Pelatihan

Cyber Series

CPD POINTS | ERMA | LSP MKS | LSP GRK Certification Holder

16 Learning Hours

Auditing Cyber Security

Audit Kemanan Siber

Creating Resilience Mastering Sustainability

CRMS Center for Risk Management & Sustainability ™

Winner of SNI Award 2024

crmsindonesia.org

CRMS Center for Risk Management & Sustainability™

Auditing Cyber Security

Sinopsis

Di tengah meningkatnya serangan ransomware, kebocoran data, dan insiden rantai pasok yang menimpa organisasi di Indonesia, asurans independen atas kontrol keamanan siber bukan lagi pilihan, di mana auditor internal serta tim risiko dan kepatuhan dituntut untuk dapat mengaudit risiko siber dengan metode yang terstruktur dan tertelusur. Kini keamanan siber juga telah bergeser dari sekadar urusan teknis menjadi tanggung jawab tingkat pimpinan organisasi. Bahkan di Indonesia, tuntutan regulator agar organisasi dapat membuktikan bahwa kontrol benar- benar berjalan semakin tinggi.

Program pelatihan intensif dua hari ini membekali auditor dan profesional manajemen risiko untuk merencanakan, melaksanakan, dan melaporkan audit keamanan siber yang kredibel, mulai dari kerangka kerja dan penilaian risiko hingga kontrol teknis dan pelaporan hasil audit keamanan siber, menggunakan rujukan dari NIST, CIS, COBIT, dan ISO/IEC 27001.

MENGAPA PROGRAM INI PENTING

Akuntabilitas UU Pelindungan Data Pribadi (UU 27/2022)

Ekspektasi ketahanan siber OJK dan Bank Indonesia

Standar dasar dan panduan keamanan nasional BSSN

Meningkatnya insiden ransomware dan kebocoran data

Meningkatnya kebutuhan auditor yang kompeten di bidang siber

Manfaat

- Membedakan audit dari asesmen, penilaian kerentanan (*vulnerability assessment*), dan uji penetrasi (*penetration test*), serta menjelaskan peran dan nilai tata kelola auditor.
- Menerapkan kerangka kerja terkemuka: NIST CSF 2.0, CIS Controls v8, COBIT 2019, ISO/IEC 27001, serta UU PDP Indonesia dalam pekerjaan audit nyata.
- Merencanakan audit keamanan siber berbasis risiko: menetapkan ruang lingkup dan tujuan, menyusun program audit, memilih sampel, dan mengumpulkan bukti yang andal.
- Mengevaluasi kontrol tata kelola dan manajemen, seperti kebijakan, risiko pihak ketiga, akses dan identitas, manajemen insiden, serta kelangsungan bisnis.
- Menilai kontrol teknis keamanan jaringan dan *cloud*, pengamanan sistem komputer (*system hardening*), patch and *vulnerability management*, serta uji penetrasi.
- Mendokumentasikan temuan dan menyusun laporan stratejik dengan prioritas.

Peserta

Pelatihan ini direkomendasikan untuk:

- Auditor internal dan auditor TI yang ingin berkembang ke bidang keamanan siber
- Profesional bidang tata kelola, manajemen risiko, dan kepatuhan
- Pimpinan dan manajer keamanan informasi & keamanan TI
- Auditor eksternal, regulator dan penyedia jasa asurans
- Pemilik kontrol dan staf pendukung komite audit
- Profesional pada jalur karier CISA / CISSP / audit siber

