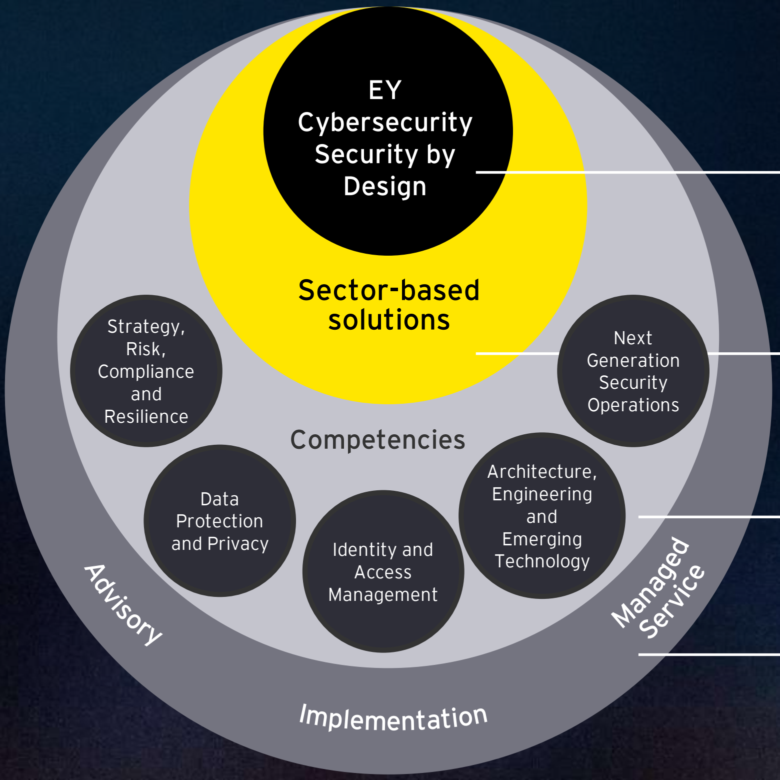
EY Cyber Security and Data Privacy

Facilitating trust and shaping the future of cyber security

EY
Building a better
working world

In a nutshell

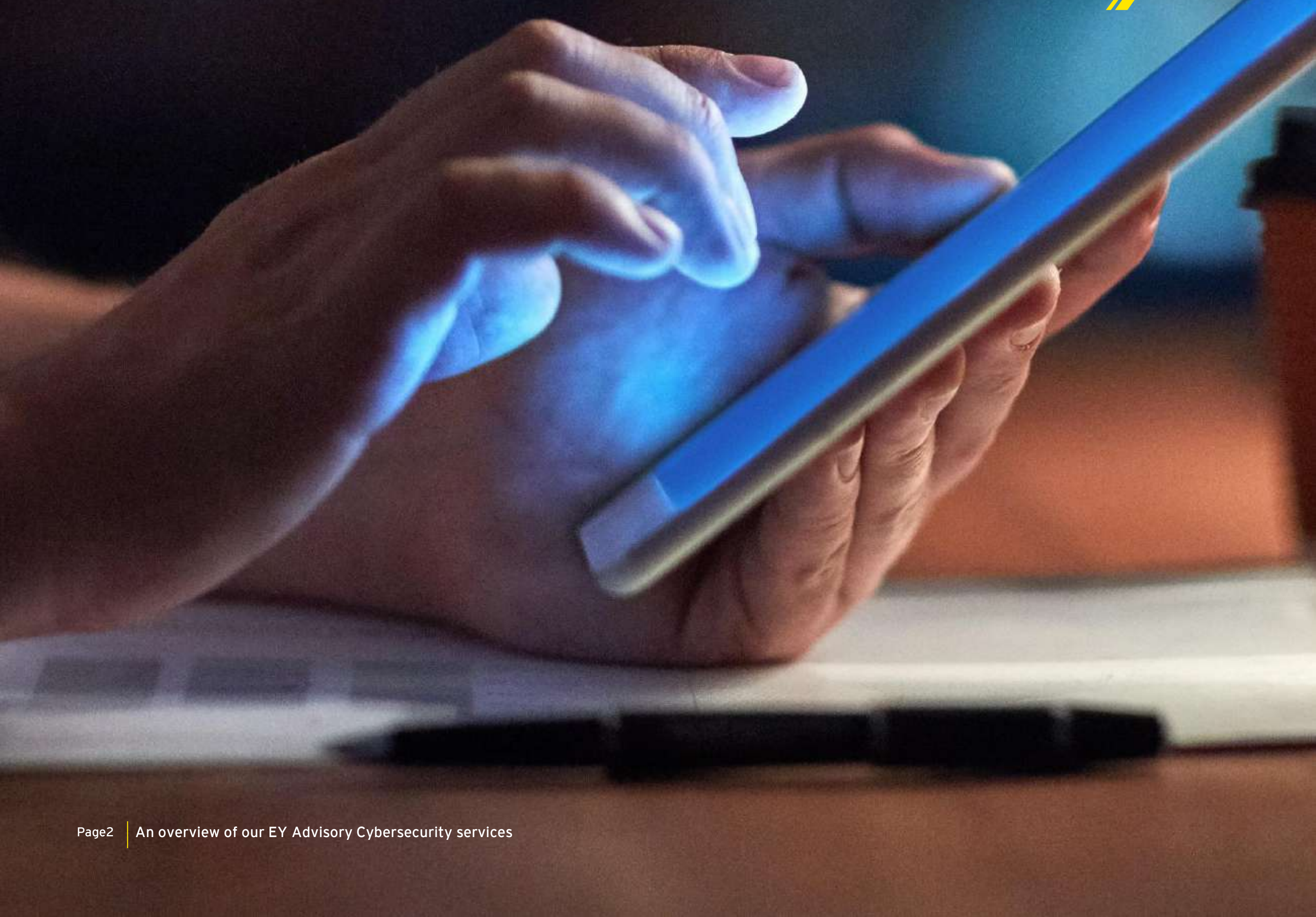

EY Cybersecurity Security by Design
Sector-based solutions
Strategy, Risk, Compliance and Resilience
Next Generation Security Operations
Competencies
Data Protection and Privacy
Identity and Access Management
Architecture, Engineering and Emerging Technology
Advisory
Managed Service
Implementation

EY Cybersecurity enables trust in systems, design and data, so that organizations can take more risks, make transformational changes and enable innovation with confidence.

We accomplish our mission by developing solutions that can be used to assure security and resilience of key business transformation initiatives and/or business functions.

These solutions are built using talent, experience and capabilities which reside within our 5 competencies.

We deliver solutions to our customers as part of a design, implementation or run phase of an engagement.



Cybersecurity and business resilience overview

EY Cybersecurity enables trust in systems, design and data, so that organizations can take more risks, make transformational changes and enable innovation with confidence.

Cyber strategy, risk, compliance and resilience

These solutions help organizations evaluate the effectiveness and efficiencies of their program in the context of business growth and operations strategies. The solutions apply consistently, regardless of where they are applied (IT, IoT, OT, Cloud), provide clear measurement of risks and capture current risks to the organization and demonstrate how cyber risks will be managed going forward.

Data protection and privacy

These solutions are designed to help organizations protect their information over the full data lifecycle – from acquisition to disposal. Our service offering helps companies and organizations stay up to date with data security and data privacy good practices, as well as compliance with regulations, in a constantly evolving threat environment and regulatory landscape.

Identity and access management

These solutions are designed to help organizations with their definition of access management strategy, governance, access transformation, and ongoing operations. The solutions help organizations ensure that the right users validate who they are and get access to the right organization resources.

Architecture, engineering and emerging technology

These solutions are designed to help organizations protect themselves from adversaries that would seek to exploit weaknesses in the design, implementation, and operation of their technical security controls, including disruptive technologies in the marketplace.

Next generation security operations and response

These solutions help organizations proactively identify and manage risks, monitor threats, and investigate the effects of real-world attacks. These rapidly integrate cybersecurity functions and technologies to adapt to demands.

