



## Software Technology Parks of India, Bangalore

Society under Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

# Setting high standards of service

- India at a glance
- Why Karnataka
- CMM Level 5 companies
- Other Important sites
- Performance Analysis
- STPI Holiday List
- STPI B'lore contacts
- Feedback

Home > [OCTAVE®](#)

### O is for OCTAVE

INDIA'S ONLY IT BUSINESS WEEKLY!

EX|P|R|E|S|S  
**Computer**

### Trend

### O is for OCTAVE

OCTAVE has emerged as the preferred security methodology in the security consulting space, says Abhinav Singh



OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning methodology for security developed by the Software Engineering Institute, Carnegie Mellon University's CERT team. OCTAVE differs from typical technology-focused assessments by focusing upon organisational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology. The US Secretary of Defence and Health Affairs has approved OCTAVE risk assessment as the preferred security risk assessment for

HIPAA compliance. This assessment method is being followed by various commercial and government organisations across the world. It is slowly surfacing in India where it has been adopted by organisations such as Software Technology Parks of India (STPI) Bangalore, Ascendus Technologies, a logistics company and a few others in the BFSI (banking, financial services and insurance) space.

SISA Information Security expert is sole implementer of OCTAVE in the Asia-Pacific region. The company has a tie-up with the Software Engineering Institute (SEI) at Carnegie Mellon University for OCTAVE related training and implementation. OCTAVE, which employs best practices such as the ISO 17799, HIPAA Privacy Laws, CERT Practices and NIST principles has helped organisations across the world to mitigate risks associated with critical assets.

### Faster implementation cycles

B Sankaralingam, deputy director, Software Technology Parks of India, Bangalore is upbeat about OCTAVE methodology. He says, "This [OCTAVE] methodology is flexible. We follow it as per our requirements and the implementation cycles are very short." Little wonder STPI Bangalore is the first organisation in India to go in for the OCTAVE methodology and it was implemented by SISA Information Security across STPI's departments in Bangalore in twenty days. Users of this methodology such as STPI, Bangalore feel that in case of other standards such as BS-7799 implementation cycles can range from one to two years depending upon the critical assets of an organisation. The faster implementation cycles have resulted in lesser efforts vis-à-vis other standards.

### Justifying investments

It is been claimed that as a security methodology OCTAVE helps an organisation in



OCTAVE helps in effectively identifying, measuring and mitigating security risks in an organisation.  
Dharshan Shanthamurthy,

Director,  
Operations,  
SISA Information



Sign in for a  
newsletter

## SoftLink

Internet access on  
a shared and  
premium basis  
[read more](#)

understanding the level of security risk an organisation and the amount of loss, which can occur in case of a security breach. Dharshan Shanthamurthy, director, operations, SISA, Information Security, says, "OCTAVE helps in effectively identifying, measuring and mitigating security risks in an organisation. It also helps an organisation in justifying any investment they might make in plugging security loopholes."

### **Reassuring clients abroad**

Many Indian companies especially BPOs have signed back to back Service Level Agreements (SLAs) with their customers which mandate that they have an effective and efficient security methodology in place. Companies developing software for their clients in the US need to build up a credible image to show prospective customers that they are following certain security initiatives. Says Vikram Narayan, chief executive officer, Ascendus Technologies that has recently adopted OCTAVE methodology within five days, "OCTAVE gives you a framework to think of security as an asset. Our software development house collects social security numbers from some of our clients in the US— which is a vital piece of information of a client. The OCTAVE methodology is very popular in the US and helps us reassure our client that their information is safe and secure with us."

With organisations such as STPI Bangalore going in for OCTAVE many others in the BFSI, BPO and the software development space are expected adopt this methodology.

#### **STPI Bangalore's the first Indian adopter**

STPI Bangalore was the first organisation in India to go in for OCTAVE. The implementation kicked off with the formation of a core analysis team of five people—one from SISA Information Security and four from various departments of STPI (such as IT, finance and administration) who knew the processes well. The goal of the team was to assess risk vulnerabilities at the departmental level. A supplementary analysis team was also formed with one person from SISA and four from STPI with the aim of collecting information from various departments. The full analysis team was trained on the OCTAVE methodology. A number of workshops such as an operational management workshop and a senior management workshop were conducted by SISA, and the process of identifying critical assets for different departments of STPI Bangalore began. After the assets were identified and organisational vulnerabilities noted, the analysis team took up penetration testing. A risk mitigation plan was drawn up as part of the assessment. Sankaralingam of STPI Bangalore says, "OCTAVE will go a long way towards protecting us against emerging threats associated with the service industry as it can be a stepping stone for any new security framework we may plan to implement in the future. Since OCTAVE has been adopted by the US Department of Defense, we at STPI wanted to reciprocate the same level of a security framework in our organisation as well."