BT Compute. Services that adapt

BT Cloud Compute Security

Together, we make the cloud secure

This white paper describes the security perspective of IaaS (Infrastructure as a service) for BT Cloud Compute

Author: Charles Fox, Enterprise Architect Cyber Warfare, BT

Table of contents

1. Introduction

Our expertise. Your ownership. World-leading cloud security

As the popularity of BT cloud services grows, our approach to helping you keep your data secure becomes ever more proactive and innovative. Always remember that real security in the cloud is the result of a joint effort: it involves you as much as us.

This document makes you aware of the threats every cloud user potentially faces. We'll introduce you to advanced security measures to counteract them, and the policies and procedures we have in place to help you safeguard your valuable information.

We'll also make you aware of the responsibility you must necessarily take for the protection of your own data.

You can then enjoy not only the freedom of control, but also the reassurance of security, from one of the world's leading cloud service providers.

Together, we can make sure your company enjoys all the advantages and power of the cloud, without the worry for your data's safety.

When choosing your cloud service, we'll advise you where the responsibilities for your data's security lie – both on our side and yours – so that we join forces to successfully guard against error and fight malicious intent.

Your role in your security

If you're considering cloud services today, we encourage you to ask some fundamental questions, and understand who needs to take responsibility for security. You may ask:

- *Who's really responsible for my data?* The short answer is: you are. As the data owner, it's your responsibility, not that of your Cloud Service Provider (CSP), to secure your data.
- *Where's my data?* Your data in the cloud must reside in a physical location. Many don't realise this, so make sure you discuss with your CSP which Country / Countries your data will reside in. Be aware that different countries have different requirements and controls placed on access
- *Who has access to my data and my code?* Insider attacks are a huge risk, and a potential hacker can be someone with approved access to the cloud. You need to know who's managing your data and the types of control applied to these individuals
- *What is the current maturity and long-term viability of my chosen CSP?* How long have they been in business? What's their track record? Are they operationally effective and secure? If they go out of business, what happens to your data?
- *What happens if there's a security breach?* What support will you receive from the provider? Many claim to be hack proof, but cloud-based services are an attractive target to determined hackers
- *What is the disaster recovery/business continuity plan?* Remember your data is physically located somewhere, and all physical locations face threats such as fire, storms, natural disasters, and loss of power. So how will your CSP respond, and what guarantee of continued services do they promise?

We'll address all these questions during the course of this document.

BT Cloud Compute services: security in safe, trusted hands

With BT Cloud Compute, you get highly advanced self-service IaaS capability, allowing you to rapidly build, deploy and manage your own virtual infrastructure and cloud solution, including virtual machines, network, storage and security from the cloud.

In the IaaS service model, you have control over operating systems, storage, deployed applications and limited control of selected networking components such as host firewalls.

With any cloud service, it's important to remember how security responsibilities must be shared:

- Secure *delivery* depends on the *CSP's* (ie, BT's) personnel, processes and technologies
- Secure *usage* of cloud services remains *your* responsibility.

The following table illustrates how we need to share responsibility for security in the BT Cloud Compute IaaS context.

Layer of the Cloud	Client Security Responsibility	BT Cloud Compute / CSP Security Responsibility
Data	🟦	
Interfaces (APIs, GUIs)	🟦	
Applications	🟦	
Operating Systems (OS)	🟦	
Virtual Machines	🟦	
Virtual network infrastructure	🟦	
Templates used to create VMS	For customer provided templates	For provider supplied standard templates
Virtual Firewall	For configuration and useage	For provision of secure software. e.g. suitable EAL
CloudPortal and API	For usage	🟩
Hypervisors		🟩
Processing and Memory		🟩
Data Storage (hard drives, removable disks, backups, etc.)		🟩
Network (interfaces and devices, communications infrastructure)		🟩
Physical facilities / data centres		🟩

Figure 1-1 – Security responsibilities / ownership as a function of IaaS layers

BT Cloud Compute does provide security tools that allow you to set up and control sub-nets and dedicated instances to segment your data in the multi-tenanted cloud environment.

But it's your responsibility to use those tools to ensure your data is protected.

This is significant because BT Cloud Compute doesn't currently provide data encryption as part of our generally available IaaS productised service.

Your risk assessment must ask if additional data segmentation controls are required, like performing your own encryption services for data stored on the cloud.

Over the next few pages, we're going to look at potential threats to security and show you how BT's Cloud Compute services deal with the following concerns:

- Cloud vulnerabilities
- Operational security
- Personnel security
- Supply chain assurance
- Physical security
- Business and continuity management
- Regulatory and legal requirements
- Identity and access management
- Data and service portability
- Supply chain assurance
- Physical security
- Business and continuity management
- Regulatory and legal requirements.

2. The cloud: vulnerable, without protection

By understanding the vulnerabilities of the cloud and associated threats, you can better approach your risk assessments.

Cloud computing is based on a virtual environment, so the threats that apply to virtualisation also apply in the cloud computing space.

Extending virtualisation to the cloud causes your enterprise's network perimeter to become more elastic. And as cloud computing expands to cover data stored in private and public clouds, and on numerous roaming mobile devices, new threats are inevitable, as you can see here:

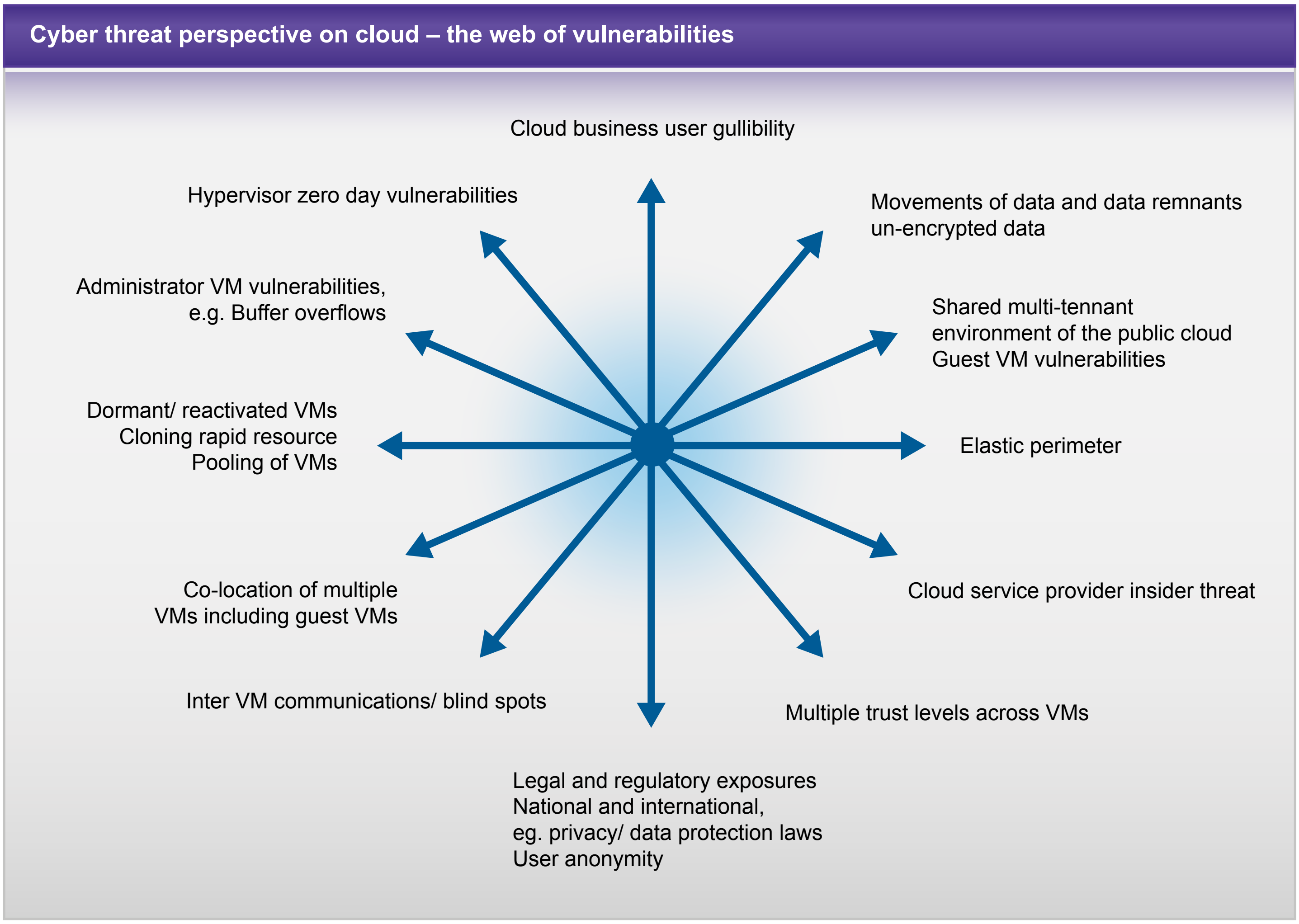

Cyber threat perspective on cloud – the web of vulnerabilities
Cloud business user gullibility
Hypervisor zero day vulnerabilities
Movements of data and data remnants un-encrypted data
Administrator VM vulnerabilities, e.g. Buffer overflows
Shared multi-tennant environment of the public cloud Guest VM vulnerabilities
Dormant/ reactivated VMs Cloning rapid resource Pooling of VMs
Elastic perimeter
Co-location of multiple VMs including guest VMs
Cloud service provider insider threat
Inter VM communications/ blind spots
Multiple trust levels across VMs
Legal and regulatory exposures National and international, eg. privacy/ data protection laws User anonymity

Figure 1-2 – Cloud vulnerabilities

2.1 Virtualisation and Hypervisor-based attacks

These threats relate to attacks targeting the Hypervisor piece of software used extensively in the IaaS delivery model of cloud services.

By manipulating and controlling the Hypervisor on a multi-platform virtualised host, an attacker can control all hardware and software commands for every guest accessing the Hypervisor. Attacks include:

- Adding Trojans to the virtual machine that are passed down through the Hypervisor to the host machine
- Installing and running resident in ring 0 on the host
- Passing destructive microcode through the virtual CPU down to the physical CPU
- Manipulating the virtual machine management interface itself to bypass authentication between the guests and host
- Using the Hypervisor to gain access to the software network subsystem
- Placing both the guest and host network interfaces into promiscuous mode allowing sniffing of the host network transparently via the guest.

In section 3 of this document, we introduce you to the BT Cloud Compute perspective on Operational Security, and look at the BT Cloud Compute security controls used to counter Hypervisor threats.

2.2 Insider threats: across the CSP and your organisation

Cloud computing extends insider threats from your own organisation to include potential insider threats from employees and contractors of your chosen CSP.

A malicious insider threat to your organisation can be a current or former employee, contractor, or other business partner who has (or had) authorised access to your network, system or data.

This insider can intentionally exceed or misuse that access to negatively affect the confidentiality, integrity, or availability of your organisation's information or information systems.

In addition to possible malicious attacks from CSP personnel, there is always the likelihood of CSP staff errors (in misconfiguring a router, Hypervisor setup etc.) leading to serious customer service disruption.

Section 4 of this document introduces you to the BT Cloud Compute perspective on Personnel Security. We look at the BT Cloud Compute security controls used to counter these insider threats in sub-section 4.1.

2.3 Data movement and remnants

Data remnants are *'the residual representation of data that has been in some way nominally erased or removed. This residue may be due to data being left intact by nominal delete operation or through physical properties of the storage medium'.*

These can lead to inadvertent disclosure of your sensitive information, if the storage media is released unto an uncontrolled environment.

The real threat comes from your data being spread across multiple parts of the CSP's infrastructure, with fragments of data and their location not being fully known.

Public cloud platforms in particular depend upon transitory use, so virtual machine and data storage is continually being created and removed. This means it's very hard to effectively remove data – the default assumption is that there will be data 'remaining' in different media across the cloud platform.

Because cloud storage networks use shared resources, it's possible that data is spread across multiple storage platforms. So an attacker can link pieces of information together from multiple sources within the cloud platform.

Also if data is not deleted properly, fragments could be spread across your CSP's platform – only to be pieced together by the CSP administration team (malicious activity).

In section 3 of this document, we introduce you to the BT Cloud Compute perspective on Operational Security; sub-section 3.3 explores the BT Cloud Compute security controls used to counter data security threats.

2.4 Phishing attacks to compromise accounts

Cloud services are managed using traditional management portals. These are safeguarded by traditional security mechanisms like password, two-factor authentication etc.

However, threats to these 'all powerful' accounts represent an operational risk associated with the use of cloud services (though not specific to the cloud). One such example is the recent spate of phishing attacks on buyer/seller Amazon marketplace accounts, leading to the compromise of the linked account.

Spear phishing attacks will target not just CSP employees but also key account holders in your organisation.

Section 4 of this document gives our perspective on Personnel Security, and introduces the BT Cloud Compute security controls used to counter phishing and targeted phishing (i.e. spear phishing) threats in sub-section 4.1.

2.5 Legal and jurisdictional threats

While so called 'western' legal jurisdictions have formal processes for searching, there are many parts of the world where searching (particularly by government agencies), and obtaining data hosted on cloud platforms located in their country, is both uncontrollable and unpreventable (by the tenant and the CSP itself).

The recently extended US Patriot Act is worth mentioning here as an example of such a legal threat.

The CSP may move data or applications – perhaps for financial reasons – into jurisdictions that expose you to new opportunities for surveillance or interference, in such forms as regulation or taxation.

In addition, this could be in violation (or result in your organisation being in breach) of data protection legislation e.g. moving data outside of the EU. The threat posed by the US Patriot Act is again relevant here.

A sealed search warrant, served at the CSP, may allow law enforcement to search your systems while forbidding the provider from notifying you that a search has taken place.

