Acronis

WHITE PAPER

Acronis Cloud data centers

October 2022

A primer on security, privacy, and compliance

Acronis
Cloud data centers

October 2022

Table of contents

Introduction

Since 2003, Acronis has offered industry-leading backup and disaster recovery solutions to businesses of all sizes. Today, numerous government, financial, and other organizations with extreme data sensitivity and robust security requirements, and zero tolerance for data loss and downtime trust Acronis to protect their business-critical systems and data all over the world.

Acronis has unparalleled experience in designing and executing critical data protection solutions. Acronis cloud data centers leverage sophisticated enterprise-level security, privacy and compliance mechanisms for organizations operating within variety of business sectors. Few of our over 500,000 customers can implement the same level of security on their premises, or in their private clouds, by relying only on their own resources. This white paper describes the stringent Acronis privacy and data security practices addressing the confidentiality, integrity and availability of your data.

Given the accelerating rate of change in the information technology industry, and its ever-evolving capabilities, technical details in this white paper are subject to change. What never changes is the unwavering dedication of Acronis to protecting your data.

Information security and compliance program

Customers entrust Acronis with the safety of their information, because they recognize Acronis as a continually vigilant and committed partner, capable of fulfilling their requirements.

We look at information security not just as a steady set of strategies for managing processes, tools and policies, but rather as an ongoing process with multiple players, where the role of the individual matters and the key role player is information. That is why Acronis maintains a comprehensive information security and compliance program that includes administrative, physical and technical controls, established using the graded approach, which involves safety assessment modeling and ensures that the necessary level of risk analysis, documentation and security measures implemented are commensurate with the magnitude of the possible information security risks. Our information security and compliance program embraces broadly accepted security standards such as ISO/IEC ISO 27000 series and standards issued by the National Institute of Standards and Technology (NIST).

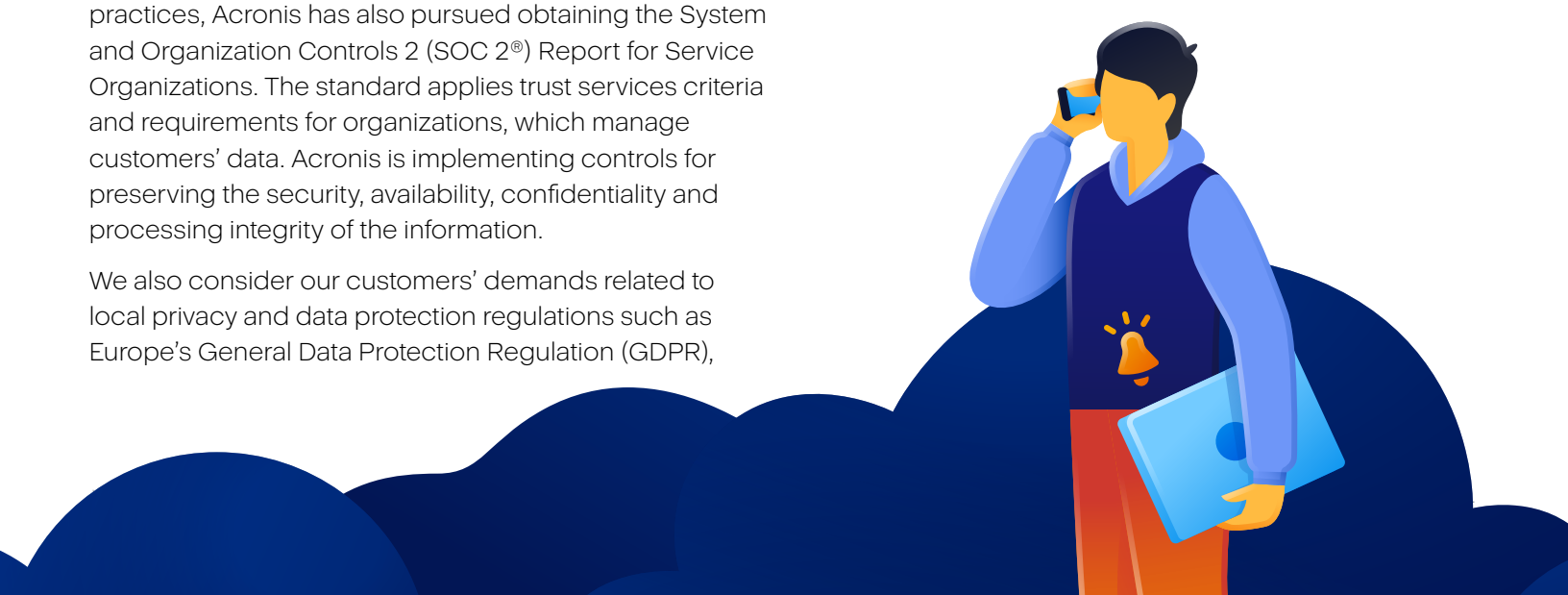
The Acronis Information Security Management System (ISMS) has been certified by independent third-party auditors in accordance with the ISO/IEC 27001:2013 framework for information security, which has become an industry gold standard.

