# الإدارة الاستراتيجية للأمن السيبراني

د. المهندس محمد جبار العبيدي

رؤية استباقية لإدارة المخاطر وبناء حوكمة سيبرانية متكاملة للمؤسسات المعاصرة

# محاور البحث الرئيسية

## أولاً: المعايير والمواءمة

مقدمة حول معايير الأمن السيبراني وعلاقتها الاستراتيجية بإدارة وضوابط المؤسسات الحديثة.

## ثانياً: الحوكمة والتشغيل

تفاصيل نموذج الخطوط الثلاثة (IIA) والربط بأطر العمل المرجعية (COBIT & NIST CSF).

## ثالثاً: النتائج والتكامل

الاستنتاجات والتوصيات، آليات التوثيق والتقييم، مع استعراض شامل لأبرز المصادر والمراجع.

# المقدمة: المعايير وإدارة المؤسسات

## عناصر أساسية في الحوكمة

تعد معايير الأمن السيبراني الصادرة عن الجهات المهنية (مثل معهد المدققين الداخليين IIA) مكملاً أساسياً للمعايير العالمية للتدقيق الداخلي.
إنها توضح كيفية حماية أصول المعلومات الحساسة ومواءمة أهداف الحماية مع الأهداف الاستراتيجية العليا للمؤسسة لدعم نموها المستدام.

## قابلية التطبيق والالتزام

لا يقتصر الأمن السيبراني على الجانب التقني البحت، بل يتطلب تقييماً سنوياً مستمراً للمخاطر وتحديداً دقيقاً للموارد اللازمة لدعم البنية الأمنية.
يتحمل قادة المؤسسة المسؤولية الكاملة عن تقييم مدى تطبيق المتطلبات الإلزامية وتوثيق أدلة الامتثال بدقة.

# الربط الاستراتيجي بأطر العمل العالمية

يعتبر الربط الاستراتيجي بين سياسات المؤسسة والضوابط المعتمدة خطوة حاسمة لضمان بيئة عمل آمنة وموثوقة:

- **إطار NIST CSF 2.0:** يركز على دورة الحماية من خلال ست وظائف رئيسية تتصدرها وظيفة الحوكمة لتوجيه بقية المكونات.
- **منهجية COBIT 2019:** بمثابة الجسر الناقل الذي يربط استراتيجيات تقنية المعلومات وصنع القرار التنفيذي بفعالية.
- **معيار ISO 27001:** يحدد المتطلبات الأساسية لبناء نظام شامل ومرن لإدارة أمن المعلومات (ISMS).

# نموذج الخطوط الثلاثة (IIA Three Lines)

**3**

**خطوط دفاعية تكاملية للحوكمة**

- **الخط الأول (الإدارة التشغيلية):** يمتلك المسؤولية المباشرة عن تطبيق الضوابط الوقائية والرقابة اليومية على الأصول والبرمجيات.
- **الخط الثاني (إدارة المخاطر والامتثال):** يتولى المراقبة المستمرة، ووضع السياسات الأمنية، ومتابعة سد الثغرات وتدريب الموظفين.
- **الخط الثالث (التدقيق الداخلي):** يقدم تأكيدات موضوعية مستقلة لمجلس الإدارة حول كفاءة خطوط الدفاع السابقة.

# ثلاثية الاستقرار: حوكمة، مخاطر، وضوابط

## الحوكمة (Governance)

تحديد الأهداف والسياسات، مع التقارير الربع سنوية المقدمة لمجلس الإدارة من رئيس إدارة أمن المعلومات (CISO).

