Cloud Governance Success: A Practical Framework to Getting Started with Cloud Data Governance

November 2021

Authors:

Carla Arend, Senior Program Director: Lead Analyst, Cloud in Europe, IDC

Ralf Helkenberg, Research Manager, European Privacy and Data Security, IDC

IDC #EUR148304021

An IDC InfoBrief, sponsored by

Microsoft

A Framework for Success with Cloud Data Governance

As cloud becomes mainstream it can unlock significant business value. Time to business value can be accelerated if cloud is viewed as an architecture and an operating model and not as a location. Cloud data governance defines the rules and controls for identifying and mitigating security and compliance risks wherever the data resides in a hybrid and multicloud operating model. This is of particular importance for highly regulated organizations.

This guide lays out a **practical approach to implementing a successful data governance** framework. It focuses on the three initial steps to **Plan, Understand and Assess** the organizational data landscape. This will allow you to identify, assess, mitigate, and manage risk in your hybrid multicloud environment.

Five Phases of a Cloud Data Governance Framework

Getting Started Phase

PLAN

- Initial preparation to ensure the **functional structures and organizational roles** are in place to build and implement cloud data governance.

UNDERSTAND

- **Evaluate** current state of cloud data governance with a maturity model.
- **Understand** what data governance policies and compliance regulations apply to your organization.
- Understand the data landscape with **data discovery and classification**.

ASSESS

- Define responsibilities under the **cloud responsibility model**.
- Define **risk appetite and tolerances**.
- Identify risks and evaluate against **risk acceptance** criteria.
- Specify **response to risk**.

OPERATE

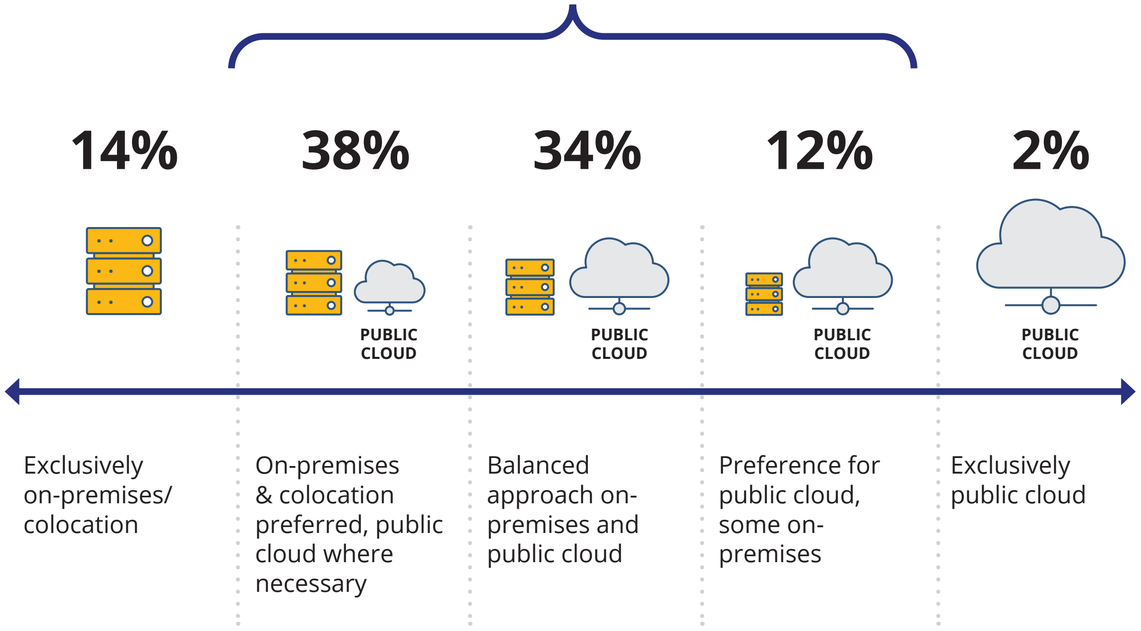
- **Operationalize and automate** data governance policies & procedures across the organization.

MONITOR

- **Monitor, measure, and adapt** the framework to meet the changing business, policy, regulatory, and security landscape.
- Share results with staff to promote an organization-wide **culture of learning about data governance**.

