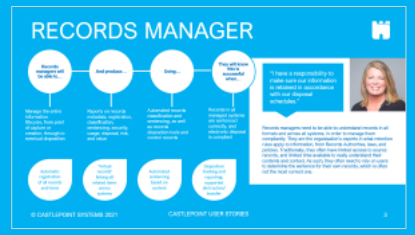
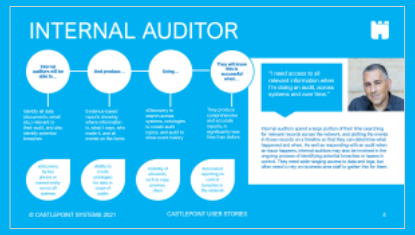
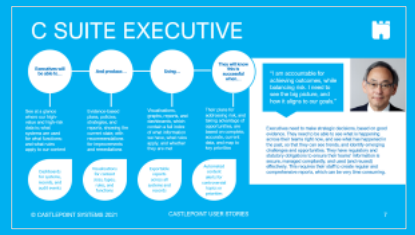
CASTLEPOINT

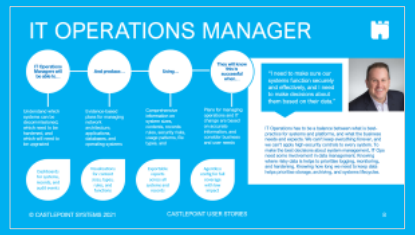
USER STORIES

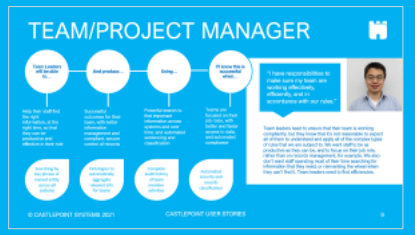
OVERVIEW











This document shows some example user stories for different kinds of business user. It shows the goals, outcomes, and capabilities for each user type, and their organisational and operational context.

These user stories provide a picture of the challenges each type of user encounters, the opportunities they have, and how Castlepoint can help to address them.

RECORDS MANAGER

Records managers will be able to…

Manage the entire information lifecycle, from point of capture or creation, through to eventual disposition

And produce…

Reports on records metadata, registration, classification, sentencing, security, usage, disposal, risk, and value

Using…

Automated records classification and sentencing, as well as records disposition tools and control records

They will know this is successful when…

Records in all managed systems are sentenced correctly, and electronic disposal is compliant

Automatic registration of all records and items

'Virtual records' linking all related items across systems

Automated sentencing based on content

Disposition tracking and reporting; supported destruction/ transfer

"I have a responsibility to make sure our information is retained in accordance with our disposal schedules."

Records managers need to be able to understand records in all formats and across all systems, in order to manage them compliantly. They are the organisation's experts in what retention rules apply to information, from Records Authorities, laws, and policies. Traditionally, they often have limited access to source records, and limited time available to really understand their contents and context. As such, they often need to rely on users to determine the sentence for their own records, which is often not the most correct one.

INTERNAL AUDITOR

Internal auditors will be able to…

Identify all data (documents, email etc.) relevant to their audit, and also identify potential breaches

And produce…

Evidence-based reports showing where information is, what it says, who made it, and all events on the items

Using…

eDiscovery to search across systems, ontologies to curate audit topics, and audit to show event history

They will know this is successful when…

They produce comprehensive and accurate reports, in significantly less time than before

eDiscovery by key phrase or named entity across all systems

Ability to create ontologies for data in scope of audits

Visibility of all events, such as copy, preview, share

Automated reporting on control breaches in the network

"I need access to all relevant information when I'm doing an audit, across systems and over time."

Internal auditors spend a large portion of their time searching for relevant records across the network, and plotting the events in those records on a timeline so that they can determine what happened and when. As well as responding with an audit when an issue happens, internal auditors may also be involved in the ongoing process of identifying potential breaches or lapses in control. They need wide-ranging access to data and logs, but often need to rely on business area staff to gather this for them.

SECURITY MANAGER

Security managers will be able to…

Identify sensitive, classified, or other high risk information on the network, and track what happens to it in real time or near time

And produce…

Reports and recommendations on what security tools and protocols to deploy, or what data to move or restrict

Using…

Ontologies to generate lists of risky information across the network, and audit tracking capabilities to alert to exceptions

They will know this is successful when…

Risk is well understood across systems and over time, and security recommendations are evidence-based

Automatic registration of all records and items

Ontologies that automatically match and list risky data

Visibility of all events, such as copy, preview, share

Automated reporting on control breaches in the network

"My focus is on the risk profile of the enterprise – I need to know where our risky information is, and what happens to it."

Security managers need to know what we have, where it is, what risk it has, and who is doing what to it. It's not always possible to harden every system to a high level, or turn on logging on every drive. Knowing what information is inherently risky, and where it is, means we can focus our efforts on that data and those systems. We may find information that needs to be moved or deleted, or systems that should be better secured. As well as these preventative controls, we need detective controls, to identify any breaches that happen so we can respond.

LEGAL OFFICER

Legal officers will be able to…

Identify all data (documents, email, database etc.) relevant to their eDiscovery, without needing source system access

And produce…

Complete and accurate responses, including in-scope records, but excluding those that should not be released

Using…

Powerful search and ontology tools, which work across all systems, as well as regulatory rules matching that reports exclusions

They will know this is successful when…

eDiscoveries are responded to within the required timeframes, including all (and only) relevant information

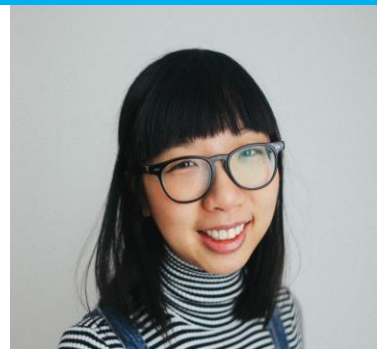
eDiscovery by key phrase or named entity across all systems

Ability to create ontologies for data in scope of requests

Alerts when relevant content is added or modified in systems

Regulatory rules applied to data showing what cannot be released

"I am responsible for an ever-increasing amount of discovery year-on-year, across all types of ESI, stored in many systems."



Legal officers are responsible for managing and responding to eDiscovery and eHold requests across all kinds of records, stored in all types of systems. The consequences for ineffective management of legal and FOI discoveries can be serious. A large portion of the job for legal officers is searching for potentially relevant information, but as they do not always have full access to source systems, they rely on the business to help find relevant records. This is costly, and can cause delays that affect the statutory reply timeframes.

C SUITE EXECUTIVE

Executives will be able to…

See at a glance where our high-value and high-risk data is; what systems are used for what functions; and what rules apply to our content

And produce…

Evidence-based plans, policies, strategies, and reports, showing the current state, with recommendations for improvements and remediations

Using…

Visualisations, graphs, reports, and dashboards, which contain a full index of what information we have, what rules apply, and whether they are met

They will know this is successful when…

Their plans for addressing risk, and taking advantage of opportunities, are based on complete, accurate, current data, and map to key priorities

Dashboards for systems, records, and audit events

Visualisations for content sizes, types, rules, and functions

Exportable reports across all systems and records

Automated content alerts for controversial topics or priorities

"I am accountable for achieving outcomes, while balancing risk. I need to see the big picture, and how it aligns to our goals."

Executives need to make strategic decisions, based on good evidence. They need to be able to see what is happening across their teams right now, and see what has happened in the past, so that they can see trends, and identify emerging challenges and opportunities. They have regulatory and statutory obligations to ensure their teams' information is secure, managed compliantly, and used (and reused) effectively. This requires their staff to create regular and comprehensive reports, which can be very time consuming.

IT OPERATIONS MANAGER

IT Operations Managers will be able to…

Understand which systems can be decommissioned, which need to be hardened, and which will need to be upgraded

And produce…

Evidence-based plans for managing network architecture, applications, databases, and operating systems

Using…

Comprehensive information on system sizes, contents, records rules, security risks, usage patterns, file types, and

They will know this is successful when…

Plans for managing operations and IT change are based on accurate information, and consider business and user needs

Dashboards for systems, records, and audit events

Visualisations for content sizes, types, rules, and functions

Exportable reports across all systems and records

Agentless config for full coverage with low impact

"I need to make sure our systems function securely and effectively, and I need to make decisions about them based on their data."

IT Operations has to be a balance between what is best-practice for systems and platforms, and what the business needs and expects. We can't keep everything forever, and we can't apply high-security controls to every system. To make the best decisions about system management, IT Ops need some involvement in data management. Knowing where risky data is helps to prioritise logging, monitoring, and hardening. Knowing how long we need to keep data helps prioritise storage, archiving, and systems lifecycles.

TEAM/PROJECT MANAGER

Team Leaders will be able to…

Help their staff find the right information, at the right time, so that they can be productive and effective in their role

And produce…

Successful outcomes for their team, with better information management and compliant, secure control of records

Using…

Powerful search to find important information across systems and over time, and automated sentencing and classification

I'll know this is successful when…

Teams are focused on their job roles, with better and faster access to data, and automated compliance

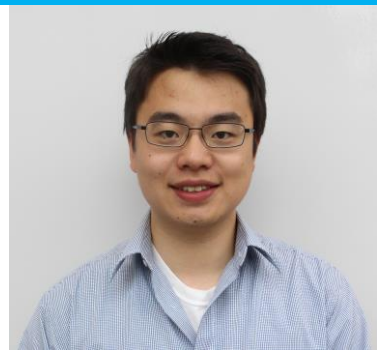
Searching by key phrase or named entity across all systems

Ontologies to automatically aggregate relevant info for teams

Complete audit history of team member activities

Automated security and records classification

"I have responsibilities to make sure my team are working effectively, efficiently, and in accordance with our rules."



