TOP 5 M365 COMPLIANCE FEATURES LEGAL SHOULD KNOW ABOUT

www.lighthouseglobal.com
Microsoft + Lighthouse Alliance

- Working relationship began 20 years ago
- Grew up together in eDiscovery
- Lighthouse is the leading Microsoft Compliance Partner for Microsoft 365
- Lighthouse is Microsoft’s eDiscovery service provider
- Engaged in all major U.S. regions, the UK and EU; working with 200+ corporations globally
- Key advisory positions include Partner Advisory Council (PAC); GDPR partner program; Financial Services Consortium
- Relationships within the Security and Compliance Product Group, O365 PAC, and CELA
- Strategic alignment between Microsoft and Lighthouse
James Hart

Governance Risk Compliance Consultant, Global Advisory Services

- Microsoft 365 Certified: Security Administrator Associate
- Certified Information Privacy Professional – Europe (CIPP/E)
- Over 10 years of in-house and consultancy experience in the legal technology services.
- Strong track record in supporting global corporations on high profile projects in the areas of Information Governance, Incident Response and E-Discovery.
- Former roles with Barclays PLC, developing their eDiscovery technology and operations capabilities before moving onto Advisory Services.
Introduction

A quick introduction of M365

Top 5 Features for Legal
The accessibility of data

• Adoption of cloud-based data is one of the most disruptive and significant trends to hit the information governance profession in the past 20 years
• Having data in the cloud (e.g. in M365) means you have the data in, effectively, one place and in, effectively, one searchable format
The availability of tools

- **Information Protection & Governance**: Protect and govern data anywhere it lives
- **Insider Risk Management**: Identify and remediate critical insider risks
- **Discover & Respond**: Quickly investigate and respond with relevant data
- **Compliance Management**: Simplify and automate risk assessments
Microsoft’s Investment in Compliance (Including GDPR)

- Retention & Disposition
- Cloud DLP
- Communications DLP
- Rules-based auto classification
- Machine Learning auto classification
- Records Management
- Customer Key
- Advance Message Encryption

- Insider Risk Management
- Communications Compliance
- Information Barriers
- Customer Lockbox
- Privileged Access Management

- Advanced Audit
- Core eDiscovery
- Advanced eDiscovery
- Data Subject Access Requests

Compliance Management
- Compliance Manager
- Compliance Score
- GDPR Dashboard
eDiscovery Reference Model

Typical Use cases
- Litigation
- DSAR
- Compliance / HR investigation
- Regulatory requests
- Law Enforcement requests

Key Factors
- M365 License Model (E3 vs. E5)
- Processing, Analysis & Review capabilities or workflows
- Manual vs Automated processes
- Task ownership
Introduction

A quick introduction of M365

Top 5 Features for Legal
1. In-Place Legal hold

When a reasonable expectation of litigation exists, organizations are required to preserve electronically stored information (ESI), including email that’s relevant to the case. Also known as, in-place hold, or legal hold.
Traditional eDiscovery and M365

Core eDiscovery
- Identification
- Preservation Collection

Advanced eDiscovery
- Identification
- Preservation Collection
- Processing
- Analysis
- Review

Compliance Tools
M365 In-Place Legal Hold

- Create a eDiscovery Case
- Create a Legal Hold
- Select User Locations (SharePoint/OneDrive/Exchange)
- Use Conditions/Filters
Legal Holds – Litigation vs In-Place Holds

Litigation Hold

- Applied in Exchange Admin Center
- Applied on a Resource
- Covers the entire resource
- Holistic Approach
Legal Holds – Litigation vs In-Place Holds

Litigation Hold

Applied in Exchange Admin Center
Applied on a Resource
Covers the entire resource
Holistic Approach

In-Place Hold

Applied in Compliance Center
Applied using Conditions
Covers a specific resource
Targeted Approach
Triggers litigation hold (500+ keywords)
2. In-Place Search

If your organization adheres to legal discovery requirements (related to organizational policy, compliance, or lawsuits), In-Place eDiscovery in Microsoft Exchange Server and Exchange Online can help you perform discovery searches for relevant content within mailboxes.
Content Search

Fast & Powerful

- Multi-threaded makes content searches built for scalability and speed.
- Includes key storage locations (Exchange, SharePoint & OneDrive)
- Using powerful Keyword Query Language (KQL)

Preview

- Ability to sample the data found during the search

Export

- Ability to export the results for downstream analysis
- Provide a report of the results