The Cloud Journey is evolving — The Destination is Hybrid and Multicloud Cloud

Hybrid and multicloud architectures are becoming the most common operating model, with 84% of European organizations operating a combination of on-premises IT and public cloud.



58% of European organizations have a cloud governance framework

Adoption leaders by country:

Why Is It Important?

Operating hybrid and multicloud architectures can be complex, but also unlocks innovation.

Cloud governance enables IT modernization, cloud migration, and business innovation while mitigating the security and compliance risks.

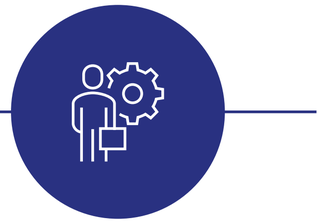
These are opportunities for organizations that have not yet implemented a Cloud Governance Framework.

PLAN

Organizational Readiness for Data Governance

The essential business requirements for the cloud governance framework are defined in the planning phase.

Business Case



The data governance framework is driven by the strategic goals and priorities of the organization, and in response to external regulations and requirements.

Identify use cases and desired business.

Typical goals are:

- Data quality improvement
- Ongoing data privacy, security, and compliance
- Optimize business intelligence and decision making
- Reduce costs and increase operational effectiveness

Governance Metrics

Supplement goals with specific, actionable statements that describe the framework scope, expected results, and how success is measured.

Success metrics should be SMART: Specific, Measurable, Actionable, Relevant, and Timely.

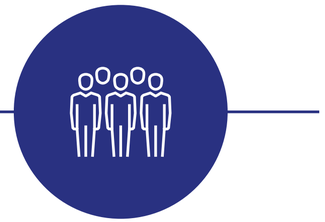
Policies, Standards, and Procedures

Common policies and standards are agreed and documented.

They should include data accountability and ownership, roles and responsibilities, data capture and validation standards, information security and data privacy guidelines, data access and usage, data retention, data masking, and archiving policies.

Repeatable processes are designed to enable policies and governance tasks.

People



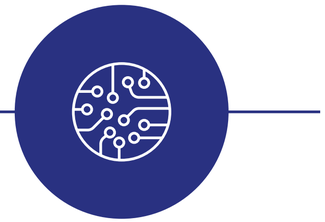
Organizational structures are in place to support the framework.

Data governance is a cross-functional effort. Stakeholders typically involved are:

- Data governance
- Legal & Regulatory Affairs
- Privacy and compliance
- IT and security
- Data science
- Line of business
- Data stewards

A workforce strategy is in place to address data skills and capability gaps.

Technology



Compliance-as-Code

Governance architectures can discover and organize data at scale, automate workflows, help embed privacy and security by design, monitor success, and enable organization-wide collaboration.

Manual processes should be automated within the operational architecture.

Technology solutions offer a scalable delivery model with the appropriate tools and capabilities to accelerate tasks.

UNDERSTAND

The Data Governance Maturity Model

The maturity model defines a pathway for organizations to improve their cloud data governance. Organizations can evaluate the current state of their cloud data governance, identify gaps in their practices and define improvement measures with the model.

Ungoverned

Organizations have no policies, processes and technology in place to govern their data. No roles and responsibilities have been established.

People
- No data governance control board
- No data owner accountable for data

Process
- No processes to monitor data privacy, quality, and security
- No common business vocabulary

Policies
- No policies to govern data privacy and retention

Technology
- No data governance software
- No data privacy and security tools

Partly Governed

Organizations have started with data governance. Some policies and processes are in place, technology is partially used. Not all people possess the right abilities.

People
- Data governance control board in place but no ability
- No data owners accountable for data

Process
- Some ability to monitor data privacy, quality, and security
- Common business vocabulary started in a glossary

Policies
- Some policies govern data privacy
- No policies to govern data retention

Technology
- No data governance and privacy software
- Data security across some systems

Governed

People, polices, processes, and technologies are in place to cover the most sensitive and business-critical data and systems.