Section 3 of this document outlines our approach to Operational Security; sub-section 3.3 looks at your responsibilities as the customer, as well as some BT Cloud Compute security controls used to manage legal and jurisdictional threats.

2.6 Threats to physical infrastructure

Here, the physical plant (data centre building, power, backup, air conditioning, etc.), computing hardware, and network may not be sourced or provisioned to your standards. It may be maliciously designed to subvert security, or possibly compromised by a third party. If so, the threat of a malfunction of your computer network equipment is highly likely.

In section 8 of this document, we introduce the BT Cloud Compute perspective on physical security.

2.7 Threats to shared infrastructure

When infrastructure is shared, you must be confident that mechanisms are in place to protect your data from other customers.

The sharing of resources (a crucial part of CSP delivery model, linked to the financial advantages of cloud computing) may also have a negative impact on availability.

If you are able to be identified by the resources you share with other customers, this can affect your reputation (via loss of confidence in the CSP's ability to provide secure multi-tenancy isolation).

As an example of a threat from another tenant, a malicious customer may pierce hardware, software or network isolation boundaries to compromise the confidentiality, integrity, availability of your data, code or communications (network or application resources).

Also, many customers recycle IP addresses within their account, using standard names for data volumes mounted using NFS, for example, /app and /data. If you use internal IP addresses as opposed to host names, then the mounting of volumes containing sensitive data can occur.

Section 3 of this document explores the BT Cloud Compute perspective on operational security.

2.8 In short: a summary of threats

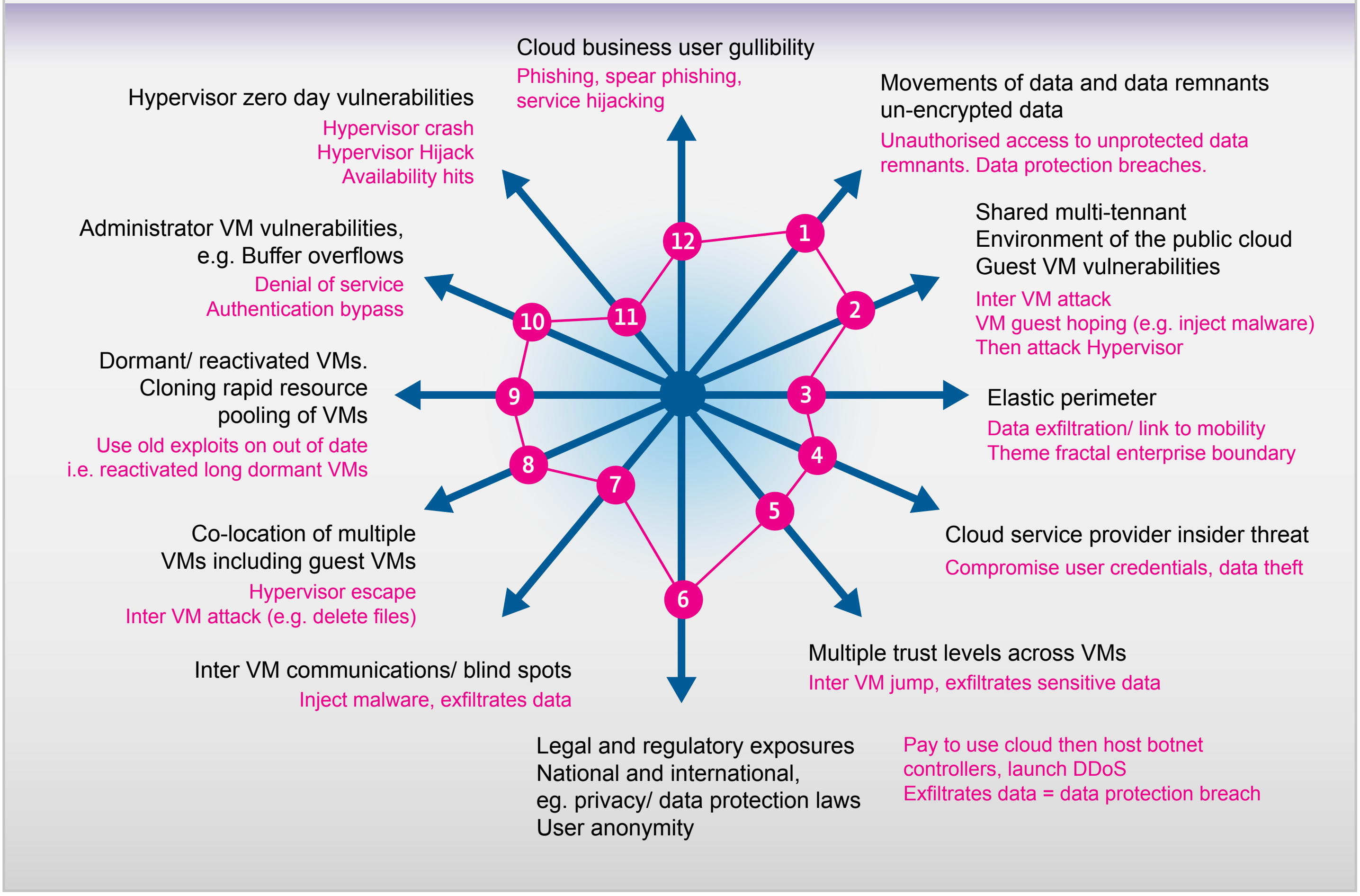
As we've already mentioned, cloud computing is founded on a virtual environment. The threats that apply to virtualisation also apply in the cloud computing space.

Extending virtualisation to the cloud – with data stored in private and public clouds and on mobile devices – causes your enterprise network perimeter to become more elastic, and therefore new threats to be introduced.

The use of standard ports such as 80 (http) and 21 (ftp) brings with it significant threats. There are many robots looking for insecure http, ftp and smtp ports; once compromised, the virtual machine can be used as a relay.

Over the next few pages, you'll see BT's own perspective on these threats, and how a correct and vigilant use of Cloud Compute – including an awareness of the ownership of security responsibility – enables you to stand firm against malicious intent.

Cyber threat perspective on cloud – the web of threats



Cloud business user gullibility
Phishing, spear phishing, service hijacking

Movements of data and data remnants un-encrypted data
Unauthorised access to unprotected data remnants. Data protection breaches.

Shared multi-tennant Environment of the public cloud Guest VM vulnerabilities
Inter VM attack
VM guest hoping (e.g. inject malware)
Then attack Hypervisor

Elastic perimeter
Data exfiltration/ link to mobility
Theme fractal enterprise boundary

Cloud service provider insider threat
Compromise user credentials, data theft

Multiple trust levels across VMs
Inter VM jump, exfiltrates sensitive data

Pay to use cloud then host botnet controllers, launch DDoS
Exfiltrates data = data protection breach

Legal and regulatory exposures
National and international,
eg. privacy/ data protection laws
User anonymity

Inter VM communications/ blind spots
Inject malware, exfiltrates data

Co-location of multiple VMs including guest VMs
Hypervisor escape
Inter VM attack (e.g. delete files)

Dormant/ reactivated VMs. Cloning rapid resource pooling of VMs
Use old exploits on out of date i.e. reactivated long dormant VMs

Administrator VM vulnerabilities, e.g. Buffer overflows
Denial of service
Authentication bypass

Hypervisor zero day vulnerabilities
Hypervisor crash
Hypervisor Hijack
Availability hits

Figure 1-3 – Cloud web of threats in summary

3. BT Cloud Compute: reassuring operational security

When choosing a CSP, you should look for some sort of reassurance regarding their current maturity, and long-term viability.

