

Editorial

As organizations increasingly adopt SaaS applications for critical business functions, security risks are no longer limited to the technology team. From a compliance perspective, understanding how data is accessed, shared and protected is equally important. A well-governed SaaS environment requires clear accountability, appropriate access controls and regular oversight.

This article is a humble attempt to simplify the concept of SaaS security and making Compliance, Legal, Secretarial, Risk and Business teams understand their role in strengthening SaaS governance and data protection

Please share your feedback on this newsletter with us at contact@cimplyfive.com, we eagerly look forward to it.

Happy Reading,
Team CimplyFive
October 06, 2026

What's more in this month's issue…

- ***What is Hot in Company Law?***
- ***Article of the Month***
- ***BLISS Tips for the Month***
- ***Test your Gray Matter!***
- ***Compliance Calendar***
- ***Regulatory Changes in the Month***

OPINION:

What is Hot in Company Law?

Our free to use website www.ca2013.com has the unique distinction of providing an integrated view of the Companies Act, 2013 ("Companies Act"), Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements), 2015 ("SEBI (LODR)") and Insolvency and Bankruptcy Code, 2016 ("IB code"). Our website has crossed **69 million page-views** as on date and attracts about 15,000 users accessing around 45,000 pages a day. List of the most viewed sections in the Companies Act, SEBI (LODR) and IB Code in the month of September 2026 here is based on visitors to our website is as follows:

For the Month of September, 2026
Companies Act, 2013 Top 5 Chartbusters

Rank in Aug	Change in Rank	Rank in Sep	Section	Section Title
2	↑	1	188	Related Party Transactions
1	↓	2	179	Powers of Board
3	↔	3	62	Further issue of share capital
4	↔	4	186	Loan and investment by company
N	↑	5	177	Audit Committee

Section 149 was replaced with Section 177 for the month of September 2026.

SEBI (LODR) Top 5 Chartbuster Regulations

Rank in Aug	Change in Rank	Rank in Sep	Regulation	Regulation title
1	↔	1	30	Disclosure of Events or Information
3	↑	2	23	Related Party Transactions
3	↔	3	17	Board of directors
N	↑	4	44	Meetings of Shareholder and Voting
5	↔	5	51	Disclosure of information having bearing on performance/operation of listed entity and/or price sensitive information

Regulation 34 has been replaced with Regulation 44 for the month of September 2026 respectively.

IB Code Top 5 Chartbusters

Sections have 21, 3 and 28 been replaced with Sections 29,30 and 33 for the month of September 2026 respectively.

Rank in Aug	Change in Rank	Rank in Sep	Section	Section Title
1	↔	1	5	Definitions
N	↑	2	29	Preparation of information memorandum.
N	↑	4	30	Submission of resolution plan..
5	↑	4	35	Powers and duties of liquidator.
N	↑	5	33	Initiation of Liquidation

 Copyright © 2026, CimplyFive

Article: SaaS Security Risks: What Every Compliance Professional Should Know

"A simple guide for Compliance, Legal, Risk, Secretarial and Business Teams"

Today, organisations rely on SaaS (Software as a Service) applications for almost every function — compliance management, HR, finance, customer management, document management, collaboration and governance.

Unlike traditional software, SaaS applications are hosted and managed by an external service provider. Users simply log in through a browser or application and access the required services and data.

This makes business operations easier, but it also creates a different kind of risk.

The question is no longer only **"Is our IT infrastructure secure?"** It is also:

"Who can access our data, what can they access, how is it shared, and what happens when that access changes?"

SaaS security is therefore not only an IT concern. It is also a **governance, compliance, risk and data protection concern**.

This article is a humble attempt to help compliance professionals make informed decisions about SaaS platforms and their requirements by understanding **where risks arise, what questions to ask, and what controls should be in place.**

What is SaaS Security?

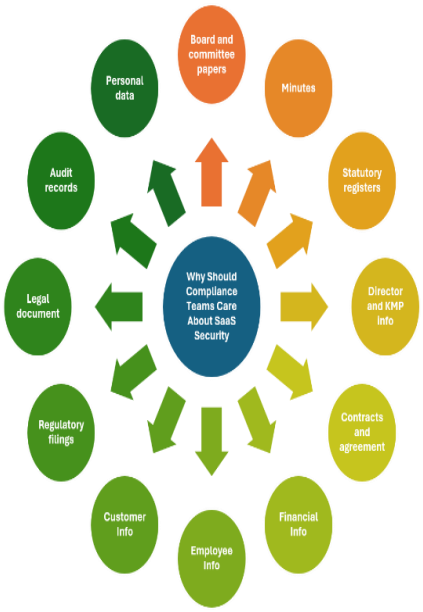
SaaS security refers to the measures used to protect **data, user access, integrations and compliance** when an organisation uses applications hosted and operated by an external service provider.

The SaaS provider manages the underlying platform and infrastructure. The customer, however, continues to remain responsible for several important areas such as:

- Deciding who gets access - Deciding what information each user can see -configuring sharing and access settings - Managing users when employees join or leave- Reviewing third-party integrations- Ensuring appropriate data governance and Meeting applicable internal and regulatory requirements

In simple terms: The SaaS provider secures the house. The customer decides who gets the keys and which rooms they can enter.

Why Should Compliance Teams Care About SaaS Security?



A security incident can potentially result in more than a technical problem. It may lead to:

Data exposure → Regulatory concern → Business disruption → Financial impact → Reputational impact. Security and data governance should form part of the **vendor due diligence process**.

The Most Common SaaS Security Risks

SaaS security failures do not necessarily begin with sophisticated cyberattacks. Many incidents arise from relatively simple issues Incorrect access permissions, Public or inappropriate sharing settings, Old employee accounts remaining active and lack of periodic access reviews

Risk No. 1 – Who Has Access to the Data?

One of the most important SaaS security questions is also one of the simplest: **Who can access the information?**

A user should ideally have access based on their role and business requirement. For example, a person who only needs to view compliance reports may not need permission to Delete records - Modify statutory data- Add new users- Change security settings- Download all documents.

This is the principle of **least privilege** — giving users only the access they actually need.

Compliance perspective: A simple question for the compliance team is:

"If an employee changes roles tomorrow, can their access be changed immediately?"

And: **"When an employee leaves the organization, how quickly is their access revoked?"** These are basic but important controls and this should be periodically reviewed.

Risk No. 2 – Misconfiguration

A SaaS platform may have strong security features, but incorrect configuration can still create risk. Consider a simple example. A document containing sensitive Board information is intended to be shared only with five directors. However, the sharing setting is accidentally changed to allow a much wider group to access the document.

The platform may be functioning exactly as designed. The problem is the **configuration**.

Common examples include - Incorrect sharing permissions - Excessive user privileges- Unrestricted downloads- Broad third-party application permissions- Incorrect security settings- Failure to review default settings

Misconfiguration is identified as one of the most common SaaS security risks.

How can organizations mitigate this?

Establish standard security settings, review configurations periodically, restrict administrative access, and ensure all changes are properly documented and traceable.

Risk No. 3 – Passwords, Credentials and User Accounts

A sophisticated security system can still be compromised if a user's credentials are stolen.

This is why organizations should implement controls such as MFA, strong password policies, SSO where appropriate, centralized identity management, timely removal of former users, and periodic access reviews.

A simple compliance checklist in this perspective :

Question	**What should the organization look for?**
Is MFA available?	Preferably enabled for sensitive access
Are administrator accounts restricted?	Yes
Are inactive accounts reviewed?	Periodically
Are former employees removed promptly?	Yes
Are access rights reviewed?	At defined intervals
Is access based on role?	Wherever practical
Are access changes traceable?	Appropriate audit logs should exist

Risk No. 4 – Third-Party Integrations

Modern SaaS applications often integrate with email, HR, ERP and other business systems. These integrations improve efficiency but create additional access points.

Excessive or unnecessary permissions can increase security risks.

