Presenter

- Dana Louise Simberkoff, JD, CIPP
- Chief Risk, Privacy and Information Security Officer, AvePoint
- Dana.Simberkoff@avepoint.com
- https://www.linkedin.com/in/danalouisesimberkoff
- @danalouise

You can't outsource chaos

"All great changes are preceded by chaos."

Deepak Chopra

COVID-19 | Paradigm Shock

In a matter of weeks commerce across the globe ground to a slow crawl:

- **Businesses went virtual or closed**
- **Individuals stayed home and purchased less**
- **Society moved at a glacial pace**

Businesses moved quickly to execute crisis plans – but as we look back over the past several months – we have learned much about how shift happens and how to prepare for what comes next

Growth

Crisis

Innovation

Stabilization
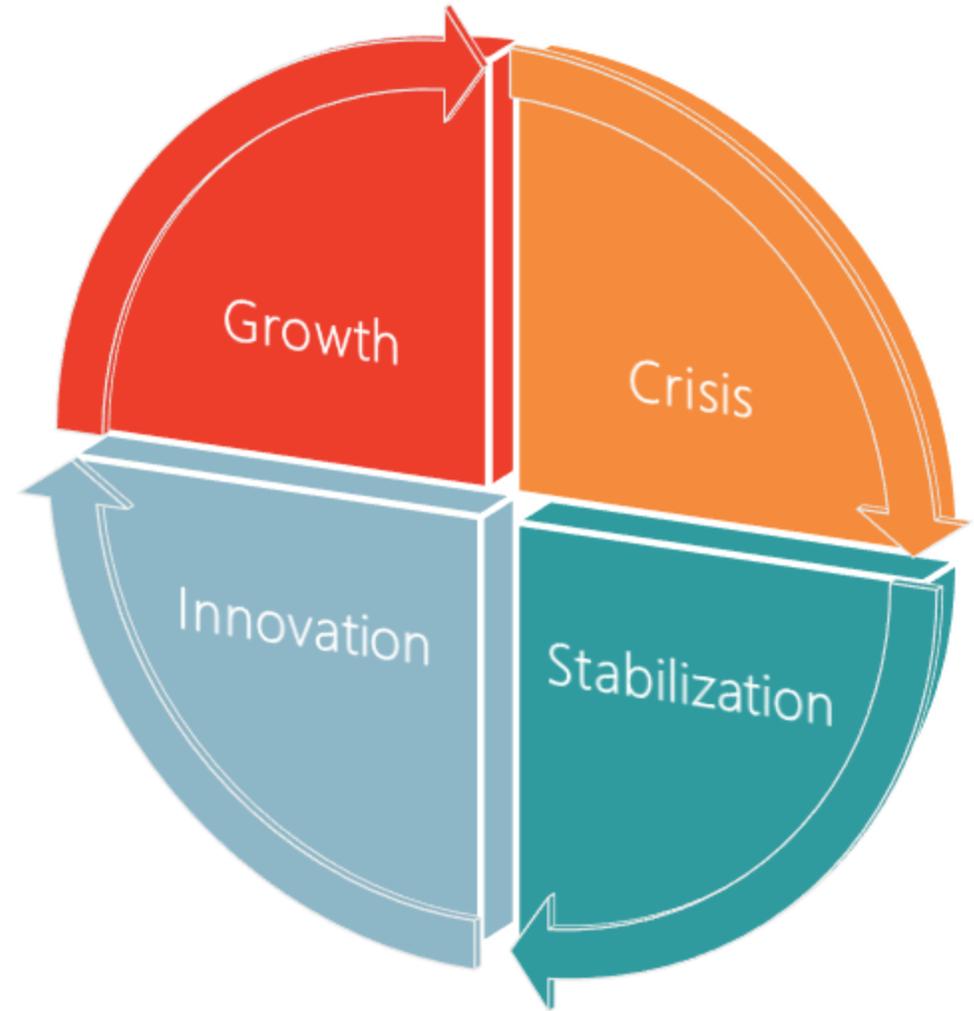
Crisis | Initial Response

Organizations worked to ensure continued operations of our business globally – while continuing to serve customer, employee and regulatory needs and requirements