You will need to ask how long the provider has been in business and what sort of track record they have. You'll want to know they're operationally effective and secure. If they go out of business, you need to know what happens to your data.

You can choose BT Cloud Compute safe in the knowledge that we:

- Are part of the UK's Critical National Infrastructure,
- Are trusted to provide security to nine of the top fourteen UK banks, as well as the Ministry of Defence,
- Have global clients including Reuters, Credit Suisse, Unilever, PepsiCo and Phillips.

However, we should again emphasise that responsibility for your data security ultimately lies in your hands. The onus is on you to back up your data to ensure your business continuity.

Regardless of the stability and maturity of any IaaS cloud provider, real security comes from a joint appreciation and awareness of threats, and the role we must both play to effectively mitigate risk.

Ask what a CSP can do for your operational security

The operational software and hardware (i.e. the whole system) that a CSP uses to power your cloud platform must be developed and managed with security as a paramount concern: secure product management, secure default configuration and change management etc.

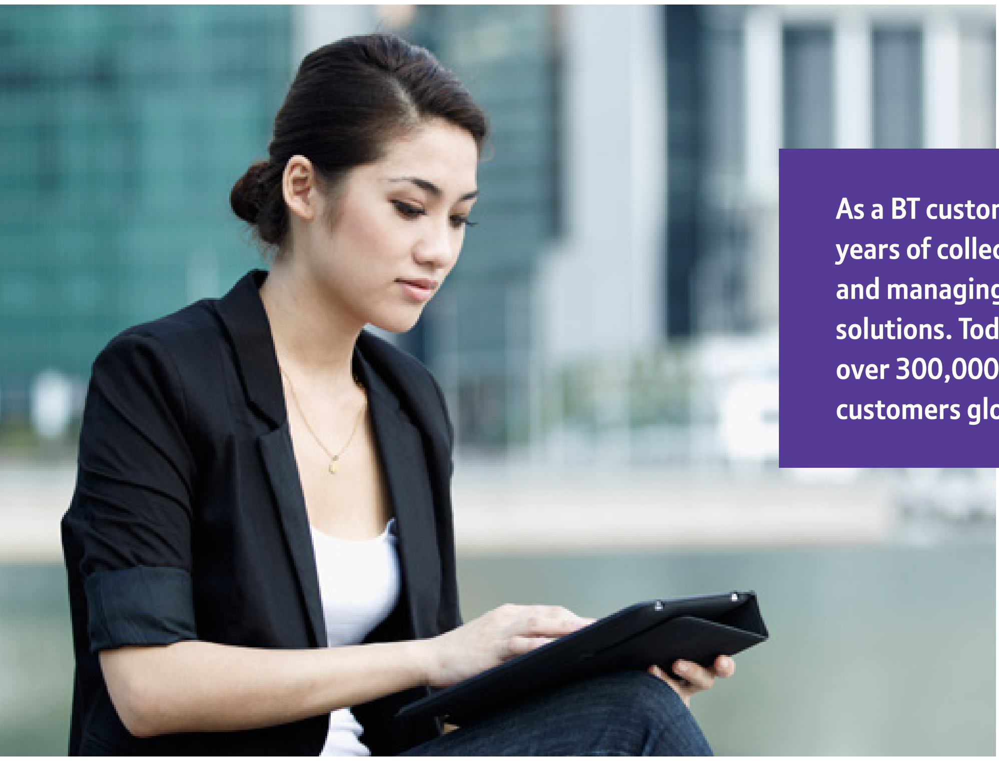
IaaS CSP developers must offer a configuration management system which:

- Controls changes to the cloud platform and management system during development
- Tracks security flaws
- Requires authorisation of changes
- Provides documentation of the change plan/request and its implementation.

This control also applies to the development actions associated with changes to the live platforms. The configuration management system should also be tested, to ensure the processes, governance and audit are validated.

What's more, for those CSPs operating and providing IaaS internationally, security compliance must be to international ISO standards.

These are the issues that BT Cloud Compute expertly addresses, giving you world-leading operational security in the cloud.



As a BT customer, you'll benefit from 30 years of collective knowledge in providing and managing security across network and IT solutions. Today, we monitor the security of over 300,000 devices for over 1,000 customers globally.

3.1 BT Operational Security Controls: ISO compliance

BT Cloud Compute conforms to ISO 27001. This is an internationally recognised information security standard designed around a set of security controls that, once implemented, provides you with solid assurance that your data is secure.

ISO 27001 requires us to demonstrate, through a series of external assessments, that we meet the requirements of over 130 security controls.

Additionally, we must also show a high level of security governance, especially in the areas of risk assessment and risk management.

This certification demonstrates to you that:

- We take information security seriously
- Our services follow the requirements of a known and respected standard
- Your data will be managed securely.

BT Cloud Compute: independently tested as secure

Beside operational security validation, CSPs should be able to demonstrate additional validation through third-party application penetration testing.

You could make an argument for sharing penetration tests with customers, because transparency builds trust. However, the counter argument says that sharing penetration tests introduces additional risk.

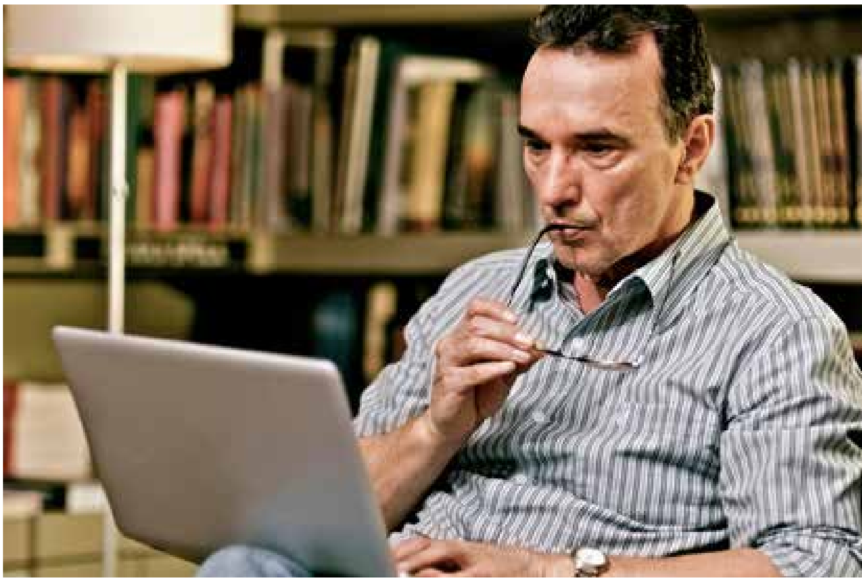
If, let's say, 'Bad Guys Inc' become a customer of the IaaS cloud service, they would also have knowledge of the penetration tests shared with them, and be in a position to exploit the information.