In order to provide further assurance about our security practices, Acronis has also pursued obtaining the System and Organization Controls 2 (SOC 2®) Report for Service Organizations. The standard applies trust services criteria and requirements for organizations, which manage customers' data. Acronis is implementing controls for preserving the security, availability, confidentiality and processing integrity of the information.

We also consider our customers' demands related to local privacy and data protection regulations such as Europe's General Data Protection Regulation (GDPR), the United States Health Insurance Portability and Accountability Act (HIPAA), etc.

Acronis has invested considerable resources to guarantee enterprise-level security for its customers at a fraction of the cost of other on-premises and cloud information security solutions. Acronis continuously works to improve asset tracking, asset profiling, access control and vulnerability management to ensure consistent services and maintain a decent level of security. Acronis actively seeks compliance with well-known information security standards and accepted best practices. All our information security measures are integrated and coordinated with the Acronis Business Continuity Management Program to minimize any security threat, and natural and human-made hazards.

To ensure the proper implementation of the information security and compliance program, Acronis continually monitors and conducts internal and external audits to verify compliance with the established requirements for information security and data processing. This allows Acronis to adequately measure the degree of our program implementation and to detect and respond to the emergence of new information security risks.



Infrastructure and network security

Acronis hosts data and cloud products at trusted geographically-distributed data centers in the U.S., U.K., France, Germany, Japan, Singapore, Switzerland, and multiple other locations, as displayed on our website (https://www.acronis.com/data-centers/).

Customers can choose which region or data center to store their data, making it possible to ensure compliance with regional requirements for data placement, as in the case of GDPR and other local privacy and data protection regulations.

When selecting our data center providers and data center locations, we thoroughly assess providers taking into account the capabilities of the facility, the current evaluation of the threats (constructional, technical, environmental, political, etc.), and the relative attractiveness and business requirements for the specific region.

To confirm the reliability of data centers providers and ensure their capability to maintain the security, availability, confidentiality and integrity of information, our data center providers are audited regularly by respected, independent organizations. The scope of such audits may include the following standards and requirements[1]:

Acronis demands that data centers employ the highest standards of physical security to restrict unauthorized physical access and protect the safety of customer data. Only authorized personnel have access to the data centers, based on strict access control measures and monitoring by surveillance cameras (CCTV). The level of protection from intruders exceeds anything that small to medium businesses can hope to implement alone.

The electrical power systems in these data centers are designed to provide an uninterrupted power supply to the entire infrastructure 24 hours a day, 7 days a week. The data centers are powered by at least two independent power sources. The use of automatic, noninterruptible power supplies protects against power surges in the case of switching power lines, and provides power support during the switchover to diesel generators.

High availability and redundant infrastructures are designed to minimize associated risks and eliminate single points of failure. Acronis follows the approach of need plus two (N+2) for greater redundancy across all hardware layers of its infrastructure. This ensures that if there is a failure in a hardware-layer component, it does not affect either the Acronis critical infrastructure or Acronis customers.