EY cyber strategy, risk, compliance and resilience services at a glance

Cyber strategy services

Cyber risk services

Cyber compliance services

Cyber resilience programs

EY security strategy, risk, compliance and resilience portfolio

This set of solutions help organizations evaluate the effectiveness and efficiencies of their cybersecurity and resiliency programs in the context of business growth and operations strategies. The solutions apply consistently regardless of where they are applied (IT, IoT, OT, Cloud), provide clear measurement of risks and capture current risks to the organization and demonstrate how cyber risks will be managed going forward. Each service can be combined to form a larger program or transformation effort.

Benefits

- Provide a clear picture of current cyber risk posture and capabilities, giving management and directors a view of how, where and why to invest in managing cyber risks.
- Implement and execute a strategy and overarching cyber program that allows for rigorous, structured decision making and financial analysis of cyber risks.
- Achieve and sustain regulatory compliance requirements as the outcome of a well-designed and executed cyber function.
- Build a more risk aware culture through education and awareness to minimize the impact of human behaviours.
- Operate a program that is resilient in the face of ever evolving cyber threats and digital business strategies.

EY cyber strategy, risk, compliance and resilience services

Cyber strategy services

Provides organizations with industry perspective on security capabilities, supports development of cost optimized operating models, and supports diligence and integration through M&A lifecycle.

- Cyber program accelerator (CPA)
- Cyber benchmarking and performance analysis
- Cyber strategy and roadmap
- Cyber operating model and organizational design
- Cyber cost optimization
- Cyber transformation and co-sourcing
- Pre-Transaction Cyber Assessment and due diligence
- Transaction cyber program strategy
- Post-transaction cyber program stand-up

Cyber risk services

Quantify cyber risks to the enterprise in financial terms, perform analysis driving business decisions on cyber risk treatment and educate key stakeholders on roles and responsibilities.

- Cyber risk management
- Cyber risk quantification
- Cyber metrics program
- Cyber performance dashboarding
- Cyber board reporting
- Cyber academy
- Security awareness-as-a-service
- Cyber marketing hub
- “Nth”-party security risk management
- Product security assessment and program management
- Supply chain security

Cyber compliance services

Helps organizations achieve, maintain and report on compliance with an ever-evolving, global cyber regulatory landscape.

- Policies, standards, processes and guidelines
- Compliance program readiness and remediation
- Compliance-as-a-service
- Cyber certification
- Cyber attestation

Cyber resilience services

Programmatic approach to identification, evaluation and implementation of cyber resilience measures.

- Secure business continuity management assessment, strategy and planning
- Secure business continuity Management exercises, simulations and testing
- Physical security and safety
- Cyber disaster recovery assessment, strategy and planning
- Cyber disaster recovery and restoration exercises, simulations and testing
- Global cyber disaster business restoration and recovery surge support
- Evidence-based resilience
- Crisis management program design and implementation
- Crisis operations command and control support
- Cyber crisis communications and public relations management

EY data protection and privacy capabilities at a glance

- Data protection and privacy assessment, strategy and transformation
- Data governance and data ethics
- High value asset (HVA) protection
- Data protection and privacy technology enablement
- Managed services
- Data protection and privacy awareness and training

EY data protection and privacy portfolio

EY's data protection and privacy services and solutions are designed to help organizations protect their information over the full data lifecycle – from acquisition to disposal. Our service offering helps organizations stay up to date with data security and data privacy good practices, as well as compliance with regulation, in a constantly evolving threat environment and regulatory landscape. In the event of misuse or breach of personal information, our services can help companies forensically identify the scope and nature of the misuse or breach, and take steps to remediate and report on the event.

Benefits

- Our portfolio of services support a more effective, maintainable data protection and compliance management posture, helping reduce associated costs. Moreover, it assists in protecting brand reputation through the protection of business, customer and other sensitive or regulated information. It empowers organizations to more effectively avert costly data breaches, and reduces risks of non-compliance that might lead to fines from regulators. If a breach should occur, our services will help companies remediate the breach and meet reporting obligations timely.

EY data protection and privacy services

Data protection and privacy assessment, strategy and transformation

Services to measure, design and improve the overall data protection and privacy strategy program and its governance.