That's why, once a year, BT Cloud Compute employs third-party 'ethical hackers' to conduct formal penetration testing of our IaaS services.

Due to the concerns raised above, we never share testing information with our global customer base, although BT Compute does allow third-party black box pen testing of its IaaS services by its customers.

What's more:

- BT adheres to ISO/IEC 12207, the international standard for software life-cycle processes
- All BT Code is subject to change control; we have operated a formal change control to ISO standard for over 50 years
- Our 'Software Vaulting' policy means revisions can only be made after change control has been undertaken by the BT CAB (Change Control Approval Board), and there are lockdown periods where revisions cannot be made in case it places projects in jeopardy.



3.2 BT Operational Security Controls: addressing security incidents

You might ask what happens in the event of a security breach. And if a security incident occurs, what support will you receive from the cloud provider?

We've already mentioned that although some providers will claim to be hack-proof, cloud-based services are an attractive target to hackers. In response, BT has in place established policies and procedures that ensure the timely and thorough management of incidents according to priority.

BT Contractors, employees and third party users have a responsibility to report all information security events in a timely manner.

Every event is reported promptly either through the BT Cloud Compute Service Desk or the Portal in compliance with statutory, regulatory and contractual requirements.

BT Cloud Compute Service Desk

Our service desk is available to accept faults, support issues and general enquiries on a 24/7 basis, every day of the year. With regard to standard incident processes, we have a service level agreement of 99.95% for BT Cloud Compute and Private Compute services.

You should initially direct all your service issues to the Service Desk by either email or phone.

The BT Service Desk will:

- Offer you a consistent customer experience via our customer experience and quality call guidelines
- Provide a receipt and ownership point for your incident or support issues, and progress the issue appropriately
- Record all information in an appropriate incident handling system
- Give you an incident reference number, an indication of the priority assigned, the target clearance time, as well as confirming your update KCI (Keeping Customer Informed) frequency
- Undertake primary diagnosis, to ascertain the second or third-line support team able to fix the incident, as well as dispatching the case and monitoring its progress
- Take ownership of your problem until it's resolved, escalating assistance as appropriate
- Provide regular progress updates against standard KCI targets, or at intervals agreed with you
- Advise you of your problem's resolution,
- Confirm resolution of the problem to your satisfaction, providing details of the cause.

In the event of follow-up legal action against a person or organisation after an information security incident, BT follows proper forensic procedures, including chain of custody as required, for the collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.

In addition:

- BT Cloud Compute has mechanisms in place to monitor and quantify the types, volumes, and costs of information security incidents
- BT SOCs (Security Operations Centres) are located in the UK (3), EU (3), US (3), India (2), Australia (1) and Brazil (1), to provide support for standard portfolio, as part of redundant management architecture
- BT also operates a global NOC/SOC (a dedicated Network and Security Operations Centre) with geographically diverse secondary and tertiary sites. The NOC/SOC monitors all our products and services, resolving issues before they can have an impact on your security. You can also add your own monitors and see monitoring from our customer-accessible portal
- BT Compute provides an Open Source-based API for the monitoring elements of the platform, allowing the construction of custom probes and monitors. This provides you with a platform view and reporting capabilities specific to your needs
- All our command and control systems are fully logged and archived under our information management policy: eg. Firewall Logs are regularly catalogued and subject to HSM (Hierarchical Storage Management), and are ultimately held on offsite WORM media to ensure no attack surfaces are left in situ.

Not only that, BT Cloud Compute audit logs/retains:

- Privileged user access activities
- Authorised and unauthorised access attempts
- System exceptions
- Information security events, complying with applicable policies and regulations.

We review audit logs regularly, and file integrity (host) and network intrusion detection (IDS) tools to enable timely detection, investigation by root cause analysis, and fast response to incidents. What's more, physical and logical user access to audit logs is restricted to authorised personnel.

3.3 BT Operational Security Controls: addressing data security threats

Naturally, data confidentiality within cloud services is a fundamental concern: you need to be confident that only authorised users have access to your data.

Here, we must stress again that, as data owner, you are fully responsible for compliance – it's up to you, not the CSP, to secure valuable data.

Public cloud computing asks you to exert control, without ownership of the infrastructure, in order to secure your information through a combination of:

- Encryption
- Contracts with service-level agreements
- By (contractually) imposing minimum security standards on your provider.

To mitigate the risks associated with virtualisation and multi tenanted aspects, BT Cloud Compute offers you data segmentation controls to protect your data confidentiality, integrity and availability.

You and BT: a responsibility shared

While we are responsible for the security of the core IaaS infrastructure, ie. the basic networking, processing and storage services, you are responsible for network administration, server administration and data storage administration.

Your responsibilities include:

- Controlling network access (opening and closing of ports and protocols)
- The granting or denial of access at the server and service layer (the customer is responsible for the server and service configuration)
- Designing, implementing, maintaining and inspecting access control within the application
- Implementing failover and other redundancy solutions
- On-going monitoring for access, security and availability.

BT Cloud Compute employs layer 3 and/or layer 1 & 2 separation, depending on your security policies, and whether you select a public or private availability zone.

- Layer 3 uses routing tables to logically separate your traffic and data
- Layer 2 uses traditional VLAN constructs
- Layer 1 deploys physical separation.

If required, Layer 2 separation ensures that each private cloud customer's virtual hosts run on dedicated server equipment. This isolates you from contention or threats that are effectively 'in-house' in a multi-tenant cloud model.

If you choose a multi-tenanted deployment model, Hypervisor separation controls are performed, with Hypervisor's in-built functions controlling routing to and from individual virtual machines, via the use of IP name space separation and routing groups.

Protective network controls include the use of virtual appliance-based intrusion detection and prevention devices. These appliances act independently of the IaaS platform and their impartial presence allows for checks and balances to counteract design weaknesses in applications or systems.

Storage security is underpinned providing you with a dedicated isolated networked storage pool (via NetApp vFiler and EMC VDM technology protection).

This robust architecture is independently endorsed by KPMG-authored audits.

Don't forget about data encryption

Remember that BT Cloud Compute IaaS does not provide a data encryption service, so you must determine if you need additional data segmentation controls.

While encryption of data in transit is commonly available from public cloud service providers (through https or SSL internet protocol connectivity), encryption is often non-existent while data is held in storage (at rest).

This is one place where data remains vulnerable, and unencrypted virtual disk volumes outside your security control can easily be mounted to gain access to your data.

In considering the use of encryption, you must consider the implications for the associated key management, and identity and access management controls you need to put in place.

As this can become complicated if you're using multiple cloud service providers, you should give some thought to using cloud broker services.

