

A guide for IT professionals

IMPLEMENTING THE HYBRID CLOUD

A guide for IT professionals

IMPLEMENTING THE HYBRID CLOUD

In this book:

- › Getting Started
- › Planning
- › Deploying
- › Privacy & Security

Cloud technology is maturing and advancing rapidly.

And for schools today, hybrid cloud computing optimizes that technology, leveraging the complementary benefits of both the private and the public cloud. With cost-efficiency, security, and much more, hybrid cloud is moving educational organizations ahead.

GETTING STARTED



WHAT EDUCATION IT NEEDS TO KNOW

Smart decisions for smarter schools.

School systems operate in a regulated environment. They use and store a wide range of highly sensitive data. They deal with minors. Given this landscape, **cloud computing presents school systems with new questions and concerns relating to data privacy, security, and regulatory compliance.**

In the rush to embrace cloud computing, it can be easy to give short shrift to these matters—or to assume that a cloud service provider will take care of security. Either course of action increases the risks, threatens to expose sensitive data, damages trust in the school system, and can incur fines from regulatory agencies.

In this book:

- ▶ Getting Started
- ▶ Planning
- ▶ Deploying
- ▶ Privacy & Security



From data privacy and security to compliance, Intel helps schools

**TAKE ADVANTAGE
OF CLOUD
COMPUTING,
THE SMART WAY.**

MAKING THE MOST OF TECH IN THE CLASSROOM

In this book:

- ▶ Getting Started
- ▶ Planning
- ▶ Deploying
- ▶ Privacy & Security

A long-term cloud strategy is critical.

When it comes to realizing the benefits of cloud computing, and determining the optimal cloud model for your organization, **the first step is to develop a cloud strategy** that includes on- and off-premise solutions that help you meet both compliance needs and educational goals. Having that strategy in place will put your organization on a path to cloud maturity—with a flexible cloud environment that scales as demand grows.

A cloud strategy helps schools

- ✓ Reduce costs
- ✓ Stretch IT capabilities further
- ✓ Deliver the latest content quickly

HYBRID CLOUD ARCHITECTURE

The best of both worlds.

Hybrid clouds combine two or more cloud deployment models—typically private and public—to enable data and application portability.

The National Institute of Standards and Technology (NIST) has described the essential characteristics of cloud computing as broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling. These characteristics can be achieved using three major cloud service delivery models together: SaaS,¹ PaaS² and IaaS,³ all of which can be implemented using several deployment models: public, private, hybrid, or community clouds.

In this book:

- ▶ Getting Started
- ▶ Planning
- ▶ Deploying
- ▶ Privacy & Security



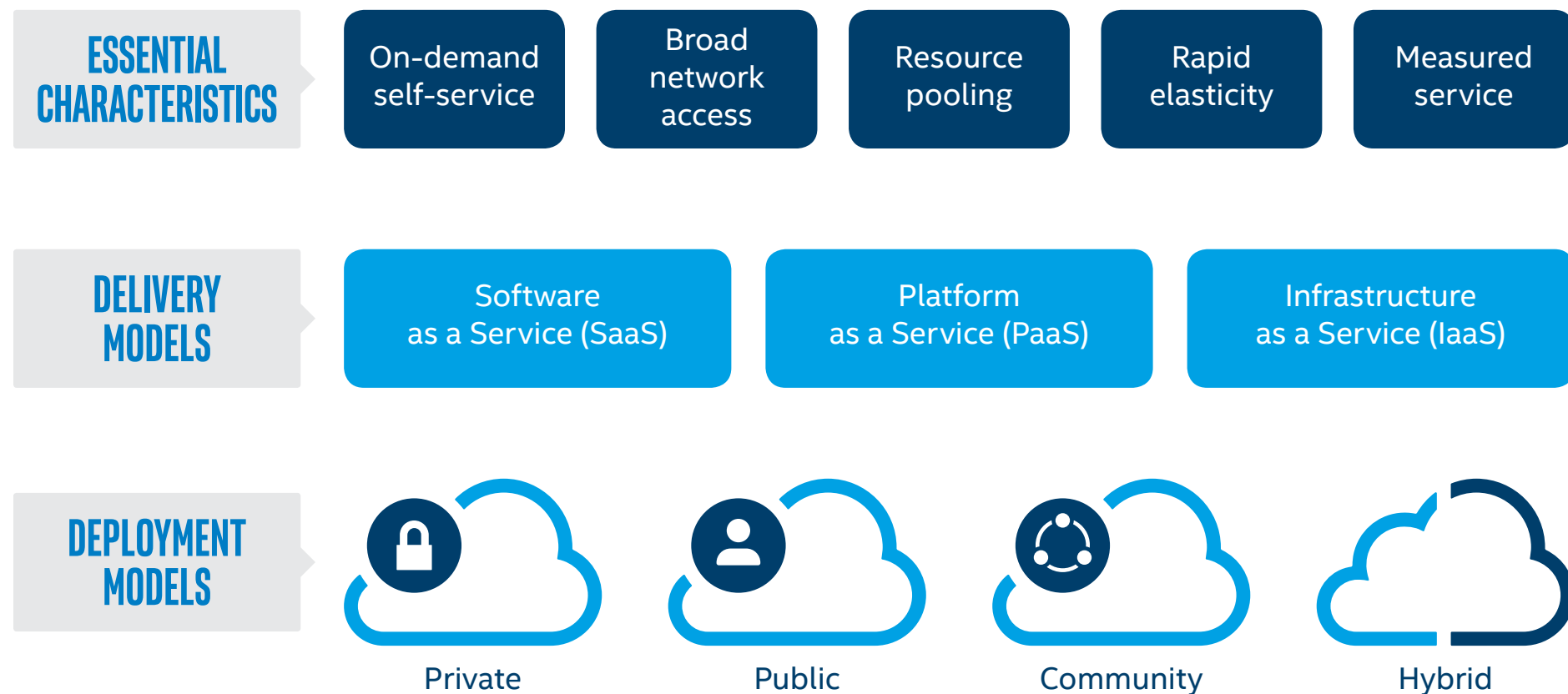
THE CLOUD COMPUTING MODEL

In this book:

- ▶ Getting Started
- ▶ Planning
- ▶ Deploying
- ▶ Privacy & Security

The cloud service and deployment models as defined by the National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology Special Publication 800-145 (September 2011). <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>



PLANNING YOUR CLOUD STRATEGY



GET TO KNOW THE CLOUD

In this book:

- › Getting Started
- › **Planning**
- › Deploying
- › Privacy & Security

Important terms and concepts.

CLOUD BURSTING

An application that runs in a private cloud or data center, but “bursts” to a public cloud when the demand for computing capacity increases.

PLATFORM AS A SERVICE (PAAS)

A cloud service model that delivers the hardware and software tools required for application development, including infrastructure and an operating system.

INFRASTRUCTURE AS A SERVICE (IAAS)

The most basic cloud service offering, IaaS provides virtualized computing resources (servers) on demand.

SOFTWARE AS A SERVICE (SAAS)

Software applications that are available through the cloud instead of requiring installation and running locally.

PLAN A CLOUD STRATEGY

Start by developing a strategy document that includes the following:

- ✓ High-level teaching and learning goals
- ✓ A client device plan (for example: laptops, All-in-Ones, 2 in 1s, and Chromebook* devices)
- ✓ Defined implementation phases
- ✓ A monitoring and management plan
- ✓ Workload ID and cloud migration timeline
- ✓ Security and compliance considerations
- ✓ An IT and education partnership plan
- ✓ Cloud architecture definition
- ✓ Budget considerations

In this book:

- Getting Started
- **Planning**
- Deploying
- Privacy & Security



BUILD A CLOUD STRATEGY

In this book:

- › Getting Started
- › **Planning**
- › Deploying
- › Privacy & Security

A close examination will help smooth the transition.

A move to cloud services delivery will impact existing processes and education goals. Consider categorizing workloads based on diverse infrastructure needs.

STANDARD

Includes productivity applications and noncore workloads and applications used daily.

For example:
email, word processing, spreadsheets, and presentations.

STRATEGIC

Includes core applications and workloads that create value for and differentiate the school or district.

For example:
student information systems, grading and assessment applications, and administrative software.

NOVEL

Includes applications and workloads that drive innovation and create new opportunities for the school or district.

For example:
collaboration, creativity applications, and analytics.

CHOOSE A CLOUD DELIVERY MODEL

In this book:

- › Getting Started
- › **Planning**
- › Deploying
- › Privacy & Security

Find what fits.

The best cloud delivery model for a school system will match workloads to environments in order to **deliver the services that administrators, students, and teachers need.**

To determine the right model, consider the factors specific to the facilities and campus, as well as the education and administrative needs. For example: demand and scale, security requirements, and service level expectations.



SECURE YOUR CLOUD INFRASTRUCTURE

In this book:

- ▶ Getting Started
- ▶ **Planning**
- ▶ Deploying
- ▶ Privacy & Security

Three steps to security.

Look for architecture in your off-premis deployments that enables a *root of trust*—a set of functions built into hardware that helps keep the server or device platform safe against cyberattacks, and confirms its integrity when it boots. And always ensure that your data is encrypted and housed in the right location required by compliance regulations. The following principles will help secure cloud infrastructure and protect data.

SECURE THE RESIDENCE

Understand where data is being stored and accessed.

SECURE THE MOVEMENT

Understand the networks through which data is being disseminated.

SECURE THE METHOD

Understand how data is being transmitted through networks to the storage points.

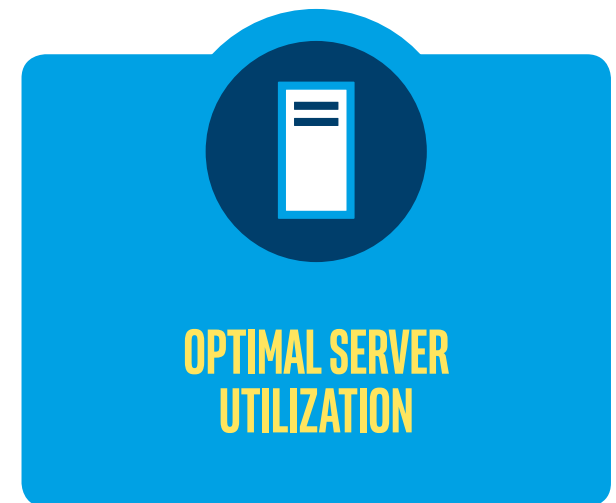
CREATE A ROADMAP

In this book:

- › Getting Started
- › **Planning**
- › Deploying
- › Privacy & Security

Assessing status.

Are you running one application on one server? Or have you taken the next step and started virtualizing your servers to improve efficiency? **After assessing the current status, create a basic roadmap for the cloud strategy** by outlining the service delivery vision against three constraints:



MOVE TO THE CLOUD

Changing technology, changing roles.

A move to cloud computing can have **a positive impact on existing school systems.**

- ✓ Shifting from manually provisioned to automated cloud infrastructure frees up IT staff to focus on classroom innovation.
- ✓ Enabling IT resources to act as a service broker will drive education goals and support office processes.
- ✓ Evolving from supporting static services to deploying dynamic services gives teachers and administrators the flexibility to try different cloud software on a pay-as-you-go basis, eliminating licensing commitments.

In this book:

- › Getting Started
- › **Planning**
- › Deploying
- › Privacy & Security

BEFORE CLOUD	AFTER CLOUD
Manual	Automated
IT resources	Service broker
Static	Dynamic

DEPLOYING THE HYBRID CLOUD



TECHNICAL CONSIDERATIONS

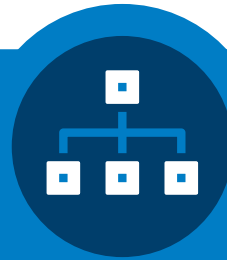
In this book:

- › Getting Started
- › Planning
- › **Deploying**
- › Privacy & Security



ACCESS

School internet access is <10%⁴ in some developing countries. While most US schools are connected, many lack high-speed connectivity.⁵



INTEGRATION

Spinning up VMs for IaaS or IaaS/PaaS combinations will ideally be the same for private *and* public clouds



PORTABILITY

A hybrid cloud infrastructure must support the dynamic movement of VMs across both cloud environments



MANAGEMENT

Visibility into system health across clouds is critical, as is the ability to ensure service availability to track against third-party SLAs



PROTECTION

Data security, compliance, and privacy rules must be maintained when moving data into public cloud environments.

CLOUD SERVICE MODELS

In this book:

- › Getting Started
- › Planning
- › **Deploying**
- › Privacy & Security

Deploying and maintaining hybrid cloud.

The goal of hybrid cloud computing is to create an open, extensible cloud ecosystem that ties an educational system's public and private cloud services together. Open standards are key when creating such an ecosystem. The Open Data Center Alliance has defined requirements for usage models in each cloud service layer in order to achieve interoperability and interconnectivity.

IAAS PORTABILITY

Moving physical or VM instances or images between environments over short or long distances while maintaining manageability, availability, security, and performance.

PAAS INTERCONNECTION & APPLICATION PORTABILITY

Moving applications between different PaaS environments—development and runtime—with cloud-aware applications that maintain attributes such as feature sets, configurability, and orchestration.

SAAS INTERCONNECTION & PORTABILITY

Connecting or transferring functionality and information via SaaS applications and creating mash-ups from multiple SaaS and non-SaaS applications via interfaces that exchange data smoothly.

THE CLOUD MANAGEMENT PLATFORM (CMP)

All the tools, all in one place.

A CMP is integrated software that simplifies management of complicated IT environments, delivering service quality, security, and availability for workloads running in these cloud environments. CMP offerings vary widely in terms of platform maturity, architecture complexity, and capabilities. Your choice of platform can simplify the management, automation, and orchestration of combined private and public clouds.

At minimum, a CMP should provide direct user access to the system, self-service capabilities and interfaces, a workflow engine, automated provisioning, and metering and chargeback functionality.

