Durasi Materi Pelatihan: 2 hari
Durasi Ujian Sertifikasi: 1 hari

Deskripsi Materi Pelatihan:

Melatih peserta menjadi kompeten di bidang keamanan jaringan. Peserta akan mempelajari cara merencanakan, merancang, membangun, menerapkan, mengelola, menilai, mengukur, dan mengendalikan sistem keamanan jaringan.
Setelah mengikuti pelatihan, peserta akan dapat mengikuti ujian Auditor Keamanan Jaringan dan mendapatkan pengakuan kompetensi dari Badan Nasional Sertifikasi Profesi (BNSP).

Sasaran Peserta Pelatihan:

Peserta yang ingin mendapatkan sertifikasi **Auditor Keamanan Jaringan** berdasarkan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang Keamanan Informasi.

Tujuan Pelatihan:

Setelah mengikuti pelatihan ini para peserta akan siap mengikuti uji kompetensi dalam sertifikasi Auditor Keamanan Jaringan dengan unit kompetensi:

1. **J.62090.002.01** Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi
2. **J.62090.008.01** Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi
3. **J.62090.013.01** Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
4. **J.62090.019.01** Melakukan Kajian Keamanan Informasi
5. **J.62090.021.01** Mengelola Audit Keamanan Informasi
6. **J.62090.022.01** Melakukan Evaluasi Kinerja Keamanan Informasi
7. **J.62090.034.01** Mengkaji Efektivitas Penerapan Kontrol Akses
8. **J.62090.036.01** Melaksanakan Uji Coba Sistem Pertahanan Keamanan Informasi
9. **J.62090.037.01** Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
10. **J.62090.038.01** Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan

Garis Besar Materi Pelatihan :

Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi

- Mengidentifikasi kesesuaian prosedur keamanan informasi yang tepat untuk tiap klasifikasi dengan misi dan tujuan organisasi
- Mengidentifikasi kelemahan dari informasi dalam system komunikasi bisnis
- Menerapkan akses kontrol lingkungan komputasi yang sesuai
- Mengidentifikasi kesesuaian dalam mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi agar misi dan tujuan organisasi terwujud
- Mengidentifikasi kesesuaian pengumpulan dan pemeliharaan data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem agar misi dan tujuan organisasi terwujud

Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi

- Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi Lingkungan Komputasi
- Menerapkan ketentuan hukum keamanan system dan peraturan yang sesuai dengan infrastruktur system teknologi informasi yang didukung
- Mematuhi hukum/regulasi keamanan sistem informasi dan segala peraturannya untuk mendukung operasi fungsional dari lingkungan jaringan
- Mengidentifikasi dan/atau menentukan apakah sebuah insiden keamanan merupakan indikasi dari pelanggaran hukum yang memerlukan tindakan hukum tertentu
- Menyusun, menerapkan, dan menegakkan kebijakan dan prosedur yang mencerminkan tujuan legislatif hukum dan peraturan yang berlaku untuk lingkungan jaringan sistem informasi organisasi
- Memberikan dukungan dalam pengumpulan dan pelestarian bukti yang digunakan dalam proses penuntutan kejahatan computer

Mengelola Proses Sertifikasi dan Akreditasi Untuk Keamanan Informasi

- Memberikan saran kepada otoritas pemberi akreditasi atas setiap perubahan yang mempengaruhi postur/kondisi keamanan lingkungan jaringan system informasi
- Melaksanakan penilaian risiko sistem informasi selama proses sertifikasi dan akreditasi
- Menyiapkan atau melaksanakan pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi

Melakukan Kajian Keamanan Informasi

- Meneliti, mengevaluasi, dan menyediakan umpan balik atas seluruh tren dan pola permasalahan keamanan informasi pada sistem yang ditangani
- Menganalisis kajian keamanan informasi dan dokumentasinya untuk dampak strategis dan mengambil atau merekomendasikan tindakan yang tepat

Mengelola Audit Keamanan Informasi

- Melakukan kerjasama dengan pihak manajemen
- Menetapkan kontrol yang akan diperiksa dalam ruang lingkup audit
- Menetapkan peralatan untuk audit system informasi
- Memisahkan peralatan audit dari system operasional dan pengembangan
- Menetapkan tingkat keamanan tambahan bila dirasa perlu

Melaksanakan Evaluasi Kinerja Keamanan Informasi

- Menganalisis kinerja sistem untuk potensi masalahmasalah keamanan
- Menilai kinerja control keamanan di dalam lingkungan jaringan
- Memonitor kinerja system dan peraturan untuk memenuhi persyaratan keamanan dan privasi dalam lingkungan komputasi
- Melacak dan melaporkan semua butir tinjauan manajemen keamanan

Mengkaji Efektivitas Penerapan Kontrol Akses

- Mengevaluasi kontrol akses yang pernah ditetapkan
- Mengevaluasi kebijakan organisasi dan kebijakan password organisasi yang pernah ditetapkan
- Mengevaluasi pengelolaan akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya

- Mengevaluasi pengimplementasian peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan system teknologi informasi
- Mengevaluasi prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi
- Mengevaluasi kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan

Melaksanakan Uji Coba Sistem Pertahanan Keamanan Informasi

- Melaksanakan uji coba konfigurasi pengamanan yang telah disesuaikan dengan rencana uji coba dan prosedur-prosedurnya
- Mendukung desain dan pelaksanaan scenario latihan

Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran

- Mendeteksi potensi pelanggaran keamanan, mengambil tindakan yang sesuai untuk melaporkan kejadian tersebut sesuai dengan peraturan dan mengurangi dampak yang merugikan
- Memeriksa seluruh potensi atas pelanggaran keamanan untuk menentukan apakah kebijakan lingkungan teknologi jaringan telah dilanggar, menganalisa dan mencatat seluruh dampak dan juga menjaga barang bukti
- Mengidentifikasi kerentanan keamanan yang dari rencana implementasi atau kerentananyang tidak terdeteksi pada saat uji coba
- Melakukan tinjauan perlindungan keamanan tertentu untuk menentukan masalah keamanan (yang diidentifikasi dalam rencana yang telah disetujui) telah sepenuhnya ditangani

Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan

- Melaksanakan koordinasi kegiatan pemeriksaan, tes, dan tinjauan keamanan dalam lingkungan jaringan system informasi
- Melacak dan melaporkan hasil tinjauan kegiatan pengelolaan system informasi

- Melakukan penilaian fisik keamanan jaringan system informasi dan melakukan koreksi atas kelemahan keamanan fisik jaringan sistem informasi
- Memeriksa kerentanan posisi strategis dan menentukan tindakan untuk penanggulangannya