3.4 BT Operational Security Controls: fighting Hypervisor attack threats

BTs Cloud Compute systems use virtualisation software with 'Evaluation Assurance Level' certification to guard against risks associated with virtualisation technology and Hypervisor-based attacks.

- We implement full lifecycle asset management
- We manage your own and BT-procured hardware, both in a BT and non-BT data centre
- We have a cloud aware configuration management database (CMDB)
- Our Cloud Compute service offers a comprehensive dashboard including the tracking of resources, their usage and associated charges, giving your developers and IT professionals the opportunity to balance time and cost efficiencies.

BT Cloud Compute also provides operational security controls to reduce the threats associated with malicious code, targeting both the VM infrastructure and your applications and data. These include anti-virus/malware scanning as standard.

What's more, we provide an advisory service if you do not want automatic patching (in case neoteric patches conflict with your applications).

Within the network layer, we can offer Layer 7 deep packet inspection (header, URL and payload) and appliance-based IDS/IPS as required.

We also offer:

- **Intelligent Intrusion Detection and Prevention (IDS/IPS)** containing a set of rules that protect known vulnerabilities from being exploited. This allows you to protect different types of applications including database, web, email and FTP servers. IDS/IPS rules also provide zero-day protection for known vulnerabilities that have not been issued a patch, as well as unknown vulnerabilities
- **Web application protection rules** containing a set of rules that can be configured to defend against common web application attacks. You can add or modify an existing security rule to protect a web application running on the end system
- **Vulnerability scanning** automatically scanning systems against known vulnerabilities and missing patches. It can then recommend which virtual patch is needed to protect a system, using either deep security solution or third-party vulnerability analysis tools.

4. Personnel security: people on your side

Control of an individual's access to your data and code is a key concern. If you're considering using the cloud, you need to look at the people managing your data and what types of controls you apply to them.

It's possible that employees selected by your CSP to administer your cloud infrastructure – with privileged access to your data/resources – may not be screened/security cleared to ensure their security skills or trustworthiness meets the standards promised to you.

And regardless of screening, they potentially pose an insider threat (which incident surveys highlight as the most likely threat source against IT systems) and may abuse their administrative rights, compromising your security.

Then of course, there's always the possibility of CSP staff errors (in misconfiguring a router, Hypervisor setup etc.) leading to service disruption to a large number of customers.

BT personnel security: part of our DNA

BT has always been a member of the UK's critical national infrastructure; our network is under continuous attack at both a physical and electronic level, so we have to work to maintain the security and integrity of our network infrastructure.

- We now have over 1,300 employees in job functions which focus specifically on security
- Key roles globally in this area include security sales specialists, security specific operations teams, security designers, security consultants, security researchers and security product managers, both for development of in-life solutions and new portfolio solutions

4.1 BT Security Controls: countering insider threats and phishing attacks

Taking into account local laws, regulations, ethics and contractual constraints, BT ensures all its employment candidates, contractors and third parties are subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.

Before we grant any physical or logical access to facilities, systems or data, we require our employees, contractors, third-party users and customers to contractually agree and sign the terms and conditions of their employment or service contract, which explicitly include the parties responsibility for information security.

BT protection against insider threats goes even deeper:

- We ensure that roles and responsibilities for performing employment termination or change in employment procedures are assigned, documented and communicated
- We ensure that all levels of user access are reviewed by management at planned intervals and documented. Where access violations are identified, remediation must follow documented access control policies and procedures
- We provide a security awareness training programme for all contractors, third-party users and your employees. Each individual with access to your data receives appropriate training and regular updates in your organisational procedures, process and policies. This is particularly relevant to help employees defend themselves against phishing and spear phishing attacks
- We identify personnel that have significant information system security roles and responsibilities during the CSP platform development life cycle. We document those roles and responsibilities, and provide appropriate information system security training
- BT Cloud Compute managers must maintain an awareness of, and compliance with, security policies, procedures and standards relevant to their area of responsibility
- BT Cloud Compute policies, process and procedures are in place to enforce and assure proper segregation of duties. Where user-role conflicts of interest exist, technical controls counter any risk from unauthorised or unintentional modification or misuse of your information assets
- We encourage you to look holistically at the issue of personnel security across your CSPs and your own organisation. For example, spear phishing attacks will target not just CSP employees but also key account holders in your own organisation.

BT Cloud Compute audit logs privileged user access activities, authorised and unauthorised access attempts, system exceptions, and information security events. Audit logs are reviewed at least daily; integrity and intrusion tools help detect, investigate and respond to incidents; and user access to audit logs is restricted to authorised personnel.

5. Successfully managing identity and access

So what are the types of control we can apply to the individuals with access to your data? As we consider them, remember that the people managing your data include both your employees and CSP employees.

Although identity and access management is not currently part of BT's Cloud Compute IaaS productised service, you can set up and manage user identities and credentials for your employees using the portal.

Introducing the BT Cloud Compute portal

The portal lets you set a hierarchy of users: the account initiator (Initial User) will be the Master User, able to set up additional users on the account. These additional users can be defined as Master Users, Power Users, Users and Billing Admin.

Operation	Master user	Power user	User	Billing admin
Dashboard request				
Provided with a security & network device	✓	✓	✓	
Provided with an external IP address	✓	✓	✓	
Provision server	✓	✓	✓	
Provision network	✓	✓	✓	
Destroy server	✓	✓	✓	
Start-up server	✓	✓	✓	
Shutdown server	✓	✓	✓	
Restart server	✓	✓	✓	
Add public IP address	✓	✓	✓	
Remove public IP address	✓	✓	✓	
Add ACL	✓	✓	✓	
Remove ACL	✓	✓	✓	
Add storage	✓	✓	✓	
Remove storage	✓	✓	✓	
Billing admin	✓	✓	✓	✓
View spend (account wide)	✓	✓	✓	✓
View spend (own resources)	✓	✓	✓	✓
Add user	✓			
Server				
Connect via console	✓	✓	✓	
Snapshot volumes	✓	✓	✓	
Template volumes	✓	✓	✓	

Figure 1-4 – the table above highlights permissions enabled for these roles

Each user's access has a set number of functions, so you can provide individual users with the specific activities/authority they require.

Of course, you should put in place policies to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants, which are generally higher-risk than non-portable devices (e.g. desktop computers at your facilities).

Note that the CSP and its employees are able to access data across multiple providers. This privileged access increases the potential malicious insider threat that's prevalent even in a non-cloud-based environment.

That's why BT Cloud Compute:

- Has adopted the 'principle of least privilege', eliminating unnecessary privileges that can result in network exploits and IaaS compromises
- Ensures that shared credentials (such as user accounts and passwords) are not used in the CSP environment – eg. for system administration and maintenance – and generic or shared accounts are not assigned to or used by our clients
- Has controlled access points that require all administrators to use multi-factor strong authentication. Individual smart cards are provisioned and configured for such access. and mechanisms allow us to routinely audit these logs for the full duration of access
- Has ensured that proper controls are in place to control access to the Hypervisors of the platform.

