

# Kyberbezpečnost

## Povinnost ze zákona – dobrá pro všechny

**Kurz: 6. října 2020**

### Proč kyberbezpečnost?

- Kyberbezpečnost jako systém řízení bezpečnosti informací, chrání data nejen v informačních systémech, ale i na papíře a v hlavách lidí.
- Tento jednodenní vstup do všech podstatných oblastí informační bezpečnosti se zaměřením na praktické zkušenosti a fungující modely, vám umožní poznat tuto velkou oblast ve vazbách mezi jednotlivými částmi
- Jaký je rozdíl mezi kyberbezpečností, bezpečností informací a bezpečností ICT?
- Praktické použití principů řízení tak, aby bezpečnost informací byla funkční.
- Organizační zajištění kyberbezpečnosti.
- Jak zrealizovat analýzu rizik a jaké praktické výstupy z ní výtěžit?
- Aplikace technických a organizačních opatření požadovaných zákonem o kybernetické bezpečnosti.
- Na co nezapomenout při zvládání bezpečnostních incidentů?

### Kurz je určen pro:

- Management
- Management IT
- Manažery kybernetické bezpečnosti / Manažery ISMS
- Architektury kybernetické bezpečnosti / Bezpečnostní Architektury
- IT Architektury
- Vedoucí projektů
- Vhodné pro všechny, kteří si chtějí vytvořit přehled, co vše obnáší systém řízení bezpečnosti informací, co v této oblasti vyžadují normy pro ISO 27001 certifikaci a co zákon o kybernetické bezpečnosti.

### Získání certifikátu

- Po absolvování kurzu získáte kredity pro získání certifikátu „Certifikovaný Manager ICT“ (Certified Manager of ICT – CMICT).

### Proč Akademie ICT managementu?

Pozice ICT manažera se stává stále náročnější. Základní rozpor spočívá v požadované dvojroli. Na jedné straně se od CIO (Chief Information Officer) očekává schopnost komunikovat s vrcholovým managementem a obchodními jednotkami o podpoře a realizaci strategických cílů (ICT enablement and alignment), na druhé straně statutární orgány předpokládají, že CIO je manažer orientovaný na efektivní řízení ICT provozní továrny (ICT management and control). Kombinace těchto dvou požadavků klade na CIO v moderní společnosti nebývalé nároky. Po mnoha letech strávených v ICT oblasti a nejen v ní se skupina sdružená kolem TATE International a časopisu Data Security Management rozhodla usnadnit současnému CIO plnění jeho dvojrole systémem vzdělávacích kurzů vycházejících z dlouholeté světové i lokální praxe.

