the compliance and effectiveness of implemented changes and remediation while monitoring their maintenance; driving further initiatives and policies.



Data Protection and Score Review



Getvisibility Remediation

Secure Deletion and Archiving

Once ROT and duplication has been identified and verified, organisations can encrypt and archive anything they choose to keep. Securely delete the remainder, reducing the level of sensitive information held, automatically with Getvisibility.

Data Security and Processes

Through additional scanning and reporting, Getvisibility can measure the updated security posture of the organisation and effectiveness of its processes.

Active Directory Redemption

Active Directory Risk reporting, enables the appropriate team to reduce risk regarding file access through policies such as: permission management, inactive user and group deletion, global access restrictions, user reviews, and domain admin deletions.

Rescan and Update Score

Scoring updates can be a valuable tool to boost and maintain morale and enthusiasm in relation to data security within the organisation at all levels. It is also a vital tool to monitor compliance and change strategy when needed.

Getvisibility Solutions

Data Hygiene Engine

The Getvisibility Data Hygiene Engine reduces data risk scores through a series of data reduction and clean-up actions. Strategic data hygiene reports enable management to assign data clean-up tasks which can then be actioned through granular tactical reporting. Tasks supported by these reports include

- Mislocated file clean-up
- De-duplication
- ROT file remediation
- Data visual labelling
- Data tagging
- Data archiving

Data Security Engine

The Getvisibility Data Security Engine integrates with existing platforms and provides data security measures to protect your data, thus reducing your risk score. Accurate discovery and classification of data through Getvisibility, allows data security platforms such as DLP and encryption to become more finely tuned and extremely effective.

Data Governance Engine

The Getvisibility Governance Engine allows organisations to reduce their risk score through granular reports and features, informed by data protection regulations and industry standards. Recurring risk reports and scheduled governance reports allow for the review of policies and procedures facilitating strategic decision making.

Sample Report Results

Data Risk Score

This score represents the overall risk an organisation's sensitive & regulated (critical) data, users, software, and policies present to the occurrence of a data breach. After scanning and assessing the selected file servers and user access, this overall score represents an aggregation of data risk across the organisation.

Data Risk Scores per Share

The individual scores that affected the data risk score for each share are also shown.

Key Data Risk Scores for: User_Documentation

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Critical Files
- 8 Duplicate Critical Files

Key Data Risk Scores for: HR

Data Risk Score

- 8 Critical Files
- 8 Critical Stale Files
- 7 Outdated Paswords

Key Data Risk Scores for: Comp_01

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Duplicate Critical Files
- 8 Critical Files

Key Data Risk Scores for Share_5

Data Risk Score

- 7 Outdated Passwords
- 7 Duplicate Critical Files
- 6 Enabled Inactive Users

Key Data Risk Scores for XD-120

Data Risk Score

- 7 Outdated Passwords
- 6 Enabled Inactive Users
- 6 Critical Files

Key Data Risk Scores for Processes

Data Risk Score

- 8 Critical Files
- 7 Outdated Passwords
- 6 Critical Stale Files

Key Data Risk Scores for Finance

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Duplicate Critical Files
- 8 Critical Files

Key Data Risk Scores for IT

Data Risk Score

- 7 Outdated Passwords
- 7 Duplicate Critical Files
- 6 Enabled Inactive Users

Sample Report Results

This score means that the content of the unstructured data on your network will cause financial, legal, or reputational damage if a breach were to occur. Critical (sensitive & regulated) data contains information that affects this damage. Steps to remediate these issues can be found in one of our more detailed reports.

Content Risk Score 8

Critical Files

- 145,945 classified files
- 75,813 critical files
- 74% of classified files are critical
- Remediation includes: Encryption software, monitoring software, classification policies

Critical Files in Everyone Group

- The Everyone Group (EG) includes all users in the network
- 85,813 critical files
- 25,744 accessible to EG
- 21% of critical files can be accessed by EG

Duplicate Critical Files

- Duplicate files contain the exact same information
- 59,242 duplicate files
- 18,938 critical duplicate files
- 59% of duplicate files are critical
- Remediation includes: file creation policies, monitoring software

Critical Stale Files

- Stale files have not been accessed in more than 6 months
- 21,149 stale files
- 8,264 critical stale files
- 34% of stale files are critical
- Remediation includes: : file creation policies, monitoring software

Highly-accessible Critical Files

- Critical files that can be accessed by the majority of users
- 85,813 critical files
- 0 highly accessible critical files
- 0% of critical files are highly accessible

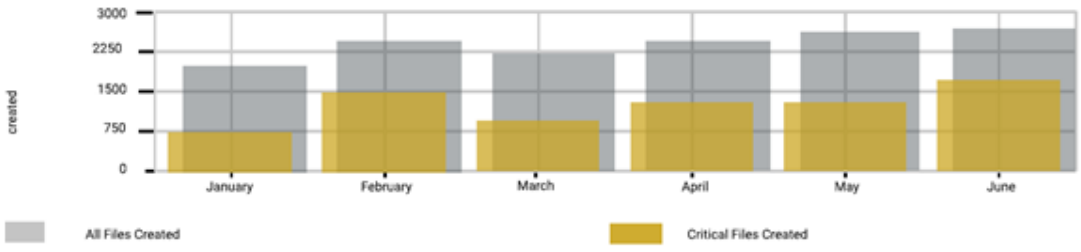
Critical Files available to Inactive Users

- Inactive Users (UI) are those that have not logged-in in more than 90 days
- 6,030 files accessible to inactive users
- 2,591 critical files accessible to inactive users
- 42% of S&R files can be accessed by Inactive groups

This score charts the creation of sensitive and regulsted files over time. While their creation is not a risk in itself, the rates that they are created may be indicitive of policy or security issues

Dynamic Risk Score 6

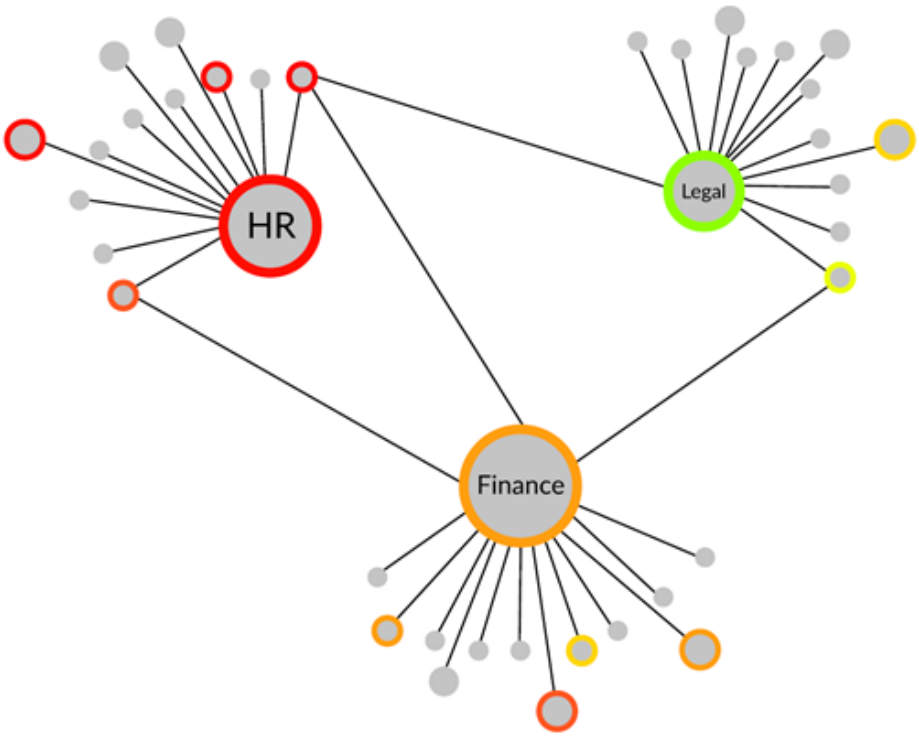
All & critical files created in the last 6 months



Sample Report Results

Getvisibility scans the endpoint devices on your company network and assesses the numbers of sensitve and regulated files that each device contains. Having these files distributed broadly increases the attack surface and risk of data exposure.

Endpoint Risk Score 7



Devices with the most critical data

Critical Files	Device ID
6,457	HR_03
6,325	HR_46
6,267	HR_25
5,234	FIN_05
4,756	FIN_62
3,895	FIN_35

The **Network Graph** shows the distribution of sensitive & regulated files persisted on devices and shares on the company network.

The coloured nodes indicate that a high percentage of sensitive & regulated files are stored in the device.