In this book:

- › Getting Started
- › Planning
- › **Deploying**
- › Privacy & Security

THE HYBRID CLOUD OFFERS:

- Performance and capacity management
- Interoperability between private and public IaaS offerings
- Connectivity to and management of external clouds
- Application life-cycle support
- Back-end service catalogs
- Integration with external enterprise management systems

CLOUD-AWARE APPLICATION DEVELOPMENT

In this book:

- Getting Started
- Planning
- **Deploying**
- Privacy & Security

Design considerations.

To prepare your organization for a hybrid cloud now, evaluate applications with capabilities that will minimize portability issues down the road. Cloud-aware application development can take full advantage of underlying cloud infrastructure for improved scalability, performance, and resiliency.



PRINCIPLES FOR CONSIDERATION

In this book:

- Getting Started
- Planning
- **Deploying**
- Privacy & Security

1 Treat everything as a service. Application capabilities should be partitioned into granular components that can be implemented, tested, and scaled separately.

2 Use RESTful APIs. RESTful APIs, or representational state transfer APIs, enable easy reuse and scaling of application capabilities, and shield applications from underlying technology implementations.

3 Separate compute and persistence. Store nothing locally on the compute instance that runs the cloud application; separation provides deployment and scaling flexibility.

4 Design for failure. Though we aim for zero failure, sometimes components fail, services become unavailable, and latencies increase. But by designing applications that can survive failure gracefully, we enhance UX.

5 Architect for resilience. An architecture designed with a focus on the mean time to recovery (MTTR) accepts imperfection and enables rapid identification and resolution of problems when they occur.

6 Operationalize everything. All services should be easy to maintain and troubleshoot. Instrumenting, logging, and analyzing application behavior will lead to operational improvements.

7 Implement security at every layer. Perimeter security isn't enough. A public cloud requires a comprehensive approach: encrypted transport into the cloud, secure coding and access control inside applications, and encryption at rest. The security of every API as well as all data should be tested and analyzed.

PRIVACY AND SECURITY



HYBRID CLOUD SECURITY

In this book:

- › Getting Started
- › Planning
- › Deploying
- › **Privacy & Security**

Key considerations in protecting student data.

In order to successfully combine cloud environments, explicit attention must be paid to security. For educational systems trying to meet both community and regulatory privacy demands established for student data, these issues can be particularly challenging. **It is imperative that schools not only create security policies, but also continually monitor and enforce these policies across cloud environments.**



5

See the following page for **FIVE IMPORTANT GUIDELINES** to help ensure a secure hybrid cloud environment.

PRINCIPLES FOR CONSIDERATION

1 Maintain your most sensitive workloads on premises.

In order to optimize control, keep core systems—such as those that contain personally identifiable student data—behind an in-house firewall.

2 Integrate security into every layer of the cloud.

Assign security policies for infrastructure and applications to specific VMs based on function. These policies are automatically assigned when that VM is provisioned.

3 Build security into server and client hardware.

Client devices and servers provide hackers with potential targets and access points to cloud resources. Intel®-based devices—and servers with built-in security features and data encryption—can enhance security.

4 Deploy antivirus software.


Protect yourself. Stealthy attacks on complex hybrid cloud environments are difficult to detect with traditional antivirus products. Safeguard against cybercriminals' rootkit attacks that infect system components, and hide the malware that spreads throughout a cloud environment.

5 Protect edge systems.

Web, portal, and email servers; bridges; routers; and other components that interact inside and outside the organization are known as edge systems, and they represent a growing attack target.

In this book:

- Getting Started
- Planning
- Deploying
- **Privacy & Security**



Technology is transforming education, from the classroom to the data center. Intel® provides guidance and resources to help make sense of it all—from simplifying implementation and advancing projects, to protecting school data across cloud environments.

For more information and resources,
visit [intel.com/educloud](https://www.intel.com/educloud)

¹ SaaS: Software applications are made available through the cloud instead of installed and run locally.

² PaaS: A cloud service model that delivers the hardware and software tools required for application development, including infrastructure and an operating system.

³ IaaS: The most basic cloud service offering, which provides virtualized computing resources (servers) on demand.

⁴ Final WSIS Targets Review: Achievements, Challenges and the Way Forward. International Telecommunications Union (2014). itu.int/en/ITU-D/Statistics/Documents/publications/wsisreview2014/WSIS2014_review.pdf

⁵ When Students Can't Go Online. The Atlantic (March 13, 2015). theatlantic.com/education/archive/2015/03/the-schools-where-kids-cant-go-online/387589/

* Other names and brands may be claimed as the property of others.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2016 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others. 1115/SK/CC/MB/PDF 333469-001US