1 **Activate Business Continuity Plans Globally**

Reinforce existing policies and controls for safeguarding company data, including sensitive financial data, confidential and proprietary information

2 **Shift to Virtual Working Environment**

Most organizations shifted to a primarily virtual work environment which also meant a RAPID acceleration in Cloud technologies - and a shift towards sometimes untested systems

3 **Enhance Capabilities to Meet Data Demands**

Increased volume and timeliness demands required comprehensive approaches to data governance, quality and access rules and processes

# Why is Data Governance/Security Important?

- Increasing data volumes from more and more sources

- More self-service reporting and analytics

- Need for a common business language

- Impact of regulatory requirements

- Cross border data transfer

ENGLAND'S 7-CIRCLE MAGIC ROUNDABOUT

NOW THERE'S **FEWER BOUNDARIES**, MORE DATA, MORE COMPLEXITY

Office 365

now

salesforce

box

On-premises
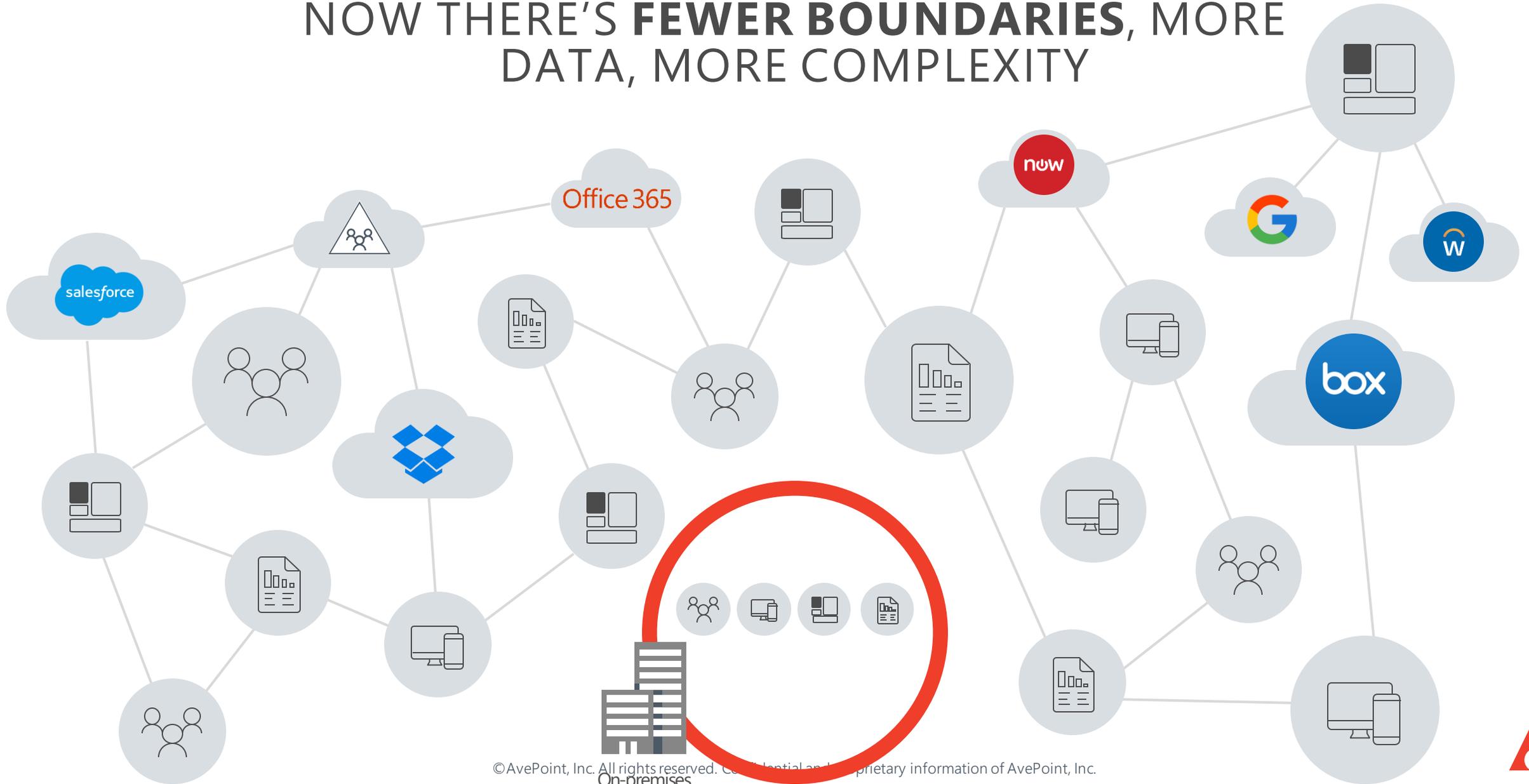
The Face of Collaboration
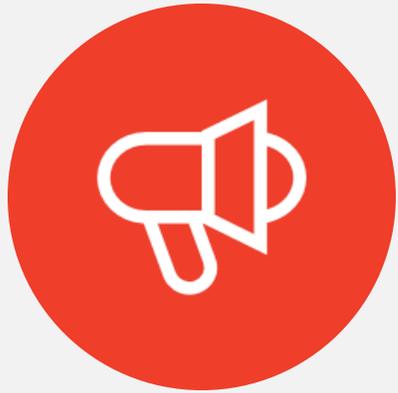
Everyone has a Voice