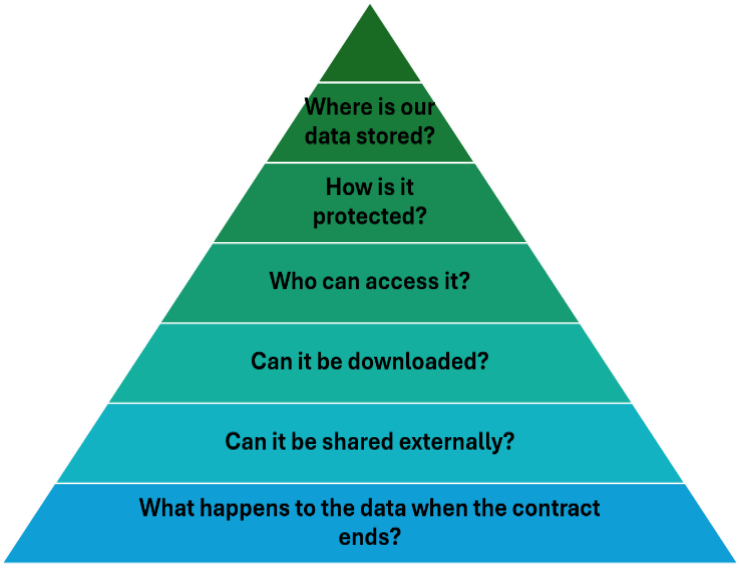
Organizations should review what data each integration can access and who approved it. Integrations should be periodically reviewed and access removed when no longer required.

Risk No. 5 – Data Protection and Encryption

When data moves between a user's device and a SaaS application, it should be protected during transmission. Similarly, data stored within the platform should have appropriate protection.

Encryption is one of the important controls used to protect data both **in transit** and **at rest**. The source material notes that SaaS providers commonly provide TLS for data in transit and platform-managed encryption for data at rest, but customers should still verify whether the protection meets their requirements.

 Copyright © 2026, CimplyFive



Risk No. 6 – Insider Threats

Not every security incident originates from an external attacker. An employee, contractor or other authorized user may accidentally or deliberately misuse legitimate access.

For example:

- A confidential document is downloaded to a personal device or A user shares a document with an unintended recipient.
- An employee exports information before leaving the organization or A user accidentally deletes or modifies important information.

Because the user is authorized, traditional security controls may not immediately identify the activity. This makes **access control, audit trails and monitoring** particularly important.

Risk No. 7 – Compliance and Regulatory Requirements

SaaS security cannot be viewed independently of the organization's legal and regulatory obligations. Depending on the nature of the organization and the data involved, applicable requirements may relate to Data protection, Audit Trails, Regulatory reporting, Contractual obligations and Industry-specific requirements.

A SaaS provider may have strong security certifications and controls, but the customer still needs to determine whether those controls are adequate for its own requirements.

Practical SaaS Security Checklist for Compliance

Data Protection	**Identify sensitive and confidential information handled by the platform and verify that appropriate safeguards are in place.**
Encryption	**Verify that data is encrypted both during transmission and while stored, particularly where sensitive or confidential information is involved.**
Integrations	**Identify all third-party integrations and assess what data and permissions are shared through each connection.**
Incident Response	**Confirm that the provider has a defined process for detecting, reporting, investigating and responding to security incidents.**
Business Continuity	**Understand the platform's backup, disaster recovery and service restoration arrangements to assess continuity of critical business processes.**
Vendor Due Diligence	**Assess the vendor's security practices, certifications, controls and track record before onboarding the SaaS platform.**
Contract	**Ensure security, confidentiality, data protection, incident reporting, access and other relevant responsibilities are clearly documented in the contract.**
Exit Management	**Ensure there is a defined process for retrieving organizational data in a usable format and securely deleting data from the platform after exit.**
User Access	**Ensure access is granted only to authorized users based on their role, responsibilities and genuine business need.**
Least Privilege	**Ensure users are given only the minimum level of access and permissions required to perform their assigned functions.**
MFA	**Check whether multi-factor authentication is available and enabled, particularly for administrators and users accessing sensitive information.**
User Lifecycle	**Ensure processes are defined to promptly provision, modify and revoke access when employees join, change roles or leave the organization.**
Periodic Review	**Conduct periodic reviews of user access to identify and remove unnecessary, outdated or inappropriate permissions.**
Admin Access	**Ensure administrative privileges are limited to authorized personnel and are subject to enhanced controls and monitoring.**
Audit Trail	**Ensure critical activities such as logins, data changes, approvals and administrative actions are recorded and traceable.**

Teams

 Copyright © 2026, CimplyFive

Conclusion - The Compliance Takeaway

SaaS security may initially appear to be a purely technical subject, but at its core, it is about **protecting information and controlling access to it**.