# Kyberbezpečnost

Datum kurzu: 6. října 2020

Počet kreditů: 8

08:45–09:00	<b>Registrace účastníků</b>
09:00–10:00	<b>IT a Kyberbezpečnost</b> <ul style="list-style-type: none"><li>■ Bezpečnostní perimetr versus Digitalizace, Cloud a Enterprise mobilita</li><li>■ Otevírání se světu v IT znamená pestřejší hrozby a výrazně horší důsledky pro korporace</li><li>■ Probíhá „Renesance Kyberbezpečnosti“ a otevírání se světu znamená hlubší a intenzivnější aktivitu v Kyberbezpečnosti a propojení s ostatními částmi bezpečnosti</li></ul>
10:00–10:05	<b>Přestávka na kávu</b>
10:05–10:50	<b>Procesy nutné pro Kyberbezpečnost</b> <ul style="list-style-type: none"><li>■ Místo a určení bezpečnosti informací a kyberbezpečnosti v organizaci (proč je mít a k čemu slouží, stanovení rozsahu působnosti v kontextu organizace, oblasti bezpečnosti a praktické zásady)</li><li>■ Systém řízení bezpečnosti informací a kyberbezpečnosti</li></ul>
10:50–11:00	<b>Přestávka na kávu</b>
11:00–12:00	<b>Procesy nutné pro Kyberbezpečnost</b> <ul style="list-style-type: none"><li>■ Řízení kyberbezpečnosti (systém řízení, procesy, podřízenost, odpovědnosti, bezpečnostní role, organizační struktura, outsourcing a řízení dodavatelů)</li><li>■ Analýza rizik a dopadů (metody, principy, realizace, výstupy pro ISMS/BCMS a jejich použití v praxi)</li></ul>
12:00–12:45	<b>Přestávka na oběd</b>
12:45–13:45	<b>Kyberbezpečnost – právní minimum</b> <ul style="list-style-type: none"><li>■ 4 oblasti zákonné oblasti</li><li>■ Dopady na management a odpovědnosti managementu</li></ul>
13:45–14:00	<b>Přestávka na kávu</b>
14:00–15:00	<b>Kyberbezpečnost v provozu IT (ICT bezpečnost)</b> <ul style="list-style-type: none"><li>■ Role a odpovědnosti (rozhraní kyber a ICT bezpečnosti, ISMS/ZKB vs. ITIL)</li><li>■ Aplikace bezpečnostních opatření v praxi</li></ul>
15:00–15:10	<b>Přestávka na kávu</b>
15:10–15:50	<b>Kyberbezpečnost v provozu IT (ICT bezpečnost)</b> <ul style="list-style-type: none"><li>■ Technická opatření (praktická aplikace požadavků InfSEC a/nebo zákona o kybernetické bezpečnosti)</li></ul>
15:50–16:00	<b>Přestávka na kávu</b>
16:00–16:45	<b>Zvládání bezpečnostních incidentů</b> <ul style="list-style-type: none"><li>■ Proces Security Incident Management a jeho zařazení v organizaci (vazby na BCM, BCP a DRP, ICT Change management a Incident management, ..., externí vazby na NCKB, PČR, CERT/CSIRT, ...)</li><li>■ CERT-CSIRT-ISIRT-SOC tým (role, klíčové role, zařazení v org. struktuře, činnosti a pravomocí, trénink)</li></ul>
16:45–16:55	<b>Přestávka na kávu</b>
16:55–17:25	<b>Kulatý stůl Q&amp;A (moderovaná diskuse)</b>
17:25–17:30	<b>Závěr kurzu</b>

## LEKTORŮ

### JUDr. Josef Donát, LL.M.

■ Josef je držitel prestižního ocenění Právník roku v oblasti práva ICT za rok 2014, je vedoucím specializace Právo ICT advokátní kanceláře ROWAN LEGAL a zapsaným mediátorem. Ve své praxi se dlouhodobě věnuje rozsáhlým projektům v oblasti outsourcingu IT, cloud computingu, elektronického dokazování, kybernetické bezpečnosti, ochrany osobních údajů a dodávek informačních systémů. V poslední době se intenzivně věnuje dopadům nařízení eIDAS do našeho právního prostředí.

### Ing. Lukáš Klášterský

■ Lukáš v současnosti působí v oblasti IT Infrastruktury v Erste group - předního poskytovatele finančních služeb ve střední Evropě. V rámci více než 20 let profesního působení v oblasti IT a telekomunikací má bohaté zkušenosti s poskytováním ICT služeb, realizací projektů a transformací s přesahy do oblasti digitalizace a bezpečnosti, expertní znalosti ICT trendů. Působil na manažerských pozicích debis IT Services Czech (později T-system), Lucent technologies, Telefonica O2, Česká pojišťovna/Generali Group.

### Ing. Richard Michálek

■ Richard Michálek má více než 20 let praxe v oboru systémové integrace, sítí, informační bezpečnosti a business continuity. Během těchto let působil na různých manažerských a technických pozicích v Armádě ČR, konzultantské společnosti i velké nadnárodní korporaci. Soustředil se na praktické výstupy systémů řízení a použití bezpečnostních technologií. Svě zkušenosti z dlouholeté praxe a mnoha úspěšných projektů nyní uplatňuje jako nezávislý konzultant pro bezpečnost informací a business continuity.