Access from Anywhere

Everyone is a Contributor

Unstructured content is all over

20% **Structured Application Content**

80% **Unstructured content**

Enterprise Applications

Student information systems
Financial systems
HR systems
CRM

Enterprise Content Management

Marketing
- Outreach
- Recruiting
- Collateral

Admissions & Enrollment
- Transcripts
- Letters of recommendations
- Application essays
- Forms

Financial Aid
- FAFSA
- Verification statements
- W2s
- Tax returns
- Scholarship tracking
- Correspondence

Finance
- Requisitions
- Purchase orders
- Invoices
- Routing & approval
- A/P & A/R supporting documentation

HR
- Staff & faculty onboarding
- Employee records
- Contracts

Records Management
- Governance
- Compliance
- Retention
- Disposition

Digital Asset Management
- Rich media files such as Images and videos
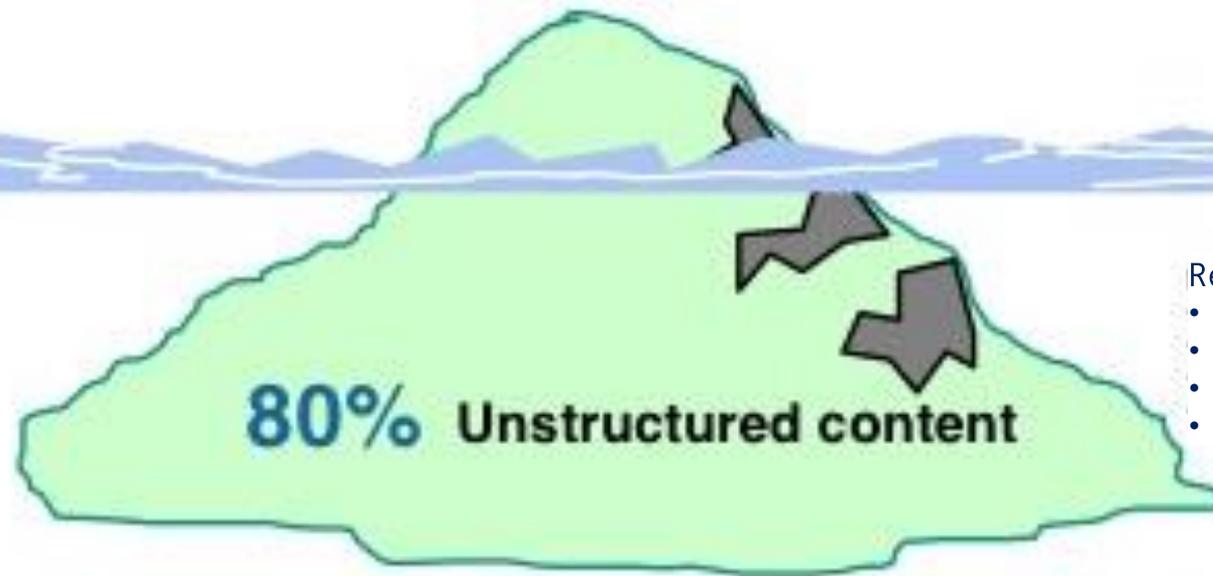
We need to establish confidence