For Compliance, Legal, Secretarial and Risk professionals, the objective is not to understand every technical component of a cloud platform. It is to ask the right governance questions, identify potential risks, and ensure that appropriate controls are in place.

As organizations increasingly move business processes to cloud-based platforms, Compliance teams have an important role to play in ensuring that **digital convenience and transformation are supported by sound data protection, access controls and governance practices**.

 Copyright © 2026, CimplyFive

BLISS Tips for the Month

BLISS Tips #352: Updating Registers in BLISS? Check One Thing Before You Upload.

When updating Registers through Excel upload, always follow the **syntax specified in blue at the top of the Excel template**.

Entering data in the prescribed format ensures **smooth and accurate uploading of Register information**.

Registers form a **core module in BLISS**, with data captured here being interconnected with and utilised across various other modules and reports. Therefore, maintaining accurate and correctly formatted Register data is essential for the **seamless functioning of the tool and consistency of information across modules**.

Tip: *Always check the blue-highlighted syntax before entering or uploading Register data to ensure error-free processing and reliable data flow across BLISS.*

BLISS Tips #353: Generate Customized Report with Ease.

The Customized Report feature in BLISS allows users to generate reports based on their specific reporting requirements. Users (Reporters) can select the relevant report type, companies, and fields to create a report with only the required information.

Key Benefits:

- **Flexible reporting:** Generate reports based on specific information and business requirements.
- **Relevant insights:** Include only the required companies and data fields, avoiding unnecessary information.
- **Better analysis:** Organise key company information in a structured format for easier review and analysis.
- **Time-saving:** Quickly generate and download customised reports without manually compiling data.
- **Easy sharing & further use:** Download reports in Excel format for further analysis, reporting, or sharing.

 Copyright © 2026, CimplyFive

Test your Gray Matter!! Take our Quiz to find out!

1. The annual secretarial compliance report under Regulation 24A (2) is to be submitted to the stock exchange(s):

a) Within 30 days from the close of the financial year.
b) Within 45 days from the close of the financial year.
c) Within 60 days from the close of the financial year.
d) Along with the quarterly financial results for Q4.

2. Under the Model Code of Conduct, the trading window must be closed:

a) Automatically for every designated person throughout every quarter.
b) Whenever the compliance officer determines that a designated person or class can reasonably be expected to possess UPSI.
c) Only when SEBI gives a written direction.
d) Only for directors, never for their immediate relatives.

3. Where an IPO's issue proceeds, excluding the offer-for-sale portion, are proposed to be used predominantly for capital expenditure, the minimum lock-in of the promoters' minimum contribution is:
a) 6 months from listing.
b) 1 year from allotment.
c) 18 months from allotment.
d) 3 years from allotment.

4. Unspent CSR amount relating to an ongoing project must first be transferred to the Unspent CSR Account within:
a) 15 days of year-end
b) 30 days of year-end
c) 60 days of year-end
d) 6 months of year-end

5. For homebuyers to initiate CIRP against a developer, the minimum joint threshold is:
a) 50 allottees or 5%, whichever is lower
b) 100 allottees or 10%, whichever is lower
c) 100 allottees and 10%, both mandatory
d) 10% of total financial creditors in all cases

 Copyright © 2026, CimplyFive

Board Leaders Integrated Software Solution

BLISSPLUS

BLISSPLUS is a Cloud hosted software that automates the routines, provides an e-repository, timely alerts, and a real-time dashboard, all aimed at ensuring compliance and good corporate governance. By doing so, it provides complete peace of mind to the Board of Directors and assurance to professionals by providing them with real-time compliance status with respect to the Companies Act, 2013. It also has multiple premium features like Directors view, facility to store past Secretarial records, automated compliance tracker for size- based compliance under the Companies Act, 2013.