## المخاطر (Risk Management)

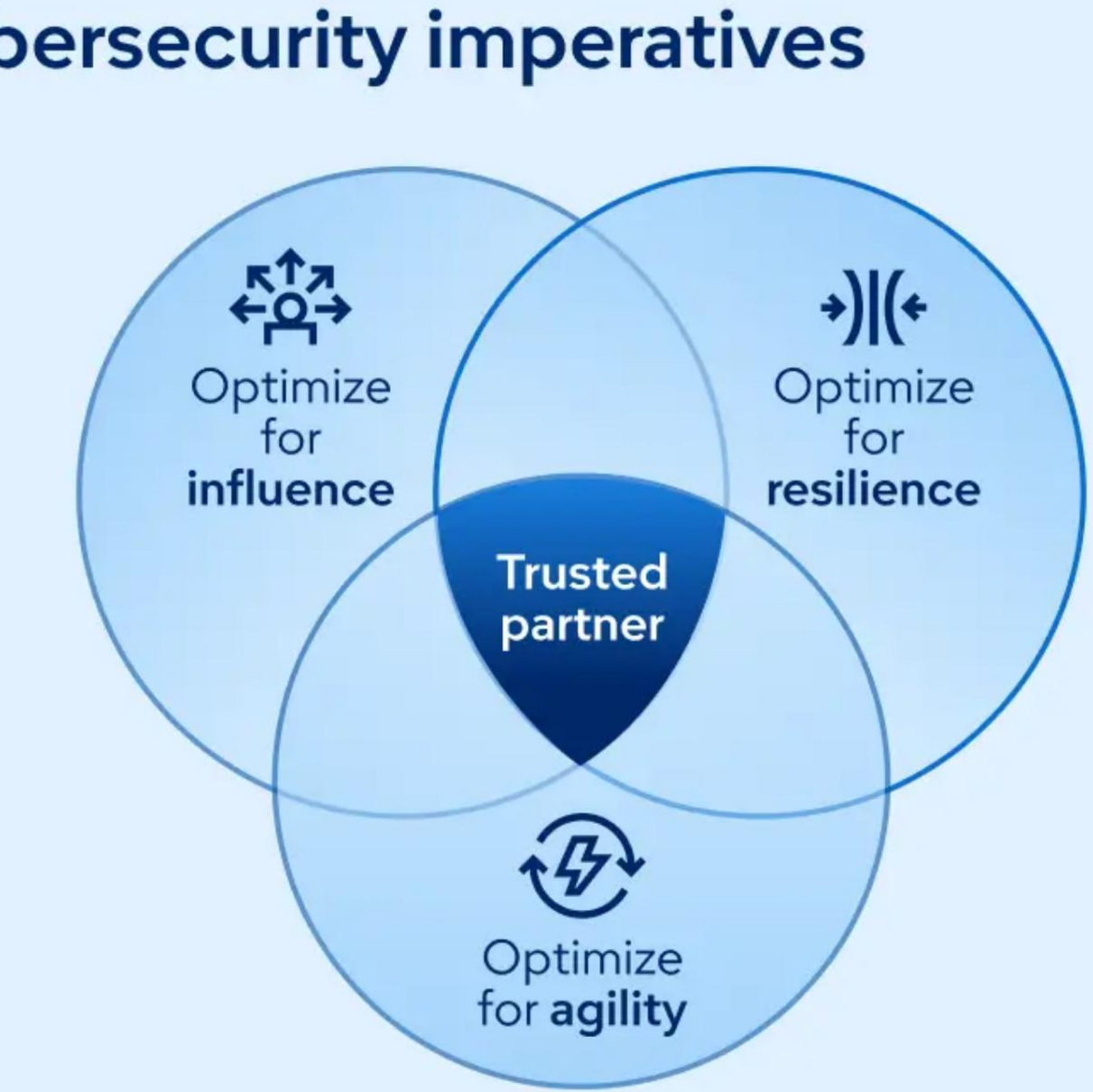
تحديد وتحليل التهديدات السيبرانية وتأثيراتها المالية والسمعة، وتطبيق إجراءات تصعيد سريعة عند حدوث خروقات مهددة.

## الضوابط (Controls)

إدارة وتأمين الأصول والبرمجيات طوال دورة حياتها، استخدام التشفير الشامل والمصادقة متعددة العوامل (MFA).