Suffered at least one breach in the last year

| 41% | 63% | 65% | 68% | 65% | 59% |
| FOR PROFIT, PRIVATELY HELD | NOT FOR PROFIT | FOR PROFIT, PUBLICLY TRADED | GOVERNMENTAL | NON-HEALTHCARE | HEALTHCARE |
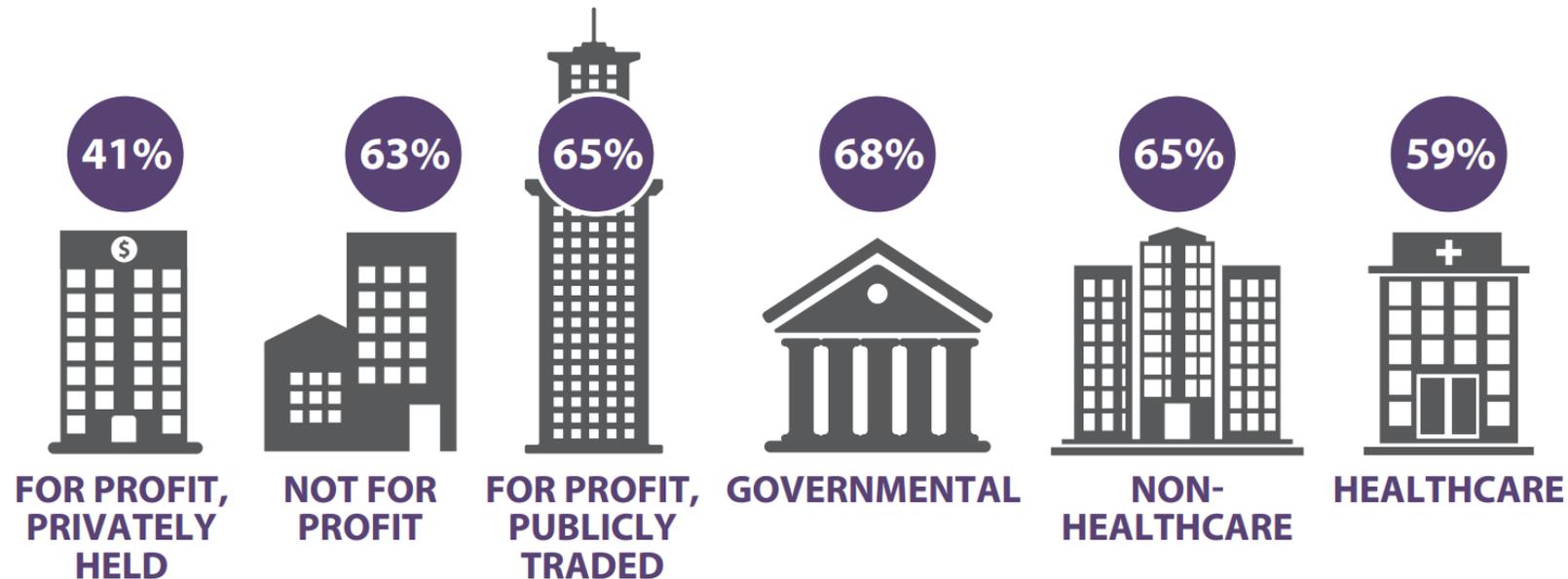
*Society of Corporate Compliance & Ethics / corporatecompliance.org*

What does the pandemic mean for the compliance team?