BLISSLISTED

BLISSLISTED is an advanced variant of BLISSPLUS for Listed Companies with Companies Act,2013 and SEBI's LODR 2015 compliances integrated to provide a single point compliance automation, risk manager & e-repository for secretarial records including past secretarial records.

BLISSDOCS

BLISSDOCS is an Android/IOS based Board app for Directors which provides secure access to Board documents on Tablets/mobile phones, enhancing Directors productivity and making the Board meetings efficient & effective

CIMPLYBEST

CimplyBest is a tailormade software for Indian Corporates in conducting Corporate Board Evaluation which will optimize Board's Time & Effort with confidentiality assured.

Clear Compass

Clear Compass is an All-law Compliance Software to ascertain, track and manage all the applicable state, central and industry-specific laws.

CAIRR LODR Integrated

CAIRR is a free to use website from CimplyFive that provides at your fingertips, an integrated view of the Companies Act, 2013, IB Code, 2016 and LODR, 2015. The site and app are updated every business day by 11 AM for changes in the Act & Regulations. For more details, please visit www.ca2013.com

Compliance Calendar for the month of October 2026

Compliances under Companies Act 2013		
ADT-1	Section 139 of the Companies Act, 2013	To be filed 15 days from the date of AGM
AOC-4 AOC-4 (XBRL)	Section 137 read with Rule 12 Section 137 and read with Companies (Filing of documents and Forms in XBRL) Rules	To be filed 30 days from the date of AGM
MGT-15	Section 121 read with 31(2) of the Companies (Management and Administration) Rules 2014	To be filed within 30 days from the date of AGM
MSME-1	Section 405 of the Companies Act, 2013 read with Companies (Furnishing of Information about payment to micro and small enterprise suppliers) Order, 2019.	To be filed on or before 31st October
MGT-7 MGT-7A	Section 92 of the Companies Act, 2013 Section 92 of the Companies Act, 2013 read with Rule 11 of the Companies (Management and Administration) Rules 2014	To be filed 60 days from the date of AGM
MGT-8	Section 92 of the Companies Act, 2013 read with Rule 11(2) of the Companies (Management and Administration) Rules, 2014	To be filed 60 days from the date of AGM
Compliances under SEBI (LODR),2015		
Indian Depository Receipt holding pattern (Only for Listed entities which has issued IDR).	Regulation 69(1)	14th October 2026
Shareholding Pattern	Regulation 31(1) (b)	21st October 2026
Disclosure of number of complaints pending at the beginning of the quarter, received during the quarter, disposed of and remaining unresolved.	Regulation 13(3A)	21st October 2026
Integrated Filing – Governance (Statement on redressal of investor grievances, Compliance Report on Corporate Governance)	Regulation 13(3) Regulation 27(2) Regulation 30	30th October 2026

Annual Compliances under PIT regulations		
SDD Compliance Certificate or a Practising Company Secretary (PCS).	Regulation 3(5)	21st October 2026
Annual Compliances under LLP Act, 2008		
LLP Form -8	Section 34(3) of the Limited Liability Partnership Act, 2008	30th October 2026
SEBI (Depositories and Participants) Regulations, 2018		
Reconciliation of share capital audit report.	Regulation 76	30th October 2026

Gist of regulatory changes in Companies Act, 2013, SEBI (LODR) 2015, SEBI (PIT) Regulations, 2015 and Insolvency & Bankruptcy Code, 2016 in the month of September 2026.

- **22/09/2026**

Insolvency and Bankruptcy Board of India (Liquidation Process) (Fifth Amendment) Regulations, 2026

The notification deals with the **modification of entries in the list of stakeholders during the liquidation process** , enabling the liquidator to modify an entry upon coming across additional information and intimate the Adjudicating Authority regarding any such modification within thirty days of the modification being made.

About CimplyFive

Mission

Provide a cost-effective, secure web-based, menu driven, subscription services that provides curated resolutions, timely alerts and informative dashboards to free the management bandwidth for pursuing business goals

Vision

Leverage research and technology to eliminate procedural non-compliance risk for entities regulated by the Indian Companies Act, 2013

Solution for Quiz
1. c
2. b
3. d
4. b
5. b



To view the previous issues of *iComply* click here