This redundant infrastructure allows Acronis to fulfill most types of preventive and maintenance activities without service interruption. Scheduled maintenance and changes to the infrastructure are carried out in accordance with the manufacturers' specifications and internal documented change management procedures. Every piece of equipment is under warranty and all elements of the infrastructure are covered under each respective vendor's SLA. A dedicated team manages all vendor maintenance contracts, which are subject to annual revision. The team follows a standardized maintenance approach designed to improve infrastructure availability and reduce operating and maintenance costs.

Acronis monitors all official repositories and bulletins for the latest information about new or existing vulnerabilities. Security and critical updates have the highest priority and are rapidly installed. Every update is fully tested before it is implemented. Acronis employs skilled technology professionals and experts at every

[1] Exact list of certifications and standards may vary for specific data centers. Please request additional information from your account manager or support team.

level of its infrastructure and actively collaborates with its third-party vendors to resolve issues.

Acronis commissions security audits from third parties to verify that all components and configurations are free from security issues.

Acronis performs daily scans of critical infrastructure and regularly checks the configuration of all network security components.

Acronis reviews the security of new services and the architecture of network interaction with these services before integrating them into the company's network.

The Acronis network is multilayered and zone based. The managed network equipment separates and isolates internal, external and customers' environments, and provides routing and filtering of network protocols and packets.

Acronis provides real-time encryption for all data transferred. Acronis utilizes secure data transfer protocols (HTTPS, TLS, SSH, OpenVPN, etc.) with crypto-strong encryption algorithms, and provides security of cryptographic key exchange (Diffie-Hellman, RSA) to protect the transmitted data and reduce the risks of unauthorized access to the transmitted data and compromised key information.

Acronis continuously monitors the security of its entire IT infrastructure to protect against advanced persistent threats and cyberattacks. Acronis controls and monitors its boundary, DMZ networks, VPN and remote connections, and internal flows. Acronis utilizes automated tools in conjunction with organizational controls to guard against human intervention.

To ensure network security and minimize the risks of external penetration, Acronis uses the most modern web application firewalls (WAF), which include instant protection against SQL injection, cross-site scripting, unauthorized resource access, remote file inclusion, and other open web application security (OWASP) threats.

Data storage security

The Acronis Cyber Cloud environment is a multitenant environment, so the architecture of our cloud services provides physical and logical isolation and separation of customers' data to ensure processing of the minimum amount of data in accordance with stated processing purposes.

Acronis stores customer data employing its own software-defined storage solution, Acronis Cyber Infrastructure with Acronis CloudRAID technology. Acronis Cyber Cloud Infrastructure delivers fast, universal, protected, efficient and proven storage that unites block, file, and object workloads.

Acronis Cyber Infrastructure utilizes a proprietary erasure-coding algorithm to enhance reliability and protection against failures. It includes scalable and efficient self-healing mechanisms which minimize data risks. In addition, Acronis Cyber Infrastructure utilizes a fully redundant architecture to safeguard data integrity for every customer.

All Acronis Cyber Cloud are encrypted at rest by the Advanced Encryption Standard (AES) with a 256-bit key.

Over the years, storage capacity at the Acronis data centers grew from hundreds of terabytes to dozens of petabytes. At the same time, the unique flexibility and scalability of Acronis Storage ensures this exponential rate of growth will not affect customer-critical data in any way.

Acronis Cyber Infrastructure drives and equipment on which the data storage and/or processing are carried out can be broken, switched out for repair, or decommissioned. In these cases, Acronis takes measures aimed at a complete erasure of data from disks and the removal of residual data from the internal memory of the equipment according to NIST SP 800-88rev1. In the event that it is not possible to erase (delete) such information, physical destruction of equipment is performed in a way that makes it impossible to read (restore) such data.

Personnel security

Maintaining data security is impossible without people. Despite the fact that personnel are an organization's most important asset, Acronis also understands that a main security concern relates to employees. No system or infrastructure can be 100% protected without establishing a corporate-wide security culture.

All Acronis personnel receive awareness education and training regarding information security, privacy protection and data processing appropriate to their job functions and assigned roles.

Acronis also pays special attention to the selection of personnel by conducting appropriate background verification checks on candidates for employment in accordance with applicable local laws, statutory regulations, and ethics. Every Acronis employee is obligated to comply with the Acronis confidentiality, business ethics, and code of conduct policies and is required to sign a Non-Disclosure Agreement (NDA), which remains valid even after employment contract termination.

Access control

Acronis has implemented an enterprise-wide access control policy to restrict access to information resources and data in accordance with official duties.

For all positions, Acronis follows the principals of segregation of duties, need to know and least privileges. This ensures that every user has the least amount of privilege necessary to complete a job, and all critical operations are controlled and accountable. Only staff with the highest clearance can access data center environments.

Internal access control procedures detect and prevent unauthorized access to Acronis systems and data. When providing access, Acronis uses centralized access control systems with secure mechanisms and authentication protocols (e.g., LDAP, Kerberos, SSH certificates, 802.1x), unique user IDs, strong passwords, two-factor authentication mechanisms, and limited control access lists to minimize the likelihood of unauthorized access.

In addition, any access is recorded in system audit logs, which are protected from changes and are periodically reviewed.

On top of logical access control practices and at rest encryption, Acronis provides customers with the capability to encrypt their data based on a key generated from a customer's password, which gives them complete control over their data.

Application security

Acronis uses the latest versions of software and regularly updates its operating systems, software, frameworks, and libraries. The Acronis software practices safeguard the confidentiality, integrity and availability of all data.

Third party components, including open-source components, are cloned into an internal Acronis repository before they can be linked to the main software. All components are reviewed by development and information security teams and approved for use in the development process. Also, the company's technical leadership is informed about components to be used in the software development. Security teams regularly monitor for updates issued for the components in use, and if an update contains a vulnerability fix, it will be reviewed and the internal repository will be updated.

Our standard software security practices include:

- Adherence to strict security policies and well-known security best practices to incorporate security at every stage of the secure software development lifecycle.
- Security review of architectures, design of features and final solutions. Information security and quality assurance teams perform security reviews. This includes application scanning for known vulnerabilities and opened ports, etc. And besides internal reviews, Acronis conducts external reviews performed by an independent third party.
- Regular source code review (manually and using static code analyzers) for security weaknesses, vulnerabilities, and code quality to provide direction and guidance for product development. During development, any modifications to the source code are reviewed by an expert in that particular software, and two engineers. All submitted changes are always linked to a ticket in a task management system used by Acronis.
- Code assessment by static application security testing (SAST) tools as part of the software continuous delivery (CI/CD) pipeline to ensure quick feedback to developers. The process is automated and all activities are recorded for the Acronis information security team's future audits.
- Build and constantly maintain security culture among all teams and keep them vigilant to known vulnerabilities and current information security threats.
- Acronis has been running a bug bounty program on HackerOne since 2018. Acronis works closely with the security community and embraces researchers who contribute toward the optimization of our products.
- As a partner of the CVE Program, Acronis is a CVE Numbering Authority (CNA) responsible for publishing disclosed cybersecurity vulnerabilities as CVE records for all Acronis products. For information on security advisories and updates, see Acronis Security Advisory Database.