Edges represent access rights. They are not weighted.

Sample Report Results

This score assesses the file access permissions of the users on the network and the vulnerability that these permission settings represent to the critical data on the file share scanned.
A list of permission changes and additional remediation steps are available in the more detailed reports.

Access Risk Score 

Critical Files in Everyone Group

- The Everyone Group (EG) includes all users in the network
- 47 critical files
- 0 accessible to EG
- 0% of critical files can be accessed by EG

Enabled Inactive Users

- Inactive uers still retain privileges
- 123 enabled users have been inactive for 100 days or more
- 19% of users are enabled inactive users

Critical Files available to Inactive Users

- Inactive Users (UI) are those that have not logged-in in more than 90 days
- 234 files accessible to inactive users
- 124 critical files accessible to inactive users
- 0% of S&R files can be accessed by Inactive groups

Outdated Passwords

- Passwords that are not changed frequently
- 199 users have outdated passwords
- 35% of passwords have not been changed in more than 100 days

Highly-accessible Critical Files

- Critical files that can be accessed by the majority of users
- 49 critical files
- 0 highly accessible critical files
- 0% of critical files are highly accessible

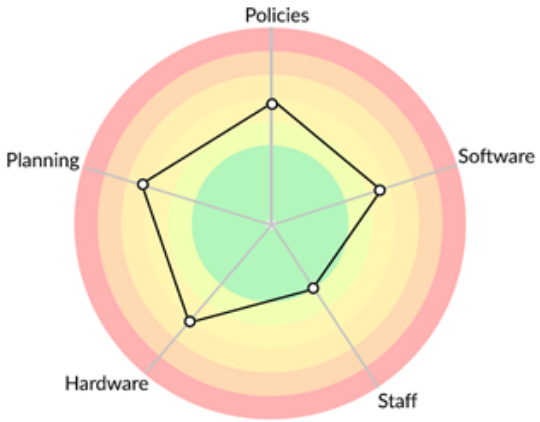
Domain Administrators

- Domain administrators are not Active Directory administrators but may have the same privilages
- 10 users have Domain Administrator privileges
- 0.18% of Active Directory accounts are Domain Administrators

Sample Report Results

The data risk survey conducted by Getvisibility gathers information about the technologies, policies, and resources of your company.
The extent and usage of software and policies is evaluated to calculate the score.

Audit Risk Score 6



A Getvisibility representative assesses each of these metrics and scores them according threat level and risk.

The **radial chart** represents the attack surface of the company s critical information. A larger area inside the lines represents a greater risk to the company s data integrity.

Steps to improve this score include: increasing policy adherence, implementing data breach planning, and identifying critical data throughout the organisation.

Scan Statistics

Statistic	Value
File Found	681,354
Shares Found	17
Shares Assessed for Data Risk	8
Total Data Size	12.68TB
Mean File Size	24MB
Median File Size	287KB
Total Users	1,098
Number of AD Groups	235
Most Numerous File Category	Technical Documents
Most Numerous File Subcategory	Configuration

Detailed Scores Table

Score	E	Computational	Users	IT	4D-110	Process Sciences
Critical Files	7.87	8.28	8.13	5.39	5.82	7.54
Duplicate Critical Files	7.76	5.23	7.23	7.35	2.43	2.78
Critical Stale Files	7.09	8.10	6.26	5.34	2.38	5.86
Critical Files in Everypone Group	8.28	1.23	1.23	1.23	1.23	1.23
Critical files accessible to Inactive Users	8.71	-	8.65	1.23	-	-
Highly Accessible Critical Files	2.94	2.84	3.84	3.84	1.94	1.84
Domain Administrators	2.52	2.52	2.52	2.52	2.52	2.52
Outdated Passwords	6.82	6.82	6.82	6.82	6.82	6.82
Enabled Inactive Users	5.23	5.03	5.75	5.25	5.95	5.95

Information based on disclosed file server(s) scanned.

The preceding information and analysis was compiled using Getvisibility's Data Risk Model Version 1.0.0.

Information based on disclosed file server(s) scanned.
Classified using Getvisibility's generic machine learning model.
Modifications based on customer specific data are not included, but can be added during future engagments.

The preceding information and analysis was compiled using Getvisibility's Data Risk Model Version 1.0.0.

GETVISIBILITY DATA RISK ASSESSMENT