IT & CYBERSECURITY AUDITOR SERIES

AUDITING THE CYBERSECURITY RISK & CONTROL

GD. BINASETRA
KOMPLEK BIDAKARA
JL. GATOT SUBROTO KAV 71-73
JAKARTA SELATAN 12870

11 - 12
NOVEMBER

24 CPE

3 HARI

Rp. 5.000.000,-
(ANGGOTA IIA)

Rp. 6.000.000,-
(NON ANGGOTA IIA)

Deskripsi Pelatihan

Serangan cybersecurity meningkat dan berkembang sangat cepat sehingga lebih sulit daripada sebelumnya untuk mencegah dan mempertahankannya. Apakah organisasi Anda memiliki metode efektif untuk mendeteksi, menggagalkan, dan memantau ancaman eksternal dan internal untuk mencegah pelanggaran keamanan? Kursus ini membantu Anda menguasai teknik dan alat khusus yang terbukti diperlukan untuk menerapkan dan mengaudit Kontrol Keamanan Kritis sebagaimana didokumentasikan oleh Pusat Keamanan Internet (CIS).

Ketika ancaman berkembang, keamanan organisasi juga harus. Untuk memungkinkan organisasi Anda tetap di atas skenario ancaman yang selalu berubah ini, SANS telah merancang kursus komprehensif tentang cara menerapkan Kontrol Keamanan Kritis, pendekatan keamanan berbasis risiko yang diprioritaskan. Dirancang oleh para ahli sektor publik dan swasta dari seluruh dunia, Kontrol adalah cara terbaik untuk mem-blokir serangan yang diketahui dan mengurangi kerusakan dari serangan yang sukses. Mereka telah diadopsi oleh pemerintah, universitas, dan banyak perusahaan swasta.

Kontrol adalah panduan spesifik di mana CISO, CIO, IGs, administrator sistem, dan personel keamanan informasi dapat digunakan untuk mengelola dan mengukur efektivitas pertahanan mereka. Mereka dirancang untuk melengkapi standar, kerangka kerja, dan skema kepatuhan yang ada dengan memprioritaskan ancaman paling kritis dan pertahanan pembayaran tertinggi, sambil memberikan garis dasar umum untuk tindakan melawan risiko yang kita semua hadapi.

MATERI PELATIHAN

- *Introduction and Overview of the Critical Security Control:*
- *Critical Control 1: Inventory of Authorized and Unauthorized Devices*
- *Critical Control 2: Inventory of Authorized and Unauthorized Software.*
- *Critical Control 3: Secure Configurations for Hardware and Software on Laptops,Workstations, and Servers*
- *Critical Control 4: Continuous Vulnerability Assessment and Remediation*
- *Critical Control 5: Controlled Use of Administrative Privileges*
- *Critical Control 6: Maintenance, Monitoring*
- *Critical Control 7: Email and Web Brows-er Protections*
- *Critical Control 8: Malware Defenses*
- *Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services*
- *Critical Control 7: Email and Web Brows-er Protections*
- *Critical Control 8: Malware Defenses*
- *Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services*
- *Critical Control 10: Data Recovery Capability (validated manually)*
- *Critical Control 11: Secure Configurations for Network Devices such as Fire-walls, Routers, and Switches*
- *Critical Control 16: Account Monitoring and Control*
- *Critical Control 17: Security Skills As-sessment and Appropriate Training to Fill Gaps (validated manually)*
- *Critical Control 18: Application Software Security*
- *Critical Control 19: Incident Response and Management (validated manually)*
- *Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)*

LAPTOP REQUIRED!

INFO:
DEWI / DITA
021 8378-2174
0812 8805-7901
info@iia-indonesia.org
www.iia-indonesia.org

The Institute of Internal Auditors Indonesia