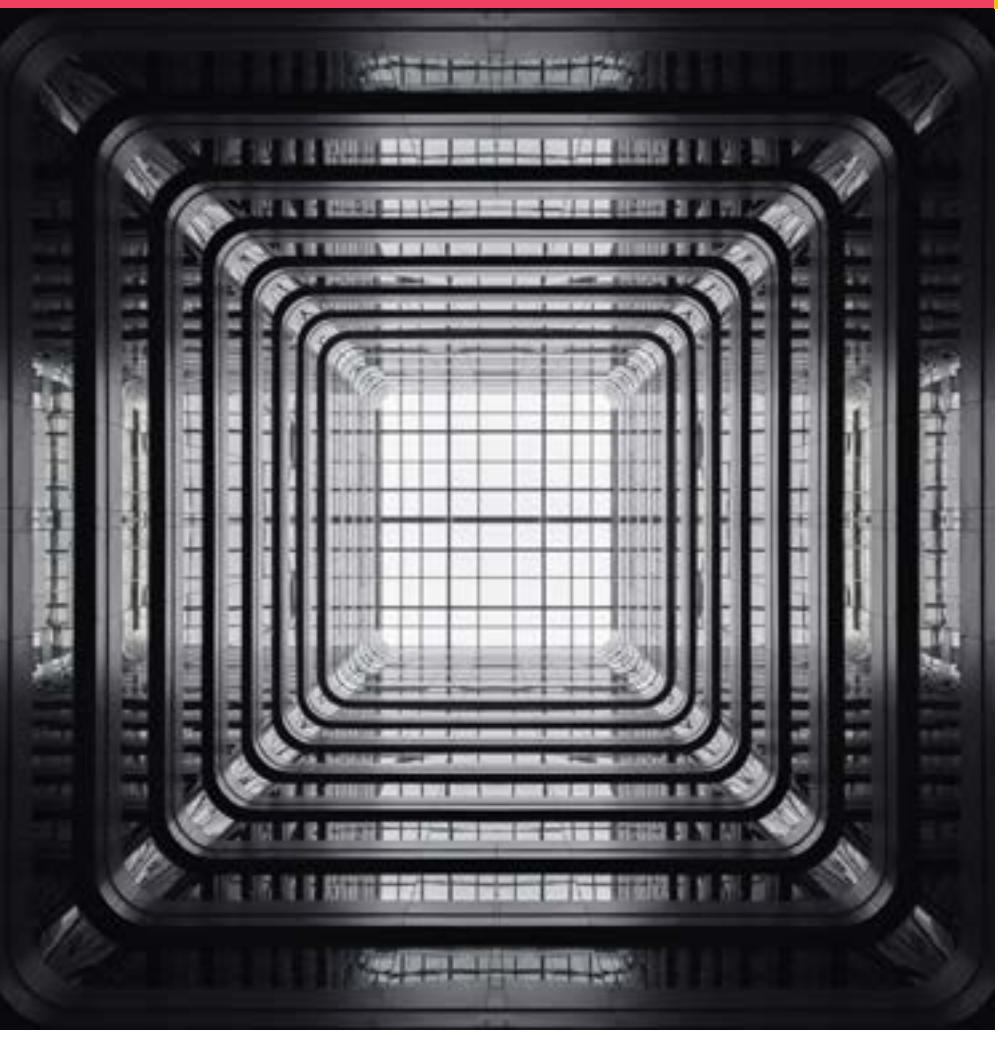
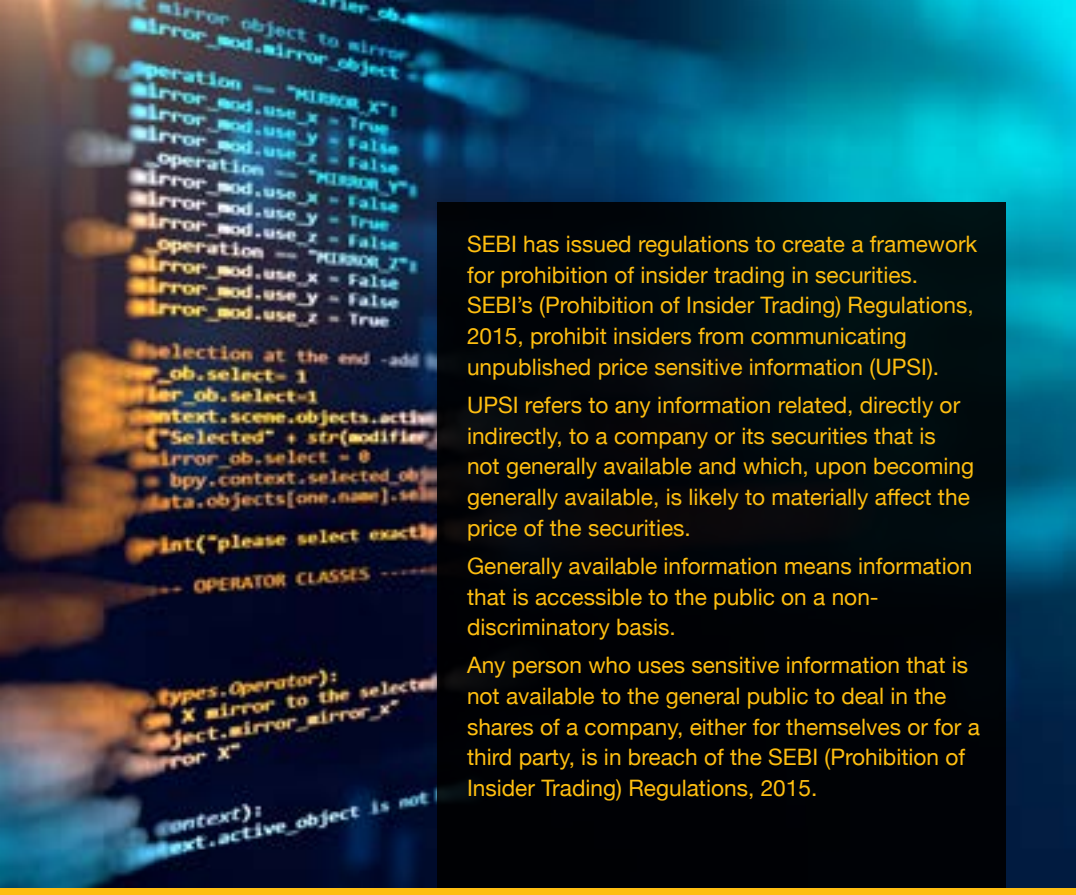
UPSI: Why and how you need to keep it safe