<table>
<thead>
<tr>
<th>No. of mailboxes</th>
<th>Speed</th>
<th>Average (Sec.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>30 seconds</td>
<td>0.3</td>
</tr>
<tr>
<td>1,000</td>
<td>45 seconds</td>
<td>0.045</td>
</tr>
<tr>
<td>10,000</td>
<td>4 minutes</td>
<td>0.024</td>
</tr>
<tr>
<td>25,000</td>
<td>10 minutes</td>
<td>0.024</td>
</tr>
<tr>
<td>50,000</td>
<td>20 minutes</td>
<td>0.024</td>
</tr>
<tr>
<td>100,000</td>
<td>25 minutes</td>
<td>0.015</td>
</tr>
</tbody>
</table>
Content Search - Example

Add conditions

- Name
- Group
- Date
- Sender/Author
- Size (in bytes)
- Subject/Title
- Retention label
- Message kind
- Participants
- Type
- Received
- Recipients
- Sender
- Content

Search

Options:

- Name
- Group
- Date
- Sender/Author
- Size (in bytes)
- Subject/Title
- Retention label
- Message kind
- Participants
- Type
- Received
- Recipients
- Sender
- Content

Add
Cancel

- 109,394 items
  - John NEAR(5) Collins
- 99,209 items
  - John NEAR(5) Collins
  - Message kind: Email
- 43,334 items
  - John NEAR(5) Collins
  - Message kind: Email
  - Date: 2020-07-25..2020-08-25
- 4,521 items
  - John NEAR(5) Collins
  - Message kind: Email
  - Date: 2020-07-25..2020-08-25
  - participants NOT john@ledlabs.org
- 528 items
  - John NEAR(5) Collins
  - Message kind: Email
  - Date: 2020-07-25..2020-08-25
  - participants NOT john@ledlabs.org
  - Has Attachment: True
3. Advanced eDiscovery

With Advanced eDiscovery, you can better understand your data and reduce your eDiscovery costs. Advanced eDiscovery helps you analyze unstructured data, perform more efficient document review, and make decisions to reduce data for eDiscovery.
Advanced eDiscovery

Core eDiscovery

Information Governance
Identification (Search)
Preservation and Collection
Processing
Review
Analysis
Production
Presentation
Advanced eDiscovery

Identification, Preservation, Collection, Processing, Analysis, Review & Production

1. Create case
2. Assign permissions
3. Add custodians and data sources
4. In-place hold on entire source or scoped
5. Conduct searches
6. Processing
7. Analytics
8. Review and production

“Deep Indexing”

Legal hold notice

Boolean, Proximity, Wildcard, date range, metadata

Themes
Near duplicate detection
Email threading
Predictive Coding

Review and tagging
Redactions
Production
Analytic values for review
Natives
HTMLs
Export load file

Ingest external Data

Exchange Online
SharePoint Online
OneDrive for Business
Teams
Groups
Exchange Public Folders

Legal hold notice

© 2020 Lighthouse. All rights reserved. Lighthouse is a registered trademark of Lighthouse Document Technologies.
DSAR Op Model

**Typical DSAR**
- Requires up to date data mapping
- Can take time to contact SME’s
- Inconsistent approach

**Advanced eDiscovery**
- Automatic data source mapping
- Simplified collection workflow
- Ability to sample/test keywords or collection scope prior to collection
- Filter by keywords, metadata, document types and dates
- Teams message thread reconstruction
- No movement or duplication of data (data remains in O365)
- Search can be run by HR/Legal/Privacy depending on Operating Model

**Identification**
- M365 Data?
- Acquire from other location

**Collection**
- M365 Content Search
- Add to Review Set
- Data Processing
- Analysis & Review
- Production

**Processing**
- Inefficient basic workflow
- Linear review (one document at a time)
- Manual document tracking
- Slow document to document speeds
- Inconsistent approach
- Limited document management can lead to duplication or spoliation of data within the organisation
- Reliance on 3rd Party tools (Adobe) for redactions
- High risk of inaccurate productions
- Manual QC
- Time take to combine production

**Analysis**
- Optical Character Recognition (OCR) and Advanced indexing enables further filtering with search
- Web based review simplifies and speeds up the review.
- Document tagging enables granular document tracking and multi level reviews.
- In-place redaction removes the need to manually export and redact documents
- Teams message threading improves the review by consolidating the full conversation into a single reviewable thread
- Full audit history of events.
- Automatic Attorney-Client Privilege detection
- Workflow can include QC prior to production
- Defensible production of documents in PDF or Native file formats.

**HR/Legal/Privacy**
- Assessment / Scoping
- Review, Tag, Redact
- Disclosure

**IT/Security**
- Request
- Identification of Data sources
- M365 Data?
- Acquire from other location
- Non-Office 365 Data Import

**Advanced eDiscovery**
- Can import non-Office 365 data sources to consolidate review
- Deduplication, Near duplication and Threading simplify and speed up the review
- Optical Character Recognition (OCR) and Advanced indexing enables further filtering with search
- Web based review simplifies and speeds up the review.
- Document tagging enables granular document tracking and multi level reviews.
- In-place redaction removes the need to manually export and redact documents
- Teams message threading improves the review by consolidating the full conversation into a single reviewable thread
- Full audit history of events.
- Automatic Attorney-Client Privilege detection
- Workflow can include QC prior to production
- Defensible production of documents in PDF or Native file formats.
Microsoft 365 Advanced eDiscovery

**Preserve**
- 2.5 TB data
- 36 People
- 70-200 sources

**Scope**
- 900 GB data
- 13 People
- 50 sources

**Minimize**
- 27 GB data
- 97% reduction in volume

**Analyse**
- De-duplication: -30%
- Threading: -25%
- Total further reduction: -45%

**Review**
- Organized
- Prioritized
- Consistent

Average Microsoft Cases for 2016 - 2019
Reduce cost per custodian

Microsoft’s legal team found 85% reduction in cost/custodian
4. Advanced Audit

The unified auditing functionality in Microsoft 365 provides organizations with visibility into many types of audited activities across many different services in Microsoft 365. Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention required to conduct an investigation.
M365 Audit Events
M365 Audit Events
5. Data Insights

Pull deep insights such as:

- Stale data
- Ungoverned and unprotected sensitive information
- Fraudulent and suspicious activity

...to identify the greatest risks in your organization.
Use eDiscovery to Identify Stale or Outdated Data

VISUALISE DATA GROWTH OVER TIME

FIND OUTDATED INFORMATION

REMEDIATE EXISTING ISSUES
Use eDiscovery to Identify Sensitive Data in SharePoint/OneDrive

**IDENTIFY SENSITIVE DATA TYPES**

**FIND SENSITIVE INFORMATION**

**REMEDiate EXISTING ISSUES**
Use DLP to Identify Sensitive Data In-Transit (Exchange Online)

**MONITOR EVENTS**

Events Over Time

**IDENTIFY PATTERNS**

Typical File Extensions

**INVESTIGATE ISSUES**

<table>
<thead>
<tr>
<th>Event Date</th>
<th>Filename</th>
<th>Modified By</th>
<th>Rule</th>
<th>Sensitive Information</th>
<th>Sensitive Information Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected France Financial</td>
<td>Credit Card Number</td>
<td>2355</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected Germany Financial Data</td>
<td>EU Debit Card Number</td>
<td>2374</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected France Financial</td>
<td>Credit Card Number</td>
<td>1400</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected Germany Financial Data</td>
<td>EU Debit Card Number</td>
<td>1268</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected Germany Financial Data</td>
<td>Credit Card Number</td>
<td>906</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file155</td>
<td><a href="mailto:name0316@email.com">name0316@email.com</a></td>
<td>High volume of content detected Germany Financial Data</td>
<td>EU Debit Card Number</td>
<td>906</td>
</tr>
<tr>
<td>03-Oct-2020</td>
<td>file0335.xls</td>
<td><a href="mailto:name0614@email.com">name0614@email.com</a></td>
<td>High volume of content detected France Financial</td>
<td>Credit Card Number</td>
<td>783</td>
</tr>
<tr>
<td>03-Oct-2020</td>
<td>file0335.xls</td>
<td><a href="mailto:name0614@email.com">name0614@email.com</a></td>
<td>High volume of content detected France Financial</td>
<td>Credit Card Number</td>
<td>731</td>
</tr>
<tr>
<td>03-Mar-2020</td>
<td>file61.xls</td>
<td><a href="mailto:ExternalName1@email.com">ExternalName1@email.com</a></td>
<td>High volume of content detected France Financial</td>
<td>Credit Card Number</td>
<td>644</td>
</tr>
</tbody>
</table>
Use Audit to Identify Unusual or Suspicious Activity

**IDENTIFY PATTERNS**
- Alert Categories:
  - Threat Management: 45.93%
  - Data Governance: 54.87%
- 247 Total Alerts
- 5,263 Documents Impacted
- 3.35 Average Event Duration
- 824 Total Event Duration

**MONITOR ALERTS**
- Events Over Time:
  - Alert Category: Data Governance, Threat Management

**INVESTIGATE ISSUES**
- Alert Name: Unusual Volume of File Deletion
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Alert Name: eDiscovery Search Started or Exported
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Alert Name: Creation of Forwarding/Redirect Rule
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Alert Name: Unusual External User File Activity
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Alert Name: OneDrive/SharePoint - External Sharing
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Alert Name: A Potentially Malicious URL Click was Detected
  - 2020: March 02, 03, 05, 08, 09, 10, 12, 13, 18
- Total: 20, 9, 8, 9, 1, 3, 8, 8, 2, 9, 8, 18, 2
Thank You.

James Hart,
Director of Advisory Services
Compliance Consultant
jhart@lighthouseglobal.com