Team leaders need to ensure that their team is working compliantly, but they know that it's not reasonable to expect all of them to understand and apply all of the complex types of rules that we are subject to. We want staff to be as productive as they can be, and to focus on their job role, rather than on records management, for example. We also don't want staff spending most of their time searching for information that they need, or reinventing the wheel when they can't find it. Team leaders need to find efficiencies.

CASE OFFICER

Case Officers will be able to…

Focus more on their cases, rather than on recordkeeping and other rules; and get better control of case-related information

And produce…

Better outcomes and recommendations, based on review of all relevant historical data, and visibility of current information and activities

Using…

Powerful search for people, places, and things; ontologies to group case-related records across systems; and alerts so nothing is missed

They will know this is successful when…

More time is spent on cases, and less time on searching, filing, classifying, securing, and compliantly managing records.

Ontologies to automatically aggregate relevant info for a case

'Virtual records' managing case records across systems

Alerts when relevant content is added or modified in systems

Regulatory rules applied to data to help prevent breaches

"I have a large case load, and often my records are sensitive or confidential. I need good control of all my information over time."

Case Officers often have large numbers of concurrent cases, all generating large amounts of data across various systems. Some cases go on for years or even decades, and the history of what happened and when can be lost. As well as challenges finding and relating all that information, Case Officers usually have to consider privacy and security obligations, which can change over time. These rules are vital, but there is little time each day to focus on compliance.

QUALITY MANAGER

Quality Managers will be able to…

Develop quality plans based on organisational risks; properly manage quality procedures and documentation; and audit quality performance

And produce…

Policies based on real customer data, risks, and regulatory requirements; and evidence-based reports to support continuous improvement

Using…

Automated linking of customer records, and mapping to functions and rules, to help define risks and obligations; search and audit tools across systems

They will know this is successful when…

They can find and track activity on every procedure document in the organisation, and ensure that QMS plans include real business context

Dashboards and discovery for high risk/high value data

Ability to create ontologies to track quality documents

Alerting and reporting of changes to quality documents

Automated application of regulatory rules to data and systems

"My role is to ensure we meet the expectations of our stakeholders, and manage our risks properly."

Quality Managers need to understand the context of the organisation, and where its risks lie, in order to develop good quality control plans and procedures. They also need visibility of how quality controls are (or are not) being met, so that they can track and report against targets, manage quality performance, and undertake continuous improvement. Quality Managers also need to control the formal quality documentation of the organisation, and help foster awareness and compliance among staff.

PRIVACY OFFICER

Privacy Officers will be able to…

Respond to queries quickly, with confidence they have found the relevant information

And produce…

Correctly scoped responses, taking into account regulatory rules for information release

Using…

eDiscovery and automated classification capability to understand risk

They will know this is successful when…

Their privacy queries are resolved faster, with less time spent on searches

eDiscovery by key phrase or named entity across all systems

Ability to create ontologies for data in scope of requests

Alerts when relevant content is added or modified in systems

Regulatory rules applied to data showing what cannot be released

"My role is to make sure that we respect and protect any personal information that we hold"

Privacy Officers need to be responsive to queries and requests from inside and outside the organisation, providing current, correct, and complete reports on the location of personal information, and its usage, governance controls, and protections. They need to understand privacy laws and how they apply to different data sets, and need to provide support with scoping and developing Privacy Impact Assessments and privacy management plans. They need to work with other teams to respond to requests for information.

CHIEF DATA OFFICER

Chief Data Officers will be able to…

Have command and control across the whole enterprise, understanding their data assets and risk

And produce…

Evidence-based reports on data holdings, systems, compliance, security, and storage

Using…

Information asset registers that are automatically updated, with classification applied

They will know this is successful when…

They are able to make valuable recommendations at the system or data set level

"My role is to get as much value as possible from our large sets of data, while making sure they are protected properly"

CDOs need to understand the scope and scale of data holdings, and identify ways to exploit them in support of business needs and innovation. They need to apply an ethical framework to ensure that information is being captured, retained, used, and retired compliantly and securely. CDOs need to provide advice to all areas of the business around how their data is managed, and work closely with ICT to make sure systems are appropriate for best control of, and access to, organisational data.

Automatic registration of all records and items

Dashboards, auditing, and discovery for high risk/high value data

Automated application of regulatory rules to data and systems

Visualisations for content sizes, types, rules, and functions