


# Digital assets protection with




Air Liquide deployed a global new digital procurement solution with Zycus to manage its Source-to-Contract activities, which will become a must in our business relationship. By building this solution, **the critical digital assets protection was a mandatory requirement** of the Air Liquide digital security program. Let's discover together how!

## > Every new business/IT system must comply with Air Liquide's security-by design requirements and controls



Security & Privacy by Design to define the level of criticality



Bi-annual critical digital assets security review on 13 criteria



## > Digital security risk assessment

For each project, security must be embedded from the project initiation in all life cycles



Act Safe



Build & Run Safe



Monitor threats

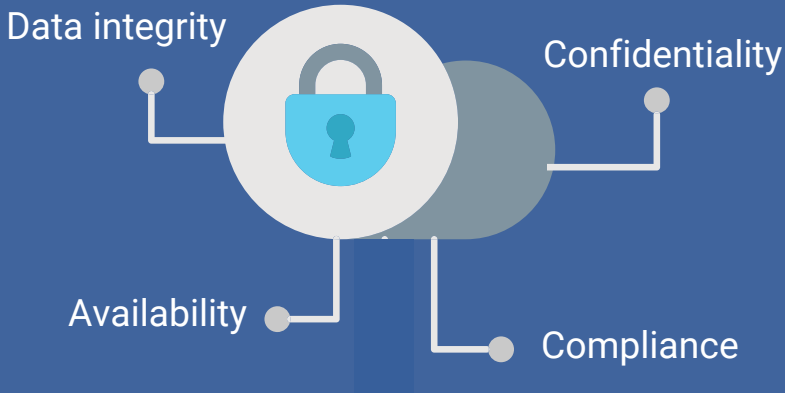


Comply with regulations



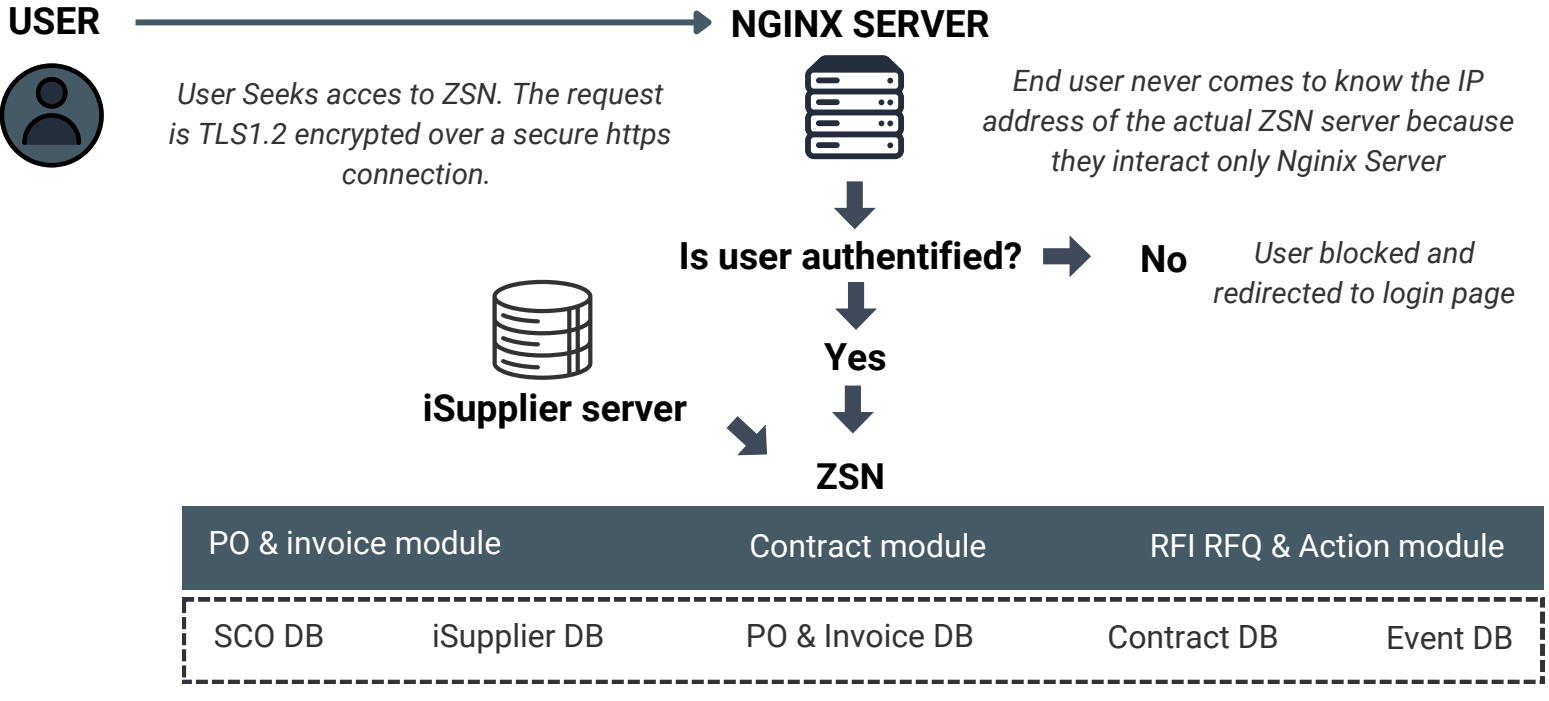
Detect & treat cyber incident

## > Digital security is evaluated through 4 criteria



## > Zycus provides strong security with its solutions

A secure connection to ZSN



## > Zycus solution benefits from strong certifications

ISO 27001: Information Security Management System SOX Compliance



ISO 9001:



ISO 27001: Security certification of IBAN.com company



## > ZSN is a reliable cloud solution, compliant with the Air Liquide checklist



**Security and compliance with Air Liquide requirements**

- Infrastructure security
- Data security
- Privacy and compliance



**Quality of service**

- Integration with Air Liquide systems
- Availability and resilience
- Service Level Agreements

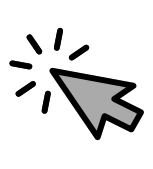


Air Liquide has put in place all the best due diligence practices to ensure your safe use of ZSN

### Need more details ?

Click on the link below for more information:

- [A. Data privacy](#)
- [B. Policy, certification, insurance](#)
- [C. Hosting and infrastructure](#)
- [D. Environment Access and Security](#)
- [E. Identity and access management](#)
- [F. Application security coding and testing](#)
- [G. Availability, Business continuity & Disaster recovery](#)
- [H. Logging, alerting, incidents management](#)



Our IT experts are also available to answer all your questions about whitelisting this solution!



# Appendices

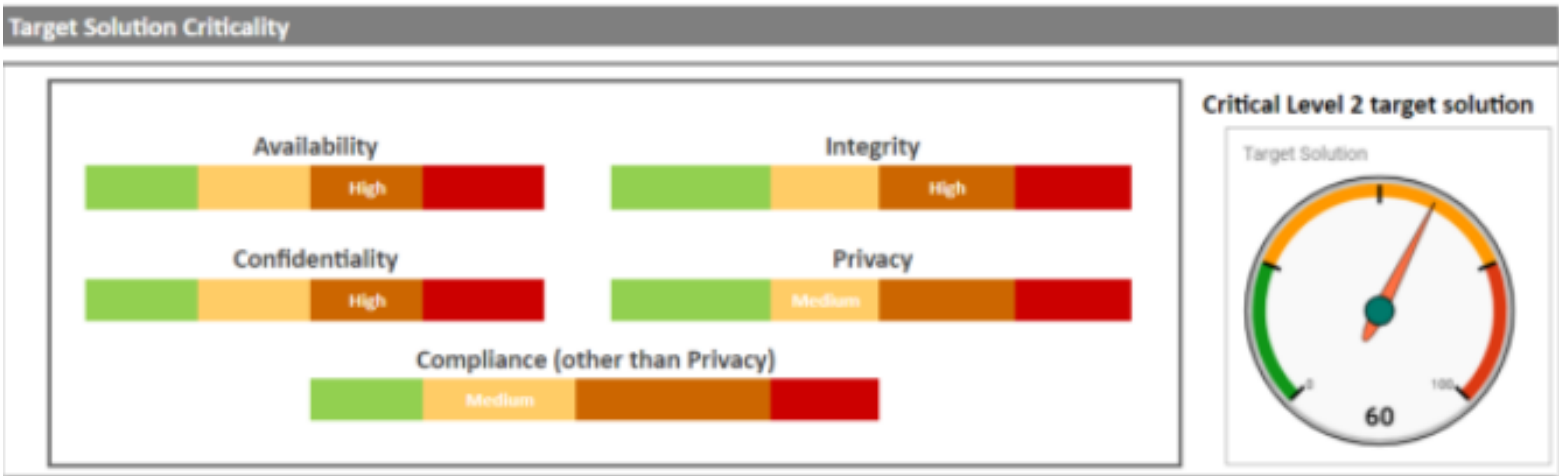
MORE INFO



## 1. How do we assess criticalty in Air Liquide

➡ Back to infographic

### Security & Privacy by Design



### 13 Security Controls with 3 leaders, every 6 months

1	2	3	4	5	6	7	8	9	10	11	12	13
IPC	IPC	IPC	ISO	ISO/GIO	ISO/GIO	IPC	GIO	GIO	ISO	GIO	ISO	IPC
Is there a Business Owner?	S&P by Design done	Have access rights been reviewed?	Is the password policy enforced (complexity, etc)?	Is there a regular backup of application and data?	Is there a documented Disaster Recovery Plan?	Is there a documented Business Continuity Plan?	Are IT unacceptable weaknesses eliminated?	Have privileged accounts been reviewed?	Have penetration tests been performed?	Is the application security monitored?	Are the 3rd Parties under control?	Compliant with privacy regulations

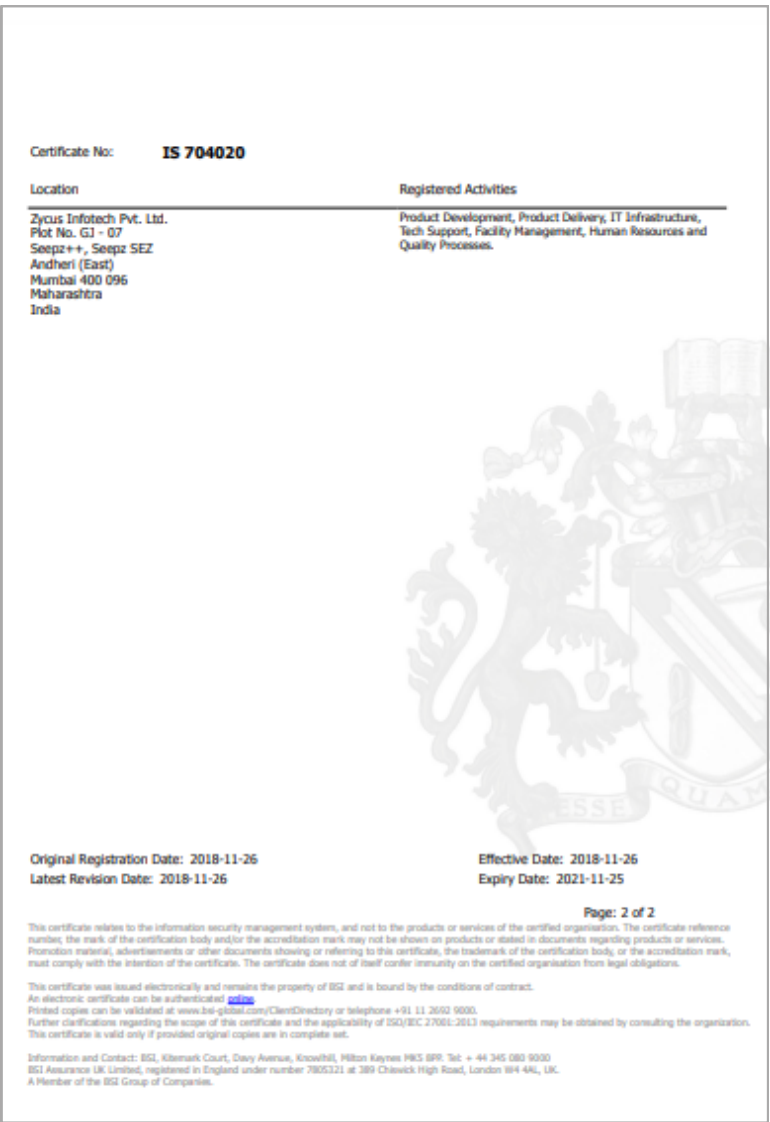
Business Owner: CPO Air Liquide

IPC : Information Protection Coordinator      ISO : Information Security Office      GIO : Global Infrastructure and Operations

## 2. Strong certifications

➡ Back to infographic

### ISO 27001: Information Security Management System SOX Compliance



### ISO 9001: Security certification of IBAN.com company



### ISO 2700: Security certification of IBAN.com company



➡ Back to infographic





## 3. Best practices in Digital Security review to ensure your safe use

### A. Data Privacy

[➡ Back to infographic](#)

Zycus undertake to comply with the applicable regulations on personal data processing, including:

- ☐ (i) The French data protection Act n°78-17 of 6 January 1978 where applicable, the directive 95/46/CE of the European Parliament and of the Council of 24 October 1995, the directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("the General Data Protection Regulation"), and
- ☐ (ii) Any other future applicable legislation which might complete or replace them.

### B. Policy, certification, insurance

[➡ Back to infographic](#)

- ☐ Zycus follows ISO270001 information security framework which has 11 domain areas, 39 control adjectives and 133 controls. Also, the application of Zycus is SSAE16 SOC1 and SOC2 type II-compliant through which it has demonstrated its commitment to providing customers with the highest standards in processes, controls and procedures.
- ☐ Zycus conducts internet security audit on half yearly basis of all its services and processes to ensure that risk is identified proactively and appropriate controls are implemented and documented. Additionally, Zycus conducts third party VAPT (Vulnerability and penetration test) of all applications & network on yearly basis to ensure that there is no data breach.

### C. Hosting and infrastructure

[➡ Back to infographic](#)

- ☐ Zycus has partnered with industries best and most secure AWS (Amazon Web Services) data centres to host it solutions.
- ☐ Zycus follows a defined disaster recovery process wherein Zycus takes full backups of all data weekly and incremental backups of all data daily. When possible, backups are run overnight and are completed before working hours enabling not greater than 24 hours of data loss. All the core operations are performed in primary data centre. However, Zycus can failover operations to secondary cloud site in less than 24 hours. This allows the customer to continue business while Zycus returns the primary site to full operation.

### D. Environment Access and Security

[➡ Back to infographic](#)

- ☐ Zycus protects all its application infrastructure by using state-of-the-art firewall at the hypervisor, kernel, and application levels, as well as intrusion detection systems across all servers. Zycus anomaly detection system instantly notifies operations staff, 24/7, if anything unusual is detected. All front-end servers are behind firewalls and only accessible via https protocol. Zycus exercises tight operating system-level security by maintaining a minimal number of access points to all production servers.
- ☐ Zycus manages its entire SaaS solution by itself. No other third-parties are involved in

### E. Identity and access management

[➡ Back to infographic](#)

- ☐ Zycus provides for RBAC (Role based access control) and leverages a dedicated Tenant Management System (TMS) to manage access as per organization's requirements. Users will have the visibility depending on the role configured in Tenant Management System(TMS).

### F. Application security coding and testing

[➡ Back to infographic](#)

- ☐ Zycus has a defined secure coding process. A secure development environment is maintained while coding. It is ensured that all systems and software used in the development environment are regularly patched with the latest security patches/upgrades. Also, all systems shall have an Antivirus software which is regularly updated with the latest signatures. Administrative access to end systems shall be restricted and internet access on these systems will be limited to certain approved websites.
- ☐ If a secure coding principle is not applicable to the project, alternate security controls/measures shall be applied. The OWASP Secure Coding Guidelines, Policy for System Acquisition, Development and Maintenance shall also be referred to, to identify, develop and maintain security best practices in the application design and development phase is no data breach.
- ☐ Rate A+: Zycus encrypts all data in motion using 2048-bit SSL encryption. All requests are only served through port 443 and other ports are blocked. Zycus uses RSA and Diffie–Hellman algorithms for key encryption. Zycus uses SHA 256-bit encryption and SHA1 with RSA for signatures. Security is ensured using TLS 1.2.
- ☐ Zycus conducts internet security audit on half yearly basis of all its services and processes to ensure that risk is identified proactively and appropriate controls are implemented and documented. Additionally, Zycus conducts third party VAPT (Vulnerability and penetration test) of all applications & network on yearly basis to ensure that the

### G. Availability, Business continuity & Disaster recovery

[➡ Back to infographic](#)

- ☐ Zycus provides 99% uptime (SLA) for all its applications excluding the scheduled downtime for upgrades / patches. The current uptime average is 99.5 % with all our customers. This does not include the non-availability due to scheduled/planned outages. Scheduled Outages will not be included as downtime in calculation of monthly availability.
- ☐ Zycus has a defined disaster recovery policy in place

### H. Logging, alerting, incidents management

[➡ Back to infographic](#)

- ☐ Zycus has an internal application “Zytrack” which tracks and log all activities conducted in the solution. Zytrack maintain descriptive logs of activities conducted, logs include information like User name, access rights, User emails address, Activity conducted, Time of activity conducted etc. The reports can be shared with Air Liquide at mutually agreed intervals
- ☐ Zycus has a defined incident management policy in place and any security incident is evaluated by our information security forum (ISI) and top management. Depending on the severity of the incident and its evaluation, Zycus can inform Autoliv within 2 to 24 hours timeline. If any customer do face security issues, they can certainly connect to customer success managers or technical account manager who will appropriately route to relevant stakeholders and resolve issues as per the timeline.

[➡ Back to infographic](#)