6. Data and service: portability and protection

Another crucial question to ask is: *Where exactly is my data?*

Yes, your data is in the cloud, but it has to reside in a physical location. This raises questions of its own. In general, in the cloud environment:

- You may have limited oversight of your data storage
- You might not know where your data is physically stored
- You might not know that the location(s) can regularly change
- You may be unaware that, for redundancy or high availability reasons, your data could be stored in multiple locations at any given time.

The power of the Patriot Act

The US Patriot Act has the authority to override other regulations. In June 2011, the managing director of Microsoft UK admitted that it would comply with the Patriot Act as its headquarters are based in the US. While it would try to inform its customers before this happens, it could not guarantee this. So let's say you do business with a UK subsidiary of a US-based cloud operator. You can specify that English law applies and choose a UK-based data centre operating under EU data protection laws, yet the FBI can still get access to your data.

If you don't know where your information actually resides (which depends on the deployment and service model you adopt, and the dynamic nature of cloud operations), concerns might arise over data ownership, as well as potential conflicts between domestic or international legal and regulatory requirements.

As just one example, the CSP's infrastructure may result in data traversing or being stored in politically or economically unstable countries.

Understanding the legal jurisdictions that apply to data in different countries can be a challenge, and if you're subject to regional laws restricting cross-border flows of data, you'll need to verify all locations/flows of data to ensure your cloud service meets your legal obligations.

Other legal considerations include:

- Requirements for electronic discovery, evidence preservation and integrity, and data custody
- Assurance that CSPs have documented processes for responding to legal requests for seizure of records, including data/audit logs belonging to the CSP and their clients
- Understanding the ramifications of such laws in countries where your data exists, as well as the processes your CSP will engage in.

So it's worth knowing that:

- BT's Cloud Compute service is available on local infrastructure with local support in Ireland, France, Italy, Spain, Germany, India, China, Singapore, Hong Kong, Brazil, Columbia, and Mexico
- We are extending and enhancing these services into additional locations.

Data crossing borders

The EU data protection act prevents the transfer of data outside the European Economic Area to a country with inadequate data protection laws or unless the recipient can provide the adequate protection.

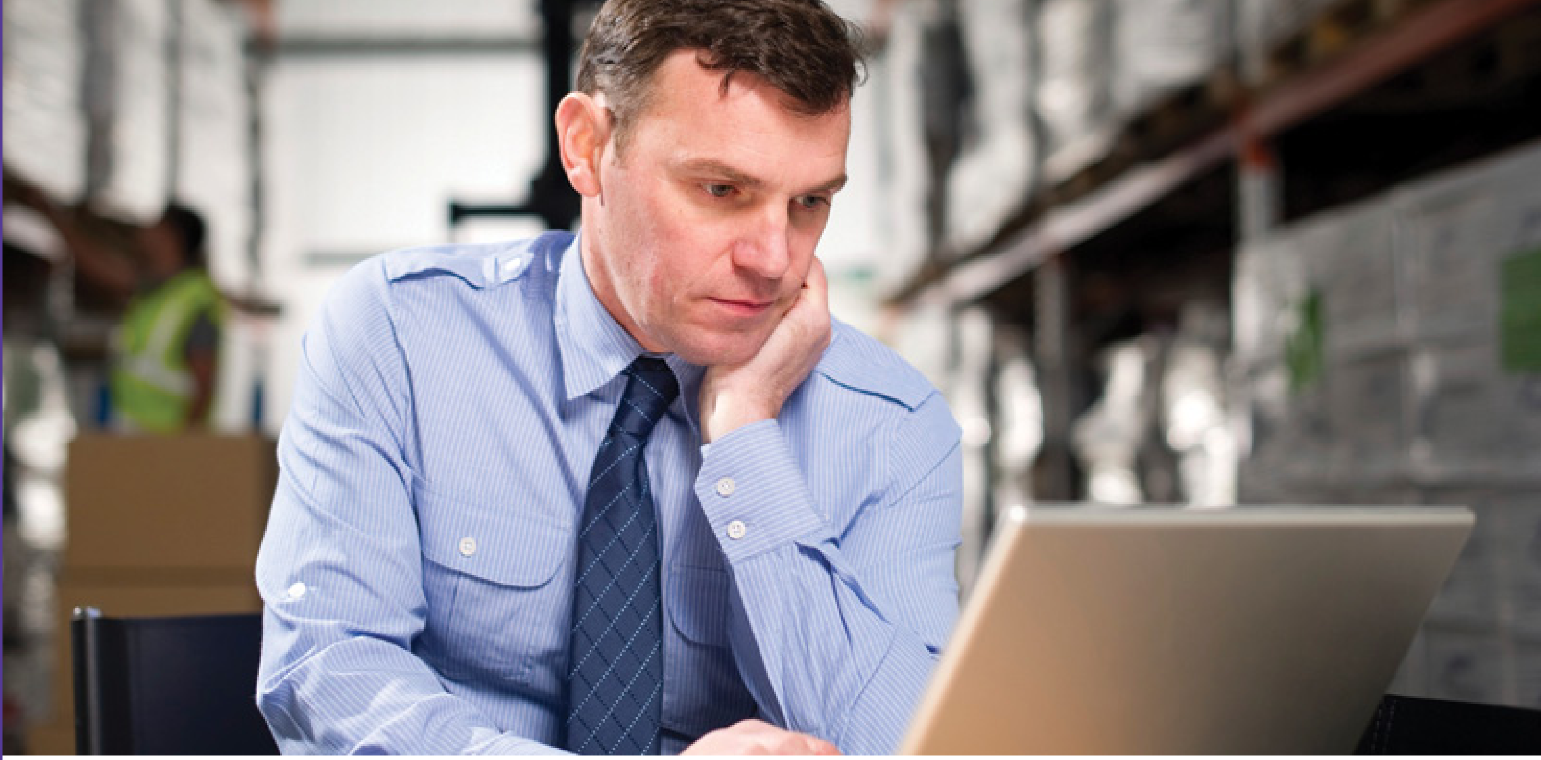
The European Commission keeps a list of safe countries. Canada and Switzerland are on this list and so is the EU/US-negotiated, self-regulated 'Safe Harbor'.

Most of the large US cloud providers have signed up to the Safe Harbor principles which allow them to transfer data from the EU to the US. As a customer, you are responsible for complying with these geo-location constraints on your data, even when it is in the cloud.

Even if the CSP retains your data within the EU, there are still issues concerning compliance.

Once again we ask for your understanding in that, as far as of the physical location of your data is concerned, you must ensure its compliance with your data protection act obligations as part of your overall risk analysis.

To help you with this, BT Cloud Compute gives you the option to geographically ring fence your data and applications within a specified geo-location.
We will ensure your data will not be allowed to transfer outside the jurisdictional boundaries specified within the contract.



7. Supply chain assurance

It’s important to remember that a CSP will typically outsource specialised services to third-party providers.

If outsourcing activities affect the security services provided to you, the reliability of outsource supply chains becomes a key issue. Any failure in them could seriously affect your security processes.

In the cloud context, the supply chain includes physical facilities such as data centres as well as the hardware and software components of the IaaS infrastructure.