Silabus

HARI 1: Fondasi, Kerangka Kerja & Perencanaan		HARI 2: Pelaksanaan & Pelaporan	
Dasar-Dasar Audit Keamanan Siber	• Audit vs. asesmen vs. VA vs. pentest • Jenis-jenis audit • Peran auditor dan nilai tata kelola • Proses audit keamanan siber • Pemantauan dan peningkatan berkelanjutan	**Audit Tata Kelola & Manajemen Keamanan Siber**	• Kebijakan & prosedur • Tata kelola & pengawasan • Peran, tanggung jawab & akuntabilitas • Risiko pihak ketiga / vendor • Klasifikasi aset & data • Manajemen akses & identitas • Pelaporan KPI / KRI • Manajemen insiden & BCP/DRP
Standar, Kerangka Kerja & Regulasi Audit	• NIST CSF 2.0 • CIS Controls v8 dan Benchmarks • COBIT 2019 • ISO/IEC 27001 (ISMS) • Undang-Undang Pelindungan Data Pribadi	**Audit Keamanan Teknis**	• Audit jaringan, aplikasi & cloud • Kontrol preventif (enkripsi, DLP) • Kontrol detektif (pemantauan, IDS/IPS) • Hardening sistem & baseline aman • Manajemen patch & kerentanan • Uji penetrasi & temuan
Penilaian Risiko, Perencanaan & Metodologi Audit	• Identifikasi dan analisis risiko • Pelaku ancaman dan kerentanan • Penilaian dan prioritas CVSS • Ruang lingkup, program & checklist • Pengumpulan bukti dan sampling • Pemanfaatan hasil kerja pihak lain	**Pelaksanaan Audit, Pelaporan & Rekomendasi**	• Melakukan wawancara • Mendokumentasikan bukti • Mengidentifikasi celah kontrol • Mengevaluasi efektivitas kontrol • Menyusun laporan audit • Peta jalan remediasi • Pelaporan kepada pimpinan organisasi
Studi Kasus & Latihan praktik	• Identifikasi dan analisis risiko • Pelaku ancaman dan kerentanan • Penilaian dan prioritas CVSS • Ruang lingkup, program & checklist • Pengumpulan bukti dan sampling • Pemanfaatan hasil kerja pihak lain	**Studi Kasus & Latihan praktik**	• Presentasi studi kasus kelompok • Pembelajaran yang diperoleh • Perencanaan tidakan

Fasilitator

Program ini akan didampingi serta difasilitasi oleh host atau fasilitator ahli dari CRMS dan praktisi keamanan siber. Selain itu juga dapat mengundang pembicara tamu untuk berbagi pengalaman praktis dengan para peserta.

Andri Apriyana

Andri Apriyana, S.Si., M.M., CISA, CEH, CRMP, IRMP, GRCP, GRCA, IPMP, IAAP, ICEP, IDPP, IAIP adalah seorang praktisi dan konsultan senior dengan pengalaman lebih dari 23 tahun di bidang GRC (Governance, Risk, and Compliance), teknologi informasi, audit internal, dan keamanan siber. Saat ini beliau menjabat sebagai Founder dan CEO sebuah perusahaan konsultan, setelah sebelumnya sukses mengemban posisi strategis di firma Big Four global.

Kompetensi dan kredibilitasnya diperkuat oleh kepemilikan berbagai sertifikasi profesional internasional yang sangat relevan, antara lain Certified Information System Auditor (CISA), Certified Ethical Hacker (CEH) dengan skor kelulusan impresif mencapai 97,33%, serta Identity and Data Privacy Professional (IDPP).

Rekam jejak kepemimpinannya di dunia audit siber terbukti sangat solid, salah satunya saat menjabat sebagai Head of Group IT Audit di PT Astra International Tbk. Selama masa bakti tersebut, beliau memimpin kepatuhan dan audit IT tahunan untuk puluhan entitas anak perusahaan Astra Group dengan menerapkan audit berbasis risiko menggunakan standar global seperti COBIT 5, COSO, dan ISMS (ISO 27001). Di samping itu, beliau juga sukses merancang sekaligus mengimplementasikan kerangka kerja manajemen dan kontrol risiko siber lintas 7 sektor industri, serta aktif membangun talenta ethical hacker dan penetration tester internal melalui berbagai program pelatihan.

Sebagai seorang pakar, beliau juga diakui secara akademis melalui publikasi ilmiah internasionalnya di Springer International Journal of Big Data yang mengupas tuntas mengenai prediksi risiko siber menggunakan Big Data Analytic.

**catatan: fasilitator pelatihan dapat berubah sewaktu-waktu.*

CRMS | Center for Risk Management & Sustainability ™

Creating Resilience Mastering Sustainability

Registrasi

bit.ly/crms_acs

Jl Batununggal Indah Raya No.289
Bandung, 40266, Indonesia
Phone: (+62)22 8730 1035
Mobile: (+62)811 22 333 075

Email: secretariat@crmsindonesia.org
www.crmsindonesia.org