pwc



SEBI has issued regulations to create a framework for prohibition of insider trading in securities. SEBI's (Prohibition of Insider Trading) Regulations, 2015, prohibit insiders from communicating unpublished price sensitive information (UPSI).

UPSI refers to any information related, directly or indirectly, to a company or its securities that is not generally available and which, upon becoming generally available, is likely to materially affect the price of the securities.

Generally available information means information that is accessible to the public on a non-discriminatory basis.

Any person who uses sensitive information that is not available to the general public to deal in the shares of a company, either for themselves or for a third party, is in breach of the SEBI (Prohibition of Insider Trading) Regulations, 2015.

Implications of a breach

Obligation related to communication of UPSI

As per Section 3(1) of the SEBI (Prohibition of Insider Trading) Regulations, 2015, no insider shall communicate, provide, or allow access to any UPSI relating to a company or securities listed or proposed to be listed to any person, including other insiders, except where such communication is in furtherance of legitimate purposes, performance of duties or discharge of legal obligations.

According to Section 3(2A) of the SEBI (Prohibition of Insider Trading) Amendment Regulations, 2018 (w.e.f. 1 April 2019), the Board of Directors of a listed company shall create a policy for determination of 'legitimate purposes' as a part of 'Codes of Fair Disclosure and Conduct' formulated under regulation 8.

According to Section 5 of the SEBI (Prohibition of Insider Trading) Amendment Regulations, 2018 (w.e.f. 1 April 2019), the board of directors shall ensure that a structured digital database is maintained containing the names of such person or entities, as the case may be, with whom information is shared under this regulation along with the Permanent Account Number (PAN) or any other identifier authorised by law where PAN is not available. Such databases shall be maintained with adequate internal control and checks such as time stamping and audit trails to ensure non-tampering of the database.

Prohibition of unlawfully procurement of UPSI

As per Section 3(2), no person shall procure UPSI or cause the communication by any insider of such information relating to a company or securities listed or proposed to be listed, except in furtherance of legitimate purposes, performance of duties or discharge of legal obligations.

Prohibition of insider trading

As per Section 12A Clause (e) of the SEBI Act, 1992, no person shall directly or indirectly deal in securities while in possession of material or non-public information, or communicate such material or non-public information to any other person, in a manner which is in contravention of the provisions of this act or the rules or regulations made thereunder.