First-class third-party support

BT Cloud Compute does use third party physical facilities – we’ll look at the security controls associated with these in the following section – but you can rest assured your security is in safe hands:

- BT Cloud Compute manages the risk of malware being injected through its supply chain through its full life cycle, and asset management and asset tracking, security controls
- We manage your own and BT-procured hardware, both in a BT and non-BT data centre
- We have a cloud-aware configuration management database (CMDB)
- Our Cloud Compute service offers a comprehensive dashboard including the tracking of resources, their usage and associated charges, allowing your developers and IT professionals to balance time and cost efficiencies
- Because any change to the system or process can mean opportunities for subversion throughout the supply chain, BT implements sustainment activities and processes. The sustainment process begins when a system becomes operational and ends when it enters the disposal process, and includes system maintenance, upgrade, patching, parts replacement and other activities that keep the system operational
- Elements, information and data can be disposed of at any time across the system and element life cycle. For example, disposal can occur during research and development, design, prototyping or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys and partial reuse of components.

8. Ensuring physical security

Cloud services are only ‘cloud’ in concept. They really involve physical resources, located at the CSP environment, which you access remotely.

When CSPs of public and shared clouds offer their services to you, you must be aware that your data and virtual components co-exist in the same physical location, and on the same physical systems, as that of other clients.

So it’s easy to see that poor physical security controls at a CSP facility may expose your own and other clients’ data to unnecessary risk, and that poor environmental controls may reduce the performance and integrity of the service on offer.

ISO 27001 compliance ensures that policies and procedures are in place for the safe and secure operation of the data centre facilities and associated offices. These include the implementation of security controls such as:

- **Appropriate physical security perimeters**
- **Physical access control mechanisms and monitoring to ensure that only authorised personnel are allowed access to the facility and its secure areas**
- **Secure full life cycle asset management of hardware and software.**

In a private cloud, the physical location of all components is known and can be verified. However, when using a public cloud, different elements of the environment, such as VMs, Hypervisors, virtual network devices, etc., could frequently be relocated according to the CSP's load-balancing strategy.

Ensuring that appropriate physical security is in place can be challenging in an environment where data and infrastructure can be in different locations at different times.

Global location, local service, high security

That's why BT Cloud Compute offers a comprehensive range of data centre services globally – all inherently resilient, security endorsed and with self-service options to enable business agility:

- BT's On Demand Compute service is available on local infrastructure with local support in the Ireland, France, Italy, Spain, Germany, India, China, Singapore, Hong Kong, Brazil, Columbia and Mexico
- Our Cloud Compute's IaaS is an international service and as such, we focus on compliance with international standards such as ISO rather than local/national standards
- Some of the data centre facilities we use are owned by us, others are operated by trusted third parties. However all the data centres that we use are at Tier 3 and ISO 27001 certified
- Tier 3 means that the data centres feature highly resilient site infrastructures and dual power supplies, resulting in 99.982% availability.

What's more, to help you with concerns regarding data protection compliance, BT Cloud Compute gives you the option to geographically ring fence their data and applications within a specified geo-location.

9. Safeguarding business continuity

It’s an unpalatable thought, but there must be room in your cloud service for a disaster recovery/business continuity plan.

As we’ve seen, while you may not know the physical location of your services, they are physically located somewhere, and prone to physical threats such as fire, storms, natural disasters, and loss of power.

In case of any of these events, how will the cloud provider respond, and what guarantee of continued services do they promise?

From your own perspective, successful business continuity depends not only on the CSP’s provision of the IaaS infrastructure, but on the timely recovery of your data, *which is your responsibility.*

Let's once again stress that your IaaS provider is responsible for maintaining service continuity of the infrastructure: with BT On Demand Compute and Private Compute, you get a 99.95% service level agreement as standard, but you have responsibility for the security of your data.

In the event of a serious disruption such as a natural disaster, BT Cloud Compute will do everything possible to provide continuity of service with a fast rebuild in a nearby virtual data centre location.

Although the generally available IaaS productised services are not contractually obliged to offer you a formal business continuity service, you can get such services from BT on a bespoke case-by-case basis.

The international standard for business continuity

BT Cloud Compute's IaaS infrastructure complies with ISO 22301, which specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your business recovers from, disruptive incidents.

This globally recognised certification verifies that we:

- Have adequately addressed business impact analyses, risk assessments and business continuity strategies
- Have established business continuity and incident management plans, and undertaken BCM
- Comply with statutory, regulatory and contractual duties.

That said, it's important to reiterate that you'll need to have your own Enterprise Business continuity plan that includes controls for the back-up and timely recovery of your data.

10. Meeting regulatory and legal requirements

Throughout this document, we have emphasised the issue of ownership of responsibility.

BT does all it can to offer you the cloud service within which to make the most of your data and information for the benefit of your business.

But please remember that the onus is ultimately on you to secure that valuable data.

This includes ensuring compliance with your local data protection act obligations. In terms of key data protection roles:

- As a customer of BT Cloud Compute IaaS services, you are always the data controller (irrespective of whether your data is being created in house or on the cloud)
- As our standard contract explains, we will not take on any role or liability associated with the custodian role for your data
- As your CSP, we are the processor for your data, but we will not undertake security/data protection responsibilities/ liabilities associated with your data.

Different countries, different rules

Understanding the legal jurisdictions that apply to data in different countries isn't easy.

As we've seen, regional laws that limit data flows across borders mean some organisations must verify all locations and flows of data to make sure their cloud service meets legal obligations.

BT Cloud Compute conforms to ISO 27001, an internationally recognised information security standard. It's designed around a set of security controls that, once implemented, provide you with a solid assurance that your data is secure.

This standard requires us to:

- Demonstrate, through a series of external assessments, that we meet the requirements of over 130 security controls
- Show a high level of security governance, especially in the areas of risk assessment and management.

You may also be interested to know that BT Cloud Compute conforms to PCI DSS Level 1. If you need to show compliance with this standard, BT Buynet – our fast, flexible and secure credit/debit card processing service – offers you a convenient route to it.

In Ireland, if you process personal data, your organisation is a 'data controller' for the Data Protection Act 1988 and Data Protection (amendment) Act 20013, which places specific obligations on those who wish to process sensitive personal data. So all personal, sensitive data should be handled with the utmost care.

If you have any questions about anything you have read in this paper or would like to discuss it in further detail, please contact your BT account manager. For more resources and information on BT's related products and services, please visit:

http://www.btireland.com/prodserve_btcompute_cloud.shtml

Bringing it all together

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to the respective British Telecommunications plc standard conditions of contract. Nothing in this publication forms any part of any contract.

© BT Communications Ireland Ltd

Registered office: Grand Canal Plaza, Upper Grand Canal Street, Dublin 4
Phone +353 (0)1 4325000 Freephone 1800 924 924
Registered in Ireland No. 141524

Find out more about BT Ireland

💻 www.btireland.com

☎ Freephone 1800 924 929

✉ business@btireland.ie