- Maturity assessments and benchmarking
- Personal data compliance assessment through data analytics
- Assessment and remediation services related to regional, national, industry data protection and privacy regulations
- Strategy, roadmap and architecture design
- Policies, procedures, notices, and consent management
- Program governance and business alignment
- Program risk assessment and remediation
- Program design, build and operate
- Privacy audit
- Incident response planning and design
- Operating model design
- Metrics and program reporting
- Cloud strategy
- PCI compliance services

Data governance and data ethics

Services to measure, design and improve the data governance program. Support of data ethics strategy.

- Data governance
- Data governance strategy
- Data ethics assessment
- Data ethics strategy
- Policies and procedures
- Program design, build and operate
- Data exposure assessment
- Access monitoring
- Data ownership
- Data management

High Value Asset (HVA) Protection

Services to design and implement HVA protection programs, including identifying, classifying, governing and securing high value information.

- Data classification models and strategies
- Data labelling and tagging methods and approaches
- Data handling methods and approaches
- High value information asset identification, crown jewels identification across business units and functions
- Trade secret and intellectual property protection
- Insider threat assessment and protection
- Application and system data assessments
- Data discovery scanning

EY data protection and privacy services

Data protection and privacy technology enablement

Services to measure, design and improve the overall data protection and privacy strategy program and its governance.

- End to end system selection and implementation services for key data protection and privacy solutions
- Data protection:
  - Data loss prevention
  - CASB (Cloud Access Security Broker)
  - Encryption and tokenization
  - Information rights management
  - Data tagging and labelling
- Privacy:
  - Consumer rights process automation
  - Governance
  - PIAs, ROPAs, data flows
  - Privacy enhancing technologies
  - Data deletion

Managed services

Services to measure, design and improve the data governance program. Support of data ethics strategy.

- Data protection technology maintenance and support
- Data protection technology rule management and improvement
- Data protection technology event management and response
- IPA/DPO one platform IT maintenance and support
- End to end data subject rights process management
- Data privacy impact assessment execution support
- Record of processing activity and data mapping maintenance support
- Data breach support
- Data protection officer outsourcing
- Contract lifecycle management for vendor processing agreements

Data protection and privacy awareness and training

Services to design and implement HVA protection programs, including identifying, classifying, governing and securing high value information.

- Data protection and privacy awareness strategy design
- Data protection and privacy awareness and training content development
- Data protection and privacy training delivery
- Data protection and privacy workshops design and delivery
- Data protection and privacy wargame delivery

EY identity and access management capabilities at a glance

- Digital identity strategy and assessment
- Business integration and intelligence
- Identity and access management, privileged and multifactor solution engineering
- Managed identity
- Digital identity innovation

EY identity and access management (IAM) portfolio

This set of solutions helps support organizations with their definition of access management strategy, governance, access transformation and ongoing operations. IAM includes the processes and technologies collectively used to manage the lifecycle of digital identities (profiles) for people, systems, services and users, and is a crucial part of keeping a client's data and key resources protected from cyber attacks and limited to only those who should have access.

Benefits

- Enables digital initiatives at organizations by connecting technologies in use.
- Reduces cyber risks by giving management and directors a clear, granular view of who has access to what resource in the company and a framework for managing that access securely.
- Improves the efficiency of existing tools and processes and identifies opportunities to reduce costs associated with maintaining identities.
- Enables compliance with technical standards, laws, and regulations.
- Enhances user experiences in the access and use of critical systems and data.

EY identity and access management services

Digital identity strategy and assessment

Services to assess, design, and implement a digital identity strategy

- Business requirement analysis
- Strategy and roadmap definition - cloud, hybrid and on-premise
- Business case development
- Tools and technology rationalisation, evaluation and selection

Business integration and intelligence

Services to measure, design and improve access management models

- Identity data analytics and remediation
- Identity and access management operation optimisation
- Access model enhancement (ABAC, RBAC, ERBAC, SoD)
- Reporting and metrics improvement

Identity and access management, privileged and multifactor solution engineering

Services to design and implement architecture and technology to enable a digital identity strategy