People
- Data governance control board is in place
- Some data owners in place

Process
- Monitoring and stewardship of data privacy and quality on core systems
- Common business vocabulary established

Policies
- Policies govern data access and privacy using classification
- Some policies to govern data retention

Technology
- Some privacy enforcement through software
- Data access security across multiple systems

Fully governed

Mature organizations are characterized by having clearly defined policies and enforced by professionals with the appropriate processes and technology in place.

People
- Data governancecontrol board in place
- All data owners in place

Process
- Monitoring and stewardship of data privacy and quality on all systems
- Common business vocabulary completed

Policies
- Polices and rules to govern data access
- Data privacy and retention consolidated in data catalog using classification

Technology
- Data privacy enforcement for all data
- Data security across all systems

UNDERSTAND

Data Discovery and Classification

Data Discovery and Classification in Seven Steps

Before data governance policies can be enforced, organizations must assess where gaps exist. This process begins with data discovery and classification.

1	**Compliance Obligations**	Identify what internal data governance policies and compliance regulations apply to your organization.
2	**Classification Policy**	Establish a classification scheme. Policies and procedure are defined and should be in alignment with the sensitivity of the data types. Responsibilities of data owners are outlined.
3	**Categorize Data**	Identify the types of data held by organization and define your classification levels.
4	**Discover Data**	Discover and catalog all data held across environments.
5	**Classify data**	Apply classification labels to data.
6	**Apply Controls**	Use data results to implement appropriate controls based on level of risk.
7	**Monitor and Update**	Data is dynamic and requires monitoring for changes or policy violations.

The Data Swamp

Data in organizations is exponentially growing and widely distributed across environments. While some data is neatly structured, much is unstructured. Data protection regulations require organizations to have a holistic view of their data, yet data visibility is a blind spot for many.

Data Discovery

Data discovery is foundational to any data governance, privacy and security program. The process enables the building of a data processing inventory and map and determines:

- The business purpose behind the processing
- Understanding how data is collected and flows through the organization
- Understanding where data is stored, who has access to it, and retention periods
- Who are the third-parties involved in the processing
- How is the data protected

Discovery-in-Depth Through Automation

Manual data discovery is resource and time intensive and fails to scale for dynamic data environments. Automated data discovery tools can scan real-time for unknown sensitive data across both cloud and on-premises environments to provide that single source of data truth.

Use of Data Discovery Tools

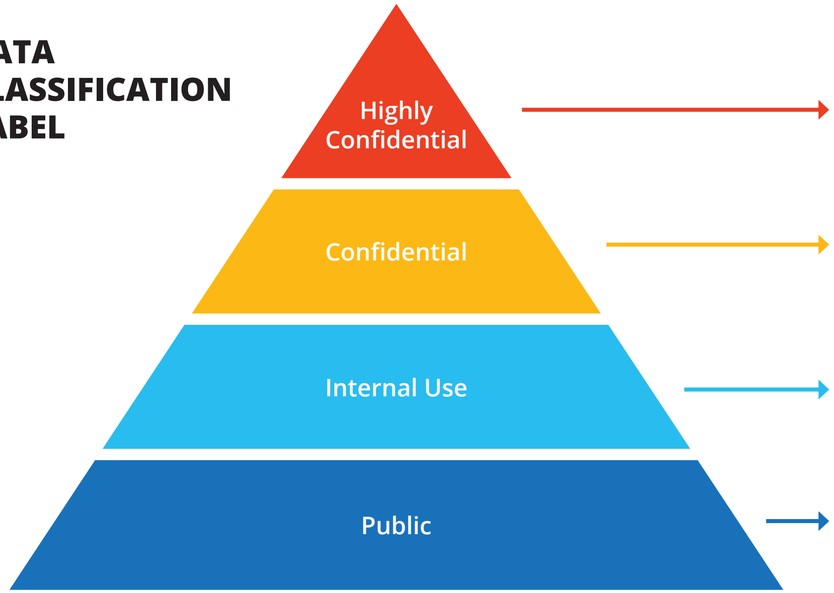
IDC Survey, Europe

UNDERSTAND

Data Classification

Data classification is used to categorize and label identified data according to its sensitivity or impact level.

DATA CLASSIFICATION LABEL



Severity	Description	Types of Data
Severe	The most sensitive type of data stored or managed by the organization. If compromised could put the organization at financial or legal risk.	Personal identifiable information Cardholder data Protected health information
High	Sensitive business data that if compromised could negatively affect operations.	Vendor contracts Employee records
Moderate	Business data that isn't meant for a public audience.	Sales playbooks Price lists
Low	Business data that is freely available and approved for public consumption.	Marketing material Contact information

DATA CONTROLS

Data classification also helps to define the controls that should be in place for each of the classification levels. These may include:

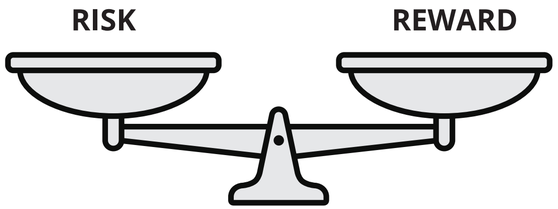
- Storage type and location
- Encryption
- Access control
- Data loss prevention
- Data retention
- Data destruction
- Public disclosure
- Logging and tracking

ASSESSMENT

Risk Management and the Shared Responsibility Model

Balancing Risk and Reward

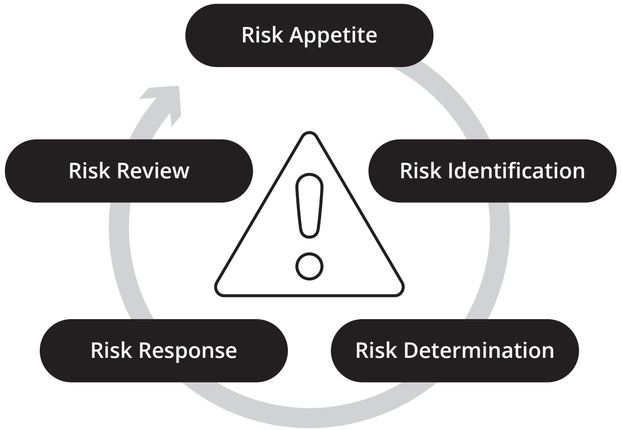
Every business strategy involves risk. Risk must be recognized and then managed.



- Organizations need to understand where significant risks arise.
- Then assess the probability and likely impact of the risks.
- Decide whether the potential rewards make the risk worth taking.

The Risk Management Cycle

Risk management is not a one-off exercise. It is an ongoing process cycle of risk appetite, identification, determination, response, and review.



Cloud Risk and the Shared Responsibility Model

Responsibility	IaaS	PaaS	SaaS
Governance Risk and Compliance	●	●	●
Data Security	●	●	●
Application Security	●	●	◪
Platform Security	●	◪	○
Infrastructure Security	◪	○	○
Physical Security	○	○	○

● Organization responsibility ○ Provider responsibility

- Many organizations underestimate the risk responsibilities that they own or share with cloud service providers.
- Risk and the responsibility for mitigating such risk will vary depending on the cloud deployment model.
- The shared responsibility model sets out the responsibilities between the cloud service provider and the customer. Typically, the cloud service provider is responsible for the security of the cloud (the infrastructure) and the cloud customer responsible for security in the cloud (data and resource configuration).

ASSESSMENT

Define Risk Appetite

Risk can come from internal or external environments and can impact strategic, financial, operational, compliance, and security objectives. It is critical to identify risks that will affect the performance and achievement of the cloud computing strategy and thereby the achievement of business objectives.

1. Organization determines the areas of principal risk in relation to its cloud governance strategy.

2. Organization defines its risk security appetite and tolerance for data in the cloud.

Risk appetite provides a framework which enables organizations to make informed management decisions. Defining risk appetite and tolerance sets the boundaries of how much risk an organization is willing to take in the pursuit of its strategic objectives. **The benefits of adopting a risk appetite:**

- Supports performance improvement
- Focuses the organization on priority areas
- Reduces uncertainty
- Informs spending and resource prioritization
- Improves governance mechanisms

Risk Appetite

Target level of risk an organization is willing to take on to actively pursue its strategic objectives.

Risk Tolerance

The degree of variance from its risk appetite that the organization is willing to tolerate.

3. Organization develops statement to describe its optimal and tolerable security position for different types of data; e.g., personal data, payment data.