CHANGE IN NUMBER OF COMPLIANCE INQUIRIES

Legend: Overall (blue), Healthcare (green), Non-Healthcare (orange)

	A large increase	Somewhat of an increase	About the same number	Somewhat of a decrease	A large decrease
Overall	11%	24%	38%	23%	4%
Healthcare	15%	27%	29%	23%	6%
Non-Healthcare	8%	22%	45%	22%	3%
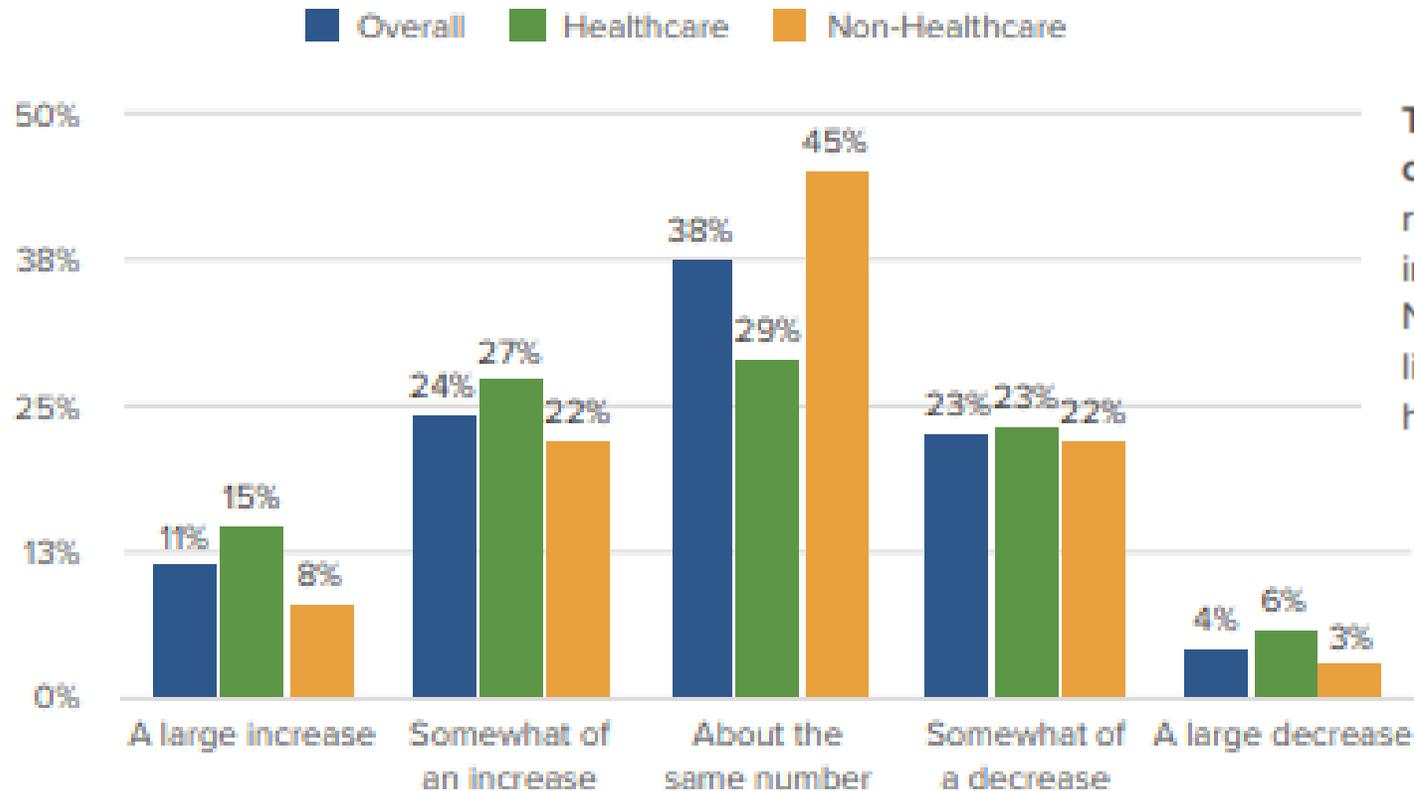
The pandemic has seen a reported increase in the number of inquiries to the compliance team. Across industries, 36% reported that there has been a somewhat or large increase in inquiries, compared to just 27% showing a decrease. Notably, the healthcare respondents were much more likely to report an increase (42%) than those outside of healthcare (30%).