- Identity and access architecture and design
- System integration and implementation
- Service deployment and transition
- Solution migration and optimisation

Managed identity

Service designed to transform, run, and, maintain Identity-as-a-service

- IAM transformation services
- Digital identity as a service, solution management
- Application onboarding

Digital identity innovation

Services designed to develop and test new identity models and methods

- Application onboarding factory
- Rapid prototyping
- Automated testing
- Visualization

EY architecture, engineering and emerging technology capabilities at a glance

Security architecture

- Security architecture transformation
- Architectural assessments
- Technical control design
- Secure integrations

Security engineering

- Security engineering transformation
- Technical implementation
- Security technology portfolio management
- Security engineering managed services

Emerging technologies

- Security solution development
- Emerging technology transformation
- Technical assessment implementation and integration
- OT/IoT security by design
- Security analytics for resilience
- OT/IoT implementation
- Security analytics and architecture
- OT/ICS and IoT operations and governance

EY security architecture, security engineering, and emerging technologies portfolio

EY's security architecture, security engineering, and emerging technologies services and solutions are designed to help companies protect their organizations from adversaries that would seek to exploit weaknesses in the design, implementation, and operation of their technical security controls, including disruptive technologies in the marketplace (e.g., cloud computing, blockchain, internet of things (IoT)/industrial control systems (ICS) devices, connected automotive, robotic process automation (RPA), etc.)

Benefits

- Our extensive portfolio of services and offerings enables EY to more comprehensively serve our organizations across multiple aspects of their cybersecurity portfolio.

Security architecture services

Security architecture transformation

Services to measure, design and improve the overall security architecture program and its governance.

- Security architecture strategy
- Security architecture assessment and design pattern development
- Policies and procedures
- Program governance and business alignment
- Program risk assessment and remediation
- Program design/build/operate
- Program strategy and roadmap design
- Operating model design
- Metrics and program reporting

Architectural assessments

Services to measure the effectiveness of an organization's security architecture, as well as frameworks they have adopted.

- Technical architecture assessments
- Technical control assessments
- Technology effectiveness assessment
- Application security architecture review and assessment
- SABSA (Sherwood Applied Business Security Architecture)
- TOGAF (The Open Group Architecture Framework)
- OSA (Open Security Architecture)
- O-ESA (Open Enterprise Security Architecture)

Technical control design

Services to design technical security solutions for our organizations, as well as processes to help them do so themselves.

- Secure Systems and Software Development Lifecycle (SDLC) process design and implementation
- DevSecOps process design and implementation
- Proof of value facilitation
- Technology strategy and requirements analysis
- Technology solution selection and evaluation
- Technology design and implementation
- Application security controls design
- Cloud security control design

Secure integrations

Services to enable our organizations to securely integrate their various corporate entities (e.g., mergers & acquisitions

- Secure integration approach design and implementation
- Current state security posture assessments before integration
- Integration fabric program design/build/operate
- Security technology portfolio rationalization for integrated entities
- DevSecOps pipeline integration
- Integration fabric risk assessment and remediation
- Metrics and program reporting

Security engineering services

Security engineering transformation

Services to measure, design and improve the overall security engineering program and its governance.

- Security engineering strategy
- Policies and procedures
- Program governance and business alignment
- Program risk assessment and remediation
- Program design, build and operate
- Program strategy and roadmap design
- Operating model design
- Metrics and program reporting

Technical implementation

Services to implement technical security solutions for our organizations, as well as processes to help them do so themselves.

- Use case workshops/definition
- Technology requirements analysis
- Technology solution selection and evaluation
- Technology design and implementation
- Technology deployment planning
- Technology operational processes creation
- Engineering documentation creation (e.g., schematics, diagrams, processes, procedures)
- Technology migration [SIEM]
- Technology uplift [Follow-up to prescriptive value path assessment]
- Application security controls implementation
- Secure SDLC
- Cloud security solution design and implementation

Security technology portfolio management

Services to continuously right size our client's security technology portfolio to maximize value to cost.

- Current state security technology assessment
- Use case analysis
- Scope of deployment analysis
- Utilization analysis
- Cost analysis
- Future state recommendations based on analysis

Secure engineering managed services

Services to continuously manage the security infrastructure for our organizations

- Security technology product management
- Security technology product deployments
- Security technology product upgrades
- Security technology product configuration changes
- Security technology product decommissions
- Cloud security monitoring

Emerging technology services

Security solution development

Services to measure, design and improve the overall state of security for emerging technologies.

- Point of view creation
- Alliance potential validation
- Security solution creation
- Go to market materials
- Policies and procedures
- Program risk assessment and remediation
- Program design, build and operate
- Program strategy and roadmap design
- Operating model design
- Metrics and program reporting

Technical assessment, implementation and integration

Services to assess the security of an emerging technology, implement changes to improve its security, and integrate the technology.

- Use case workshops and definition
- Technology requirements analysis
- Technology solution selection and evaluation
- Proof of concept/pilot
- Technology design and implementation
- Technology deployment planning
- Engineering documentation creation (e.g., schematics, diagrams, processes, procedures)
- Network segmentation
- Infrastructure configuration analysis

Security analytics for resilience

Services to apply advanced analytics to technical, network and systems configuration data to develop sustainable, data driven dependency mapping to effectuate resilience capabilities.

- Data source assessment
- Data driven asset mapping
- Use case workshop design and implementation
- Program strategy and roadmap

Security analytics and architecture

Design and implementation of bespoke analytics use cases and big data services to support client's security and business strategy.

- Custom analytical models
- Data centralization
- Architecture design
- Metrics and reporting

Emerging technology services (OT/ICS, IoT, Cloud)

Emerging technologies transformation

Security transformation programs driven by OT, IoT, cloud, and "smart" technologies

- OT/IoT cyber transformation programs
- OT/IoT security strategy
- OT/IoT transformational roadmap
- OT/IoT-specific processes and standards development
- OT/IoT security project and program management
- Smart buildings and city protection
- Smart factory and industry 4.0 protection

OT/IoT security by design

Secure design and implementation of OT, IoT, cloud and other "smart" technologies.

- Protection services (security assessments and penetration tests of emerging technologies with specific threat assessment [e.g., IoT, cloud impact])
- Smart sensors and actuators, cloud and IoT platform, connectivity assessment and protection
- Process safety (e.g., SIS/ESD systems)
- IT/OT network segmentation architecture
- OT asset management
- IoT architecture
- Cloud architecture
- SDLC and product security/connected products
- Regulatory requirements (EU NIS Directive, NIST CSF)

OT/IoT implementation and integration

Services to implement technical security for OT/IoT

- OT/IoT environment detection and monitoring, OT SOC, incident response
- IT/OT network segmentation
- OT extension of cyber security services (e.g., backup management, anti malware, active directory, asset management, vulnerability management, remote access)
- OT/IoT laboratory services (design, use, setup and implementation support)
- OT/IoT managed services

OT/ICS IoT operations and governance

Integration, convergence, standardization and harmonization across the organization to achieve successful management of cyber security with embedded OT/ICS and IoT technologies

- OT/ICS and IT security integration and convergence.
- IT/OT operating model design - security operations to prevent, detect, respond and recover from attacks
- OT organization structure definition of security roles, responsibilities and services to achieve risk management objectives
- OT security service operations
- OT security sourcing, insourcing, outsourcing
- OT security service catalogue
- OT/IoT security dashboards and KPIs

EY Next generation security operations and response capabilities at a glance

- Security operations center transformation
- SIEM design, deploy and management
- Incident readiness and response
- Cyber threat intelligence
- Attack and penetration testing
- Threat detection and response
- Vulnerability management
- Application security
- Insider threat management
- Threat hunting and compromise

EY next generation security operations and response portfolio

EY's next generation security operations and response services along with a deep portfolio of advisory, implementation and managed services, can help organizations build a transformation strategy and roadmap to implement the next generation of security operations, and provide the right amount of support to help you manage world-class security operations in a programmatic way.

Benefits

- Helps plan, design, build and optimize a world-class security operations center (SOC).
- Identifies and prioritizes capital and operational investments to help organizations apply effective defenses to cyber threats.
- Delivers just in time on-site support and remote incident response support to help quickly contain, eradicate an intruder that has compromised a client's digital assets and implement enhanced defenses to reduce risk going forward.
- Accelerates and sustains threat and vulnerability management effectiveness.
- Identifies vulnerable systems and networks through controlled penetration tests, dynamic and static application testing and helps organizations remediate to their acceptable risk tolerance.
- Monitors and responds to advanced threats via market leading technology and intelligence.
- Discover and manage critical system vulnerabilities which can act as points of entry into the environment.

The EY advantage

Speed to maturity

Ability to move your program up the maturity curve rapidly with proven methodologies, processes and technology

Lower start-up costs

No need for investment into significant staff and up-front capital to increase maturity and capabilities

Balanced investments

Helps organizations assure that a program is optimized to address risk within the context of the organization's risk appetite

Access to sector-specific innovation

Resources offer sector-specific knowledge and multidisciplinary experience and access to latest innovations

Improved trust

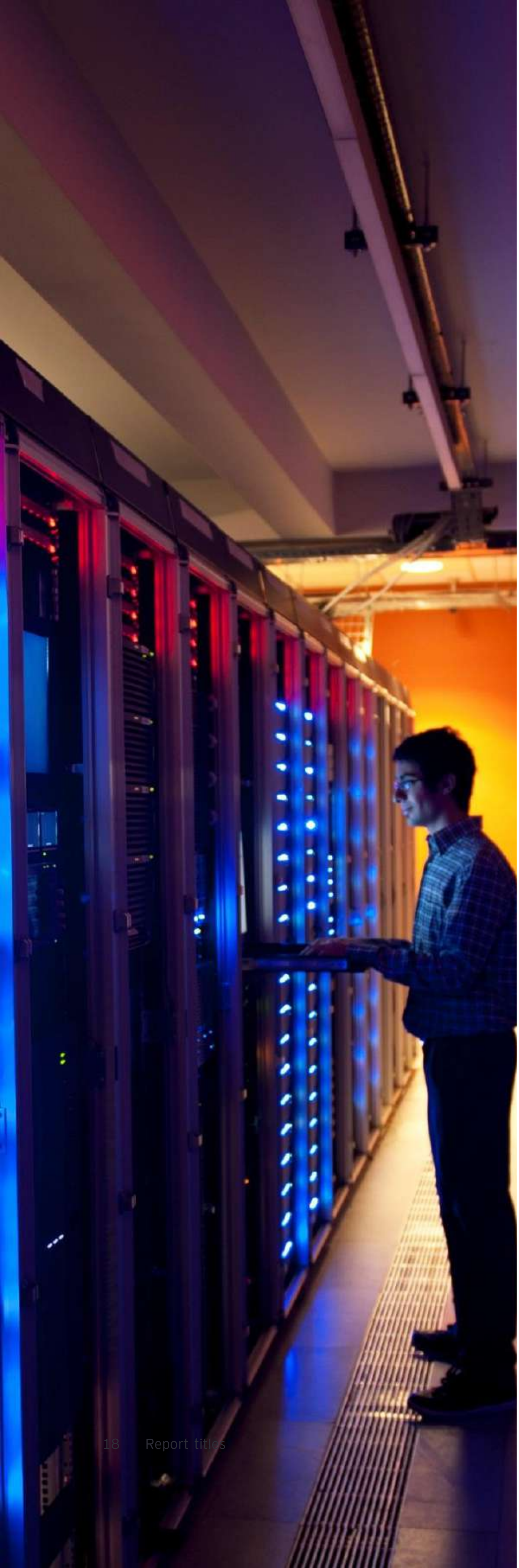
Facilitates cybersecurity trust into every business initiative from the beginning

Business aligned

Delivers integrated solutions aligned to business needs, not point solutions which add complexity and cost over time

Faster response time

Optimize processes and efficient operations to speed up response to crises



Ernst & Young LLP

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata – 700016

EYIN2012-006
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

SN

ey.com/en_in

@EY_India EY YouTube EY India EY Careers India @ey_indiacareers