ASSESSMENT

Define Risk Appetite

1 Within the information security context, identify the risks that threaten confidentiality, integrity, or availability of data. Threat describes the source of risk. Vulnerability is a weakness that can be exploited by a threat.

RISK IDENTIFICATION

Threat | Vulnerability

2 Risk determination combines the likelihood of a threat with the impact should a vulnerability be exploited, and the results are shown in a risk matrix.

RISK ANALYSIS

Likelihood | Impact

3 Mapping the risk's impact against its likelihood provides the level of risk. For example, if a risk is assessed as having a high likelihood and a major impact, it is a assigned a risk score of 16.

Impact →

Likelihood ↑

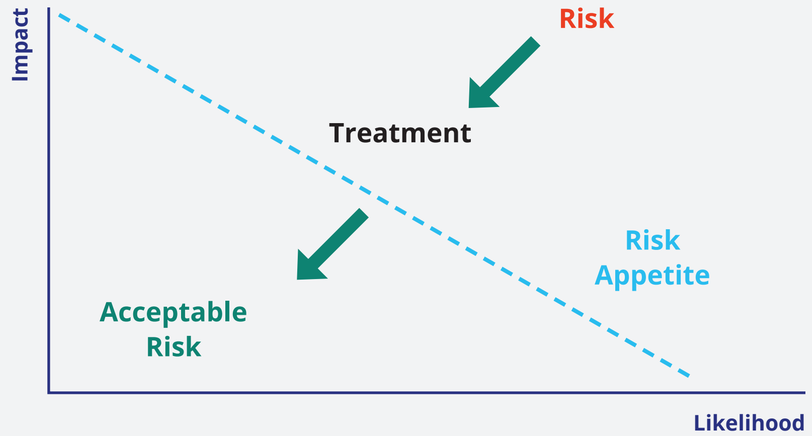
	Negligible	Minor	Moderate	Major	Severe
Certain	5	10	15	20	25
Likely	4	8	12	16	20
Possible	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5

4 A risk matrix focuses management on the higher-level risks and to evaluate them against the risk acceptance criteria.

Tolerance Level	Risk Treatment
High Risk (16-25)	Risks at this level are so significant that risk treatment is mandatory.
Medium Risk (6-15)	Risks at this level require consideration of costs and benefits (rewards) to determine what if any treatment is appropriate.
Low Risk (1-5)	Risks at this level are so small that no risk treatment is needed.

ASSESSMENT

Risk Response



Risk response will be based on the outputs of the risk evaluation, taking into account the severity of the risk, where it sits in relation to your risk criteria, the organization's risk appetite, and the availability of treatment options for the risk.

Develop a risk treatment plan to formally document the identified risks, the chosen treatments and how the treatments are to be implemented. Include responsibilities, timelines, and reporting metrics.

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived from enhancing the achievement of objectives against the costs, efforts, or disadvantages of proposed actions.

SIX STAGE PLAN

1	Prioritize actions
2	Evaluate treatment options
3	Conduct cost-benefit analysis
4	Select treatment
5	Assign responsibility
6	Implement treatment

RISK TREATMENT OPTIONS

Tolerate	An informed decision to do nothing. Applied to risks where the cost of treatment outweighs the business benefits or they are benign in terms of impact.
Avoid	Elimination of the risk in its entirety. Done by stopping the underlying activity or getting rid of the asset in question.
Reduce/Mitigate	Application of treatment measures to reduce the impact of the risk or its likelihood or reduce both.
Transfer	Sharing the risk with other parties. Usually relevant to risks that can be measured and take one of two forms — either insurance or contractual obligations with a third party.

ASSESSMENT

Risk Review

Risk Monitoring and Reporting

Ongoing monitoring supports an understanding of whether and how the risk profile is changing and the extent to which treatments are operating as intended.

Reporting information should help management to assess whether decisions and activities are being made within the organization's risk appetite and to decide whether any changes are required to strategy and objectives, risk appetite, policies, and procedures.

Governance, risk, and compliance solutions can help to organize and evaluate risk information, track incidents, measure risk factors, and modify operations to align with policies and regulations.