# مقارنة استراتيجية لمجالات الأمن السيبراني

| المجال الاستراتيجي | الهدف الأساسي | الارتباط بأطر العمل العالمية | دور مجلس الإدارة والإدارة التنفيذية |
|---|---|---|---|
| **الحوكمة السيبرانية** | توجيه الأهداف والسياسات وضمان توافقها مع رؤية المؤسسة | NIST CSF 2.0 (Govern Function) | إشراف استراتيجي واعتماد ميزانيات مستندة لتقييم الاحتياجات |
| **إدارة المخاطر السيبرانية** | تحديد وتحليل التهديدات وتحديد أولويات المعالجة | ISO 27005:2022 / COBIT 2019 | تحديد مستويات تحمل المخاطر المقبولة وإجراءات التصعيد السريع |
| **الرقابة والضوابط** | تنفيذ الحماية التقنية والتشغيلية للأصول الحساسة والشبكات | CIS Controls / ISO 27001 Annex A | تشغيل وتطوير البنية التحتية وإجراء الاختبارات الدورية |




# التأهب الاستراتيجي والتعافي

**جاهزية المؤسسة لمواجهة الأزمات**

يجب على القيادة الاستراتيجية تأسيس خطة استجابة موثقة ومُجرّبة للتعافي من الكوارث وحوادث الاختراق السيبراني بفعالية:

- **الكشف والاحتواء:** آليات رصد فورية لحصر الضرر ومنع انتشاره في الشبكة.
- **الاختبارات الدورية:** محاكاة سنوية للهجمات (تمارين الطاولة) لتدريب القيادة العليا.

# مناقشة واستنتاجات

- **الأمن كعنصر حاسم للحوكمة:** الاستنتاج الرئيسي هو أن الأمن السيبراني لم يعد مجرد قضية فنية لتقنية المعلومات، بل هو مكون حاسم لحوكمة الشركات وإدارة المخاطر على مستوى مجلس الإدارة.
- **الموازنة بين الضوابط والإنتاجية:** من الضروري الموازنة بين القيود الأمنية وسرعة أداء العمليات لضمان عدم إعاقة الأهداف التجارية للمؤسسة.
- **تفعيل دور الموارد البشرية والتدريب:** يجب تفعيل الوعي الأمني السنوي وحملات المحاكاة للموظفين بوصفهم خط الدفاع الأخير والأهم في المنظومة.
- **الاستعانة بالمصادر الخارجية بوعي:** الاستعانة بخبرات خارجية لسد النقص المعرفي لا يعفي رئيس التدقيق الداخلي أو مجلس الإدارة من مسؤوليتهم الأساسية.

# موجز العرض والمراجع المعتمدة

## الخلاصة والموجز

إن حماية استمرارية أعمال المؤسسات تكمن في الربط الواثق والدائم بين الإجراءات التشغيلية والقرارات الاستراتيجية العليا. يتطلب النجاح تدفقاً مستمراً للمعلومات والتقارير بين CISO ومجلس الإدارة، مع تفعيل مستمر لأدلة توثيق الامتثال والأداء المستند للقياس الكمي.

## المصادر والمراجع الرئيسية


- معهد المدققين الداخليين (IIA) - "المعايير الخاصة بموضوع الأمن السيبراني" إصدار 2025.
- المعهد الوطني الأمريكي للمعايير والتكنولوجيا NIST CSF 2.0.
- الاتحاد الدولي لمراقبة وتدقيق نظم المعلومات ISACA - COBIT 2019.

# نشكركم على حسن استماعكم

الباب مفتوح الآن للمناقشة وتلقي استفساراتكم الكريمة حول محتوى المحاضرة

**مقدم العرض ومستشار الحوكمة**

د. المهندس محمد جبار العبيدي

# Image Sources

https://s3.envato.com/files/656218177/01_cyberguard_preview.__large_preview.png

Source: themeforest.net


---

https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/infographics/strategic-cybersecurity-imperatives.webp

Source: www.gartner.com