

Security frameworks comparison

[Technology](#), [Information Technology](#)



COBIT, NIST and PCI DSS does not have a lot in common. One of the factors that distinguish the three is the fact that they are produced from different companies or organizations. However, it is worth noting that they are all security standards aimed at providing good security to business premises. In , addition these security standards are characterized by similar complex IT in their development and utilization.

Control Objectives for Information and Related Technology (COBIT)

Control Objectives for Information and Related Technology (COBIT) is a framework developed by ISACA for IT governance and management. Much of successful organizations understand the importance of Information technology in ensuring business success. Therefore, COBIT acts as a supporting toolset that enables managers to bridge the gap between technical issues, control requirements and business risks. The business orientation of the Control Objectives for Information and Related Technology consists of linking business goals to IT goals, providing maturity and metric models to measure their success and identifying the associated obligations of business and Information Technology process owners. The unique nature of COBIT is that: its focus is illustrated through a process model that subdivides Information Technology into 4 domains and 34 processes in line with the responsibility areas of planning, developing, running and monitoring, providing the much needed view of IT (Brand, 2007).

NIST from National Institute of Standards and Technology

Founded in the year 1901, the National Institute of Standards and Technology is one of the US oldest physical science laboratories. NIST measurements support the smallest of technologies to the largest and most

complex of human made creations. Much of its developed technology ranges from earthquake resistant skyscrapers to wide-body jetliners to world wide communication networks. The lab assists the industry in the development of technology that helps in: improving product quality, modernization of the manufacturing processes and facilitation of rapid commercialization of products based on current scientific discoveries (NIST monograph, 1900).

PCI DSS from the PCI Standards Council

Data security standard (PCIDSS) is one of the security standards offered by PCI security standards council. The PCI data security standard (PCI DSS) provides an actionable framework for building a full-bodied payment card data security process which comprise of detection, prevention and appropriate reaction to security incidents. Data Security Standard (PA-DSS) was developed to help in provision of definitive data standard for software vendors that develop payment applications. Its uniqueness is bestowed upon the fact that it is aimed at preventing development of payment applications for third parties from storing prohibited secure data including CVV2, magnetic stripe or PIN (Wright, 2011).

References

Brand, K., Boonen, H., & IT Service Management Forum. (2007). IT governance based on CobiT® 4. 1: A management guide. Zaltbommel: Van Haren Publishing.

NIST monograph. (1900). Gaithersburg, Md.: U. S. Dept. of Commerce, National Institute of Standards and Technology.

Wright, S. (2011). PCI DSS: A Practical Guide to implementing and Maintaining Compliance. Ely: IT Governance Pub.