ASAPCLOUD

Customer:
Municipality of Houten

Parter:
ASAPCLOUD

Industry:
Partner Professional Services

Size:
Small. 1-50 employees

Country:
Netherlands

Products and services:
Azure Arc; Azure Monitor; Azure Automation; Azure Policy; Azure Security Center

READ FULL STORY HERE

Microsoft

"Since its implementation in Houten, the solution has increased compliance so much that today more than 90% of all available security controls are in place. We've gained a lot of self-assurance"

—Eric Surstedt, Team Leader for IT for the municipality of Houten

Situation:

The municipality of Houten, in the Netherlands, lost two of its technology experts and was beginning to run into important compliance issues.

They were in a dire situation due to aging on-premises infrastructure, low visibility into maintenance standards, and increasing ransomware threats.

An initial inspection of Houten's regulatory compliance and security procedures revealed a dramatically low 25 percent compliance rate.

Solution:

Knowing that many municipalities like Houten are reticent to move their workloads to the cloud, ASAPCLOUD created a hybrid cloud solution that provides on-premises infrastructure the security and compliance benefits of Azure, without committing to a cloud migration.

Though Houten's datacenters remain on-premises, ASAPCLOUD was able to implement a new Azure Arc solution with a single control plane. This gave Houten access to robust security and monitoring that was previously out of reach.

Impact:

Thanks to Azure Arc, Azure Monitor, Azure Automation, Azure Security Center and Azure Policy, ASAPCLOUD was able to simplify and automate the municipality of Houten's IT management, increasing not only security and compliance, but also the ability of Houten to focus on delivering the core services its citizens depend on.

Having seen how Azure Arc and the security & compliance features of Azure can benefit an on-premises infrastructure, their mind is at ease due to better controls & transparency across their environment. They are now evaluating migrating some workloads to Azure to take their evolution even one step further.

Guidance to Achieving Good Cloud Data Governance

1 

Business-aligned: The data governance framework is tailored to the organization's needs and strategic objectives and is compatible with the cultural context.

2 

Iterative: Start small, gather feedback, and adjust accordingly. Repeat the process and allow the framework to scale gradually.

3 

Measured: Set SMART goals with clear metrics to assess whether the governance program is achieving desired outcomes.

4 

Sponsorship: Senior leadership display strong, explicit, and ongoing commitment for data governance, including budget and resource needs.

5 

Cross-functional: Broad representation from corporate, departmental, and IT management helps to strengthen communication and advocacy for the framework across the organization.

6 

Visibility: Data discovery and classification are foundational to any data governance, privacy, and security program and to provide that single source of data truth.

7 

Risk: Align risk frameworks and tolerances with data strategy in the cloud. Properly categorize and evaluate risks in terms of both potential negative impact and positive opportunity.

8 

Technology: Identify and prioritize focus areas for improvement and automation. Ensure data governance processes are well-defined before implementing technology.

9 

People: A workforce strategy is in place to address data skills and capability gaps. Educate workforce in data governance polices, procedures, and best practice.

Message from the sponsor

84% of European organizations operate hybrid & multi-cloud architectures, yet 42% of those organizations have not yet adopted formal risk management and hybrid multi-cloud governance processes.

Enabling digital transformation and creating business value while effectively managing risk is top of mind for organizations. Navigating a cloud journey with complex regulatory requirements and a dynamic threat landscape is already challenging. When combined with an operating environment including hybrid environments at the edge, multi-cloud strategies, and on-premises datacenters it can seem overwhelming.

By adopting cloud & governance frameworks this journey can be simplified, and including best practices for discovering & classifying data for risk assessment. Organizations can then create the right hybrid & multi-cloud operating model for their unique requirements.

- **Microsoft's Hybrid Cloud Adoption Framework** provides implementation guidance, best practices & tools including on-premises and multi-cloud architectures.
- **Azure Purview** is a unified data governance service that provides automated data discovery & classification on-premises, multi-cloud and SaaS sources. Azure Purview can then create a unified map of the data estate and provide insight into the location & movement of sensitive data no matter where it resides.
- **Azure Arc** unifies on-premises, hybrid and cross-cloud infrastructure into a single control plane for operations, management, faster app development enabling "compliance-as-code" with predefined blueprints.

Learn more at **aka.ms/hybridcloudgovernance**

Microsoft

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com