...ion of AvePoint, Inc.

What to Govern

What is metadata?

Made by

Volume

Contains

Made since

What Makes Your Content Classified?

Contents

Sample: HR

- Visible/ Invisible Text
- Templates
- Accessibility

Context

Sample: Finance

- Shared Path
- Site Tags
- Security

People

Sample: Info-Worker

- Department
- Geography
- Properties
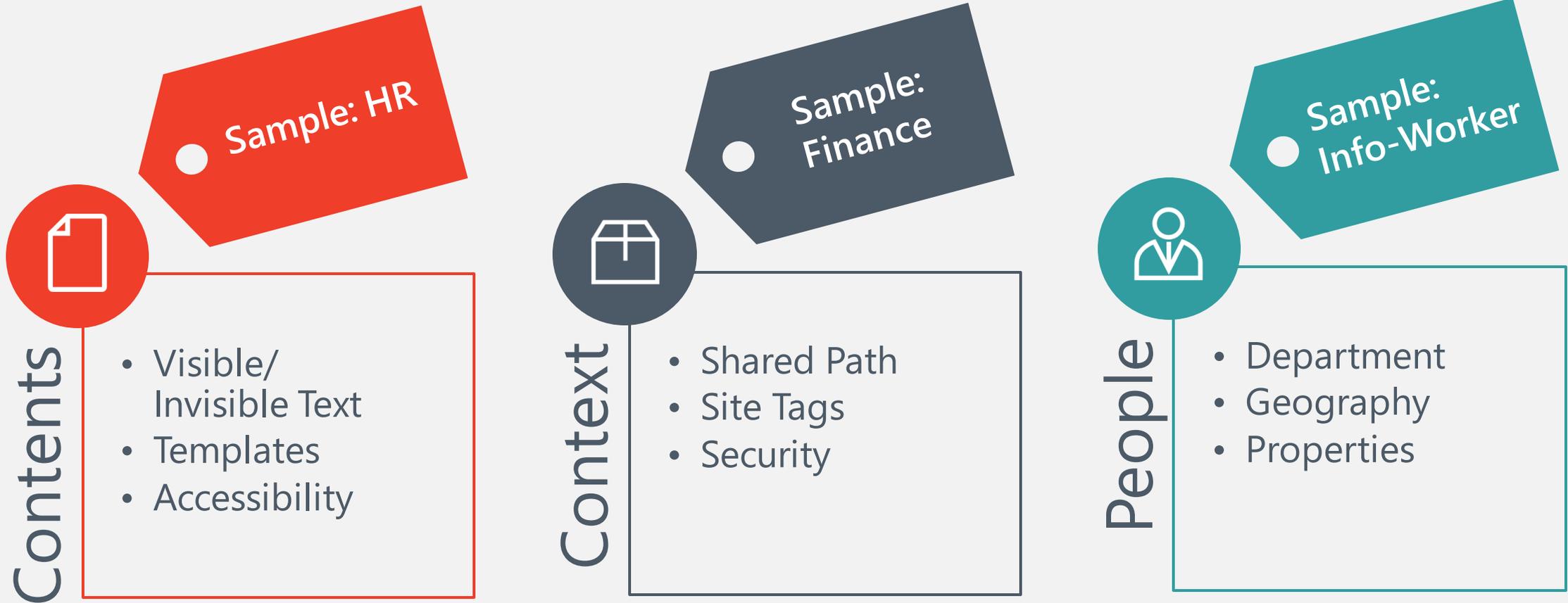
Information creation is not in a single place
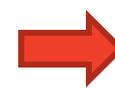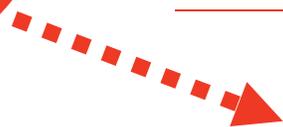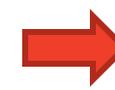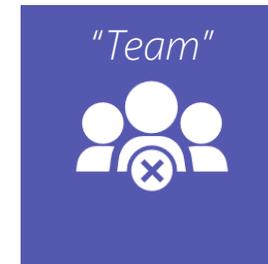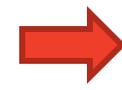
Cloud Ready