Penalties

As per Section 15G of SEBI Act, 1992, and the subsequent amendment in 2010, a minimum penalty of INR 10 lakh, which may be up to INR 25 crore, or three times the amount of profits made out of insider trading, whichever is higher, can be levied. In addition, if any person contravenes or attempts to contravene, or abets the contravention of the provisions of the SEBI Act or of any rules or regulations made thereunder, he shall be punishable with imprisonment for a term which may extend to 10 years, or with a fine, which may go up to INR 25 crore, or with both.

What you need to do

To ensure compliance with the requirements given in the SEBI (Prohibition of Insider Trading) Regulations, 2015, and to prevent insider trading, the Chief Executive Officer, Managing Director or such other analogous person of a listed company, intermediary or fiduciary has to put in place an adequate and effective system of internal controls. The internal controls shall include the following:

- All employees who have access to UPSI are identified as designated employees.
- All UPSI shall be identified and its confidentiality shall be maintained as per the requirements of the SEBI (Prohibition of Insider Trading) Regulations, 2015.
- Adequate restrictions shall be placed on the communication or procurement of UPSI, as required by the SEBI (Prohibition of Insider Trading) Regulations, 2015.
- A list of all employees and other persons with whom UPSI is shared shall be maintained and confidentiality agreements shall be signed or notice shall be served to all such employees and persons.
- All other relevant requirements specified under these regulations shall be complied with.
- A periodic process review shall be conducted to evaluate the effectiveness of such internal controls.

Information security risks

While current and former employees are the source of most insider compromises, trusted business partners can also commit or unwittingly facilitate a breach. Employees, third parties and business partners with trusted or authorised access can be a particular risk because most organisations do not adequately assess their information security practices.

Generally, the teams involved in handling UPSI are the finance and accounts team, investor relations, legal and corporate secretarial team, taxation team, MD, CEO, the CFO office, board of directors, audit committee, statutory auditors, and tax consultants.

Companies need to ask themselves if they have adequate controls in place over UPSI. An indicative list of questions that can be used for self-evaluation is provided below:

- Is an information security policy in place?
- Are there standard operating procedures (SOPs) to identify, classify, process and store UPSI?
- Is there a complete inventory of the information systems used to process and store UPSI?
- What data, if stolen, would result in a serious business risk?
- How is protection of these high-value assets prioritised?
- Are there enough controls in place to address the risk of loss of confidentiality of UPSI?
- What are the potential risks and vulnerabilities related to applications, infrastructure and network components used in relation to UPSI?
- How is access to the information systems restricted to authorised users only?
- How are information systems designed to protect UPSI from unauthorised changes and access?
- What monitoring controls have been put in place to detect any potential instances of unauthorised change, access or intrusion, or leakage of data?

How we can help

- Gap assessment of IT process followed vis-à-vis company's policies, procedures and good practices
- Diagnostic review of application configurations, operating systems and databases to identify security gaps
- Segregation of duties assessment
- IT landscape assessment
- Preparation of information security policy and SOPs for clients' IT processes
- Data flow diagram across various systems
- Mapping of sensitive information to the information systems
- Assistance in conducting training and awareness programme

Our approach

We follow a phased approach to understand the client's current state of readiness to meet the information security requirements related to UPSI. Based on our assessment of risks and evaluation of controls for safeguarding UPSI, we recommend best practices.

Understand	Evaluate	Identify	Recommend
Gain an understanding of the current environment	Evaluate risk and controls put in place	Identify gaps	Recommend improvements
• Policies and procedures • Roles and responsibilities of various teams in relation to UPSI • Identification, classification and handling of UPSI • Channels used for sharing of information • Current state of information security • Mechanism to identify breach of confidentiality/ response to incidents	• Identify teams/ persons and IT and business process in relation to UPSI • Define risk assessment criteria for handling of UPSI • Conduct risk assessment and evaluate current state of controls over UPSI for team/persons and information systems	• Identify gaps in the company's policies, procedures and best practices related to UPSI	• Discuss observations with management and submit a draft report along with a summary of recommendations for management review • Obtain management responses along with an action plan to address observations • Prepare an executive summary and submit a final report along with a summary of recommendations

Project management

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune.

For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity.
Please see www.pwc.com/structure for further details.

Contacts

Monil Gala
Partner
Telephone: + 91 98330 55589
Email: monil.gala@pwc.com

pwc.in

Data Classification: DC0

SG/May2019-17469