### Michal Wojnar

■ Konzultant a manažer, který se bezpečnosti věnuje přes 9 let a dohromady má 12 let praxe v informačních technologiích. Vede 15členný tým spadající pod oddělení Cyber & Privacy společnosti PwC, kde dnes pracuje dohromady 40 bezpečnostních konzultantů. Do portfolia Michalova týmu spadají služby v oblastech implementace ISMS, bezpečnostní auditů či analýza kybernetických rizik včetně cloudových řešení. Dlouhodobě se věnuje problematice nastavení „security posture“ organizace, strategií a zejména motivaci týmů v celém spektru KB. Michal je držitelem certifikací CISA, CISSP a CEH. Pravidelně se věnuje přednáškové činnosti, vzdělávání a konzultacemi top-managementu a je členem PV IS2 a redakční rady DSM.

## P Ř I H L Á Š K A



Termín:  
6. října 2020

**Kyberbezpečnost**

Společnost:	<input type="text"/>	Oblast podnikání:	<input type="text"/>
Adresa:	<input type="text"/>	PSČ:	<input type="text"/>
IČ:	<input type="text"/>	DIČ:	<input type="text"/>
Jméno:	<input type="text"/>	Příjmení:	<input type="text"/>
Funkce:	<input type="text"/>	Telefon:	<input type="text"/>
E-mail:	<input type="text"/>	Fax:	<input type="text"/>
		Předplatitel DSM: ne <input type="checkbox"/> ano <input type="checkbox"/>	č. předplatitele: <input type="text"/>

Zúčastním se: kurzu  workshopu  Zálohovou fakturu: ne  ano

Účastnický poplatek ve výši  Kč včetně DPH prosím uhradte na účet TATE International, s.r.o. číslo **574171183/0300** u ČSOB a.s. Praha 1, IČ: 25148125, DIČ: CZ25148125.

Variabilní symbol: IČ firmy (soukromá osoba uvede číslo 9999).

Všechny bankovní poplatky spojené s registrací hradí účastník.

Dne:  Podpis:  Razítko:

Vyplněnou přihlášku zašlete **faxem na číslo 257 313 695** nebo využijte možnosti **registrace na aict@tate.cz**.

**Akademii ICT managementu pořádá TATE International, s.r.o.,**

vydavatel časopisu DSM - data security management, Hořejší nábřeží 21, 150 00 Praha 5,  
tel.: +420 257 920 319-20, fax: +420 257 313 695, e-mail: aict@tate.cz.

### Informace a účastnický poplatek

**Cena kurzu včetně workshopu**

**11.900 Kč + DPH 21%**

Délka kurzu je 8 hodin. Počet kreditů za tento kurz je 8.

Workshopy jsou součástí všech bloků.

Účastnický poplatek kurzu zahrnuje kompletní studijní materiály a malé občerstvení.

**V případě přihlášení 3 dny předem se poplatek navyšuje o 1.000,- Kč.**

TATE International, s.r.o. si vyhrazuje právo zrušit kurz, pokud se na něj přihlásí méně jak 6 účastníků. V tomto případě Vám budou vráceny všechny již zaplacené poplatky.

### Storno poplatky:

do 15-ti dnů před termínem konání kurzu se účtuje storno poplatek 1.000,- Kč. Do 3 dnů před zahájením kurzu je storno poplatek 50% z ceny kurzu. Později jsou storno poplatky 100% z ceny kurzu.

### Detaily placení:

Platit můžete bankovním převodem nebo zálohovou fakturou, kterou obdržíte na vyžádání.

Po obdržení platby na náš účet Vám vystavíme daňový doklad a zašleme potvrzení účasti. Všechny poplatky musí být uhrazené na účet organizátora nejpozději den před konáním kurzu.

### Místo konání:

PWC  
City Green Court  
Hvězdova 1734/2c,  
140 00 Praha 4