Dark data is the key problem

- Current project files
- Current reference docs

- Client records
- Employee records
- Previous project files

Dark Data

What you need to keep...

What you use...

What do we have?
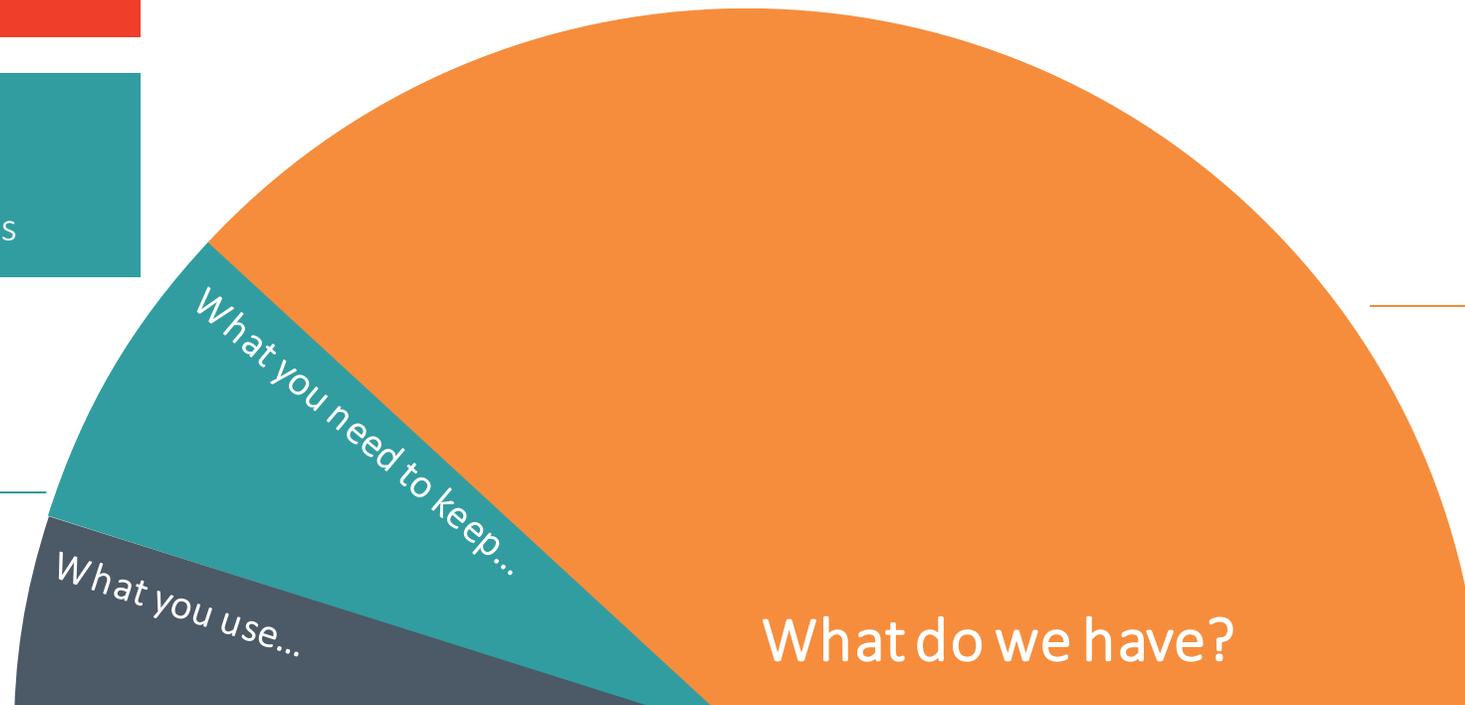
How Do You Know
Where your data is?

Best practices approach

Say It

1 Assess	2 Identify Risk	3 Prioritize

Do It

4 Data Classify	5 Take Action	6 Incident Management

Prove It

7 Ongoing Monitoring	8 Incident Tracking

It's Your Data...

- Find out what it really is
- Establish a way to identify it
- Protect what's important
- Keep what's required
- Remove what's unnecessary
- Plan for the future

Users:
Relevant Information

IT Admins:
Easier Maintenance

Compliance Officers:
Lowered Risks

Reduce **Cost**. Increase **Productivity**.

Clean-up & Consolidation

Can I get rid of it?

- Is it a record?
- Is it a duplicate?
- Is there a later version?
- Is it relevant?

Does it need to be reorganized?

- Is it a record?
- Does it belong somewhere else?

Archive

Delete

Discovery & Mapping

Where is it?

- File Share
- SharePoint
- Office 365
- Database

What is it?

File Level Analysis

- Redundant, outdated and trivial (ROT) data
- File types (Music, log files, etc..)

Content Level Analysis

- Sensitive data
- Date Created
- Owner

Who can access it?

- Who owns it?
- Who can read it?
- Who can edit it?

Tagging & Classification

Tags

Ownership	Purpose
Audience	Sensitivity level

Classify

Where should it live?	Who should have access?
Is it a record?	Is it high business impact?

Post-Analysis Options

Compliant Migration to...

Another location for "legal hold"

Another location on the file system for archiving

Another location on the file system

Another system (SharePoint, Office 365, storage, etc.)

End-of-Life

Assessments Wherever You Work

CLOUD

| Box | DropBox | Slack | Google Drive | Google Mail | Office 365 |

ON-PREMISES

| SharePoint | File Systems & Databases | Websites | Skype for Business | Exchange | Service Now |

Example: Maintaining an inventory of sensitive data

1 Lower your risk profile with content security insights by location across multiple platforms.

2 Easily navigate the structure of your sensitive content via location.

Enterprise Risk Management — admin

Go to upper level   Go to lower level   Check Incidents

Test Suites: 250 Matches

Financial Data: 100 Matches

Social Security Number (SSN): 22 Matches

Bank Account Number: 17 Matches

Taxpayer Identification Number: 11 Matches

Driver's License Number: 29 Matches

Passport Number: 12 Matches

Tax File Number: 6 Matches

Debit Card Number: 7 Matches

Phone Number: 4 Matches

IP Address: 2 Matches

Personally Identifiable Information (PII) Data: 80 Matches

Patriot Act: 50 Matches

Fedetal Trade Commission ConSumer: 10 Matches

Health Insurance Act: 10 Matches

Ongoing Control for Sensitive Content

Label / Tag Metadata
Visibly tag and classify information based on Context (Geography), Users (Properties), Regulation, and other information. Embedded tags and pointer-records for all file types

Encryption
Apply Azure Information Protection policies or AvePoint encryption on content across multiple systems and legacy file shares to protect data from exfiltration

Redaction/ Pseudonym-ization
Monitor for sensitive data shared on public sites (intranet portals) and redact any sensitive information

Move/Change Permissions
Check OneDrive for PCI / ITAR / HIPAA regulated data and automatically move content to secure sites or on-premises servers

Quarantine
Avoid fines by isolating data outside of the system where the violation occurs, including incident workflow

thank you

Gracias	ευχαριστώ	Danke	Grazie	благодаря
Hvala	Obrigado	Kiitos	شكراً	Tak
Ahsante	Teşekkürler	متشكرم	Salamat Po	감사합니다
Cám ơn	شکریه	Terima Kasih	Dank u Wel	Děkuji
நன்றி	Köszönöm	ありがとうございます	ขอบคุณครับ	Dziękuję
谢谢	Tack	Mulţumesc	спасибо	Merci
תודה	多謝晒	дякую	Ďakujem	