Incident management

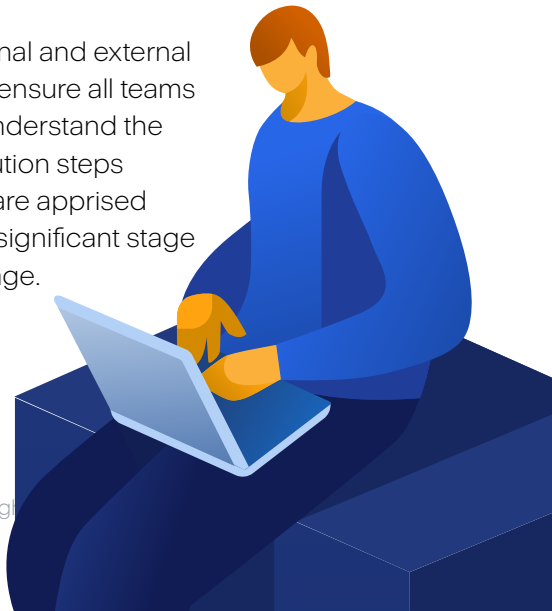
The Acronis security operation team and network operations center (NOC) takes the lead on incident identification and response, identifies the root cause of a problem, and contacts the appropriate internal incident response team to triage the technology incident.

The incident response team is comprised of a carefully selected group that includes representatives from our security and compliance department, data center operations, architecture and product development teams, as well as our public relations and communications teams.

All response times are driven by internal SLA targets (99.9% availability), legal and contract obligations.

Acronis has developed several different escalation paths, based on the type of incident and its severity. Global or high-severity level incidents are escalated and controlled by Acronis executives. The Acronis incident management culture is based on recognized best practices. There are seven stages for handling every incident:

1. **Preparation:** Appropriate security controls are in place and kept up to date. A well-defined incident response plan is established and communicated to all responsible teams. Provision of education to users and IT staff after every incident and new implementation, and training for them to be able to respond to incidents quickly and correctly.
2. **Identification:** The network operations center (NOC) monitors for suspicious system events on a 24/7 basis. The NOC can also be supported by the security operations center (SOC) by rapidly performing an initial triage and analysis to determine whether an information security event is in fact an incident, and what its scope is — such as which networks, systems, applications, hosts or data centers are affected. The objective of the initial analysis is to provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of its effects. Information about information security events is collected through different channels and Acronis monitoring systems.
3. **Containment:** This stage is important in the course of handling each incident and before the incident overwhelms Acronis resources or customer data. The team determines the coverage of the problem, its impact, the affected systems and customers. An essential part of our containment stage is decision making (e.g., for shutting down a system or disabling certain functions).
4. **Eradication:** The team investigates to discover the origin of the incident and the root cause of the problem, and begins the elimination process, such as by removing malware or disabling breached accounts. For some incidents, eradication may either not be necessary or is performed during recovery.
5. **Recovery:** Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. An additional objective of the recovery phase is to prevent similar incidents in the future. For this reason, the NOC team monitors every environment for any signs of weakness or recurrence.
6. **Lessons learned:** The team analyzes the incident and how it was handled, making recommendations for preventing a re-occurrence and a plan for future response.
7. **Notification:** Internal and external communications ensure all teams and customers understand the impact and resolution steps undertaken, and are apprised of status at every significant stage of the incident triage.



Business continuity and disaster recovery

Many potential disruptive threats can occur at any time and adversely affect business operations at any location. Acronis considers a wide range of potential threats as part of risk and business impact analysis at all Acronis locations (offices and data centers), critical processes, and systems.

Acronis recognizes the importance of having a comprehensive business continuity and disaster recovery planning program to:

- Protect employee's safety
- Safeguard the continuation of critical business processes and technology, both internal and customer facing
- Safeguard the Acronis ability to service its customers without interruption

To ensure adequate reaction and availability of its services in case potential disruptive events occur, Acronis periodically reviews and updates its internal business continuity and disaster recovery plans. Testing of disaster recovery plans is conducted at least once a year, according to scenarios for most potential threats in relation to particular assets. At the same time, these testing scenarios are coordinated with regard to stopping the provision of the service as a consequence of various threats determined by those responsible for performing the service. The testing plans are approved for a year by the information security committee and can be carried out in one of the following ways:

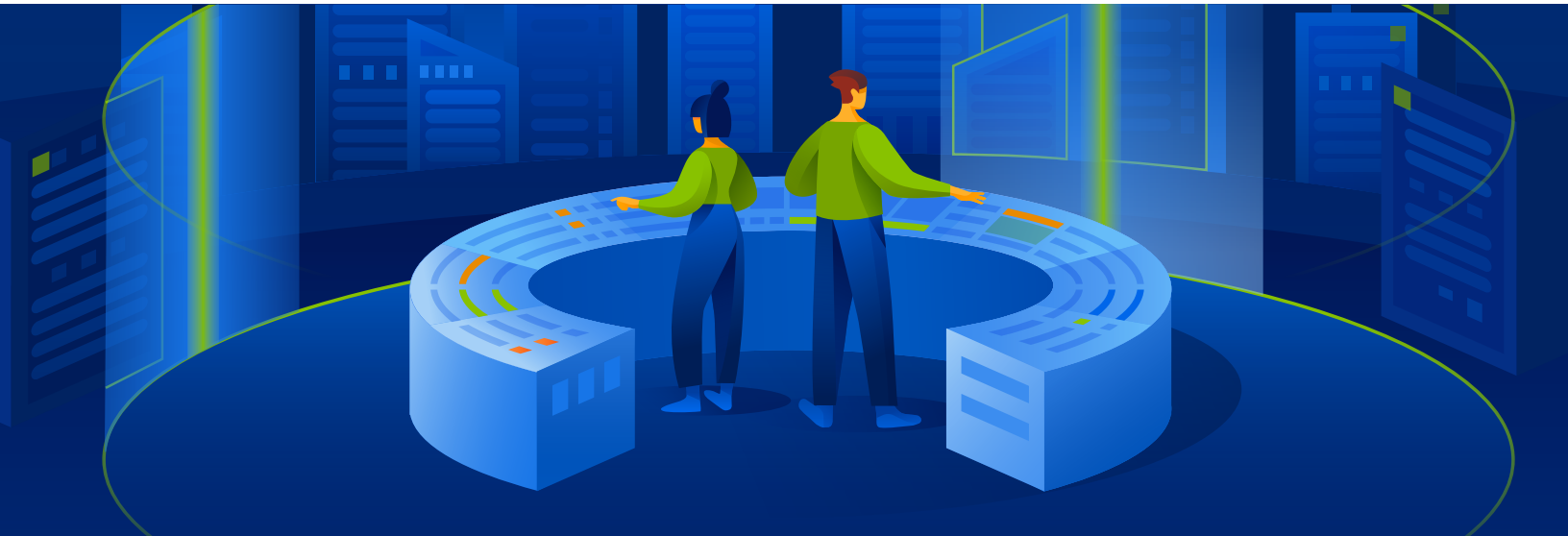
- Checklists
- Structured walk through
- Simulation
- Interruption

Acronis has established partnerships that run numerous global, collocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power, and cooling to maintain optimum conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strong requirements for data center locations to reduce or completely eliminate probability of the most natural disruptive events.

Acronis does not currently perform backup of backups. Acronis instead utilizes redundant infrastructure to eliminate single points of failure. Our backup strategy and disaster recovery plans are focused on service recovery.

Acronis requires the commitment of each employee, department and vendor to:

- Support its business continuity program objectives
- Review, build, test, and grow its business continuity and disaster recovery program
- Protect Acronis assets, mission, and survivability.



Supplier relationship management

Suppliers are an integral part of any business. However, no matter how well your assets are protected within the company, when attracting third parties, you must make sure that they are reliable.

The Acronis vendor selection process begins with defining criteria for the third party. Along with business requirements, we consider both our security and data protection requirements, as well as our customers' requirements.

Before contracting with third-party sub-processors, data centers, or service providers, Acronis conducts a thorough vendor assessment to ensure that the third parties can provide an appropriate level of security and privacy corresponding to the level of data access. Contracts with third parties contain information security, privacy and confidentiality requirements. During the term of each contract, Acronis regularly monitors and reviews the third party's security controls, service delivery, and compliance with contractual requirements.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment — from cloud to hybrid to on premises — at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

This material and any other related documentation on information security compliance produced by Acronis does not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations.

Acronis

Learn more at
www.acronis.com