EXCELIC INFOTECH

A Data Protection Company

Information Security
For
Healthcare Industry

About Excelic

For some, the path to excellence is a steady march. For others, it unfolds through bursts of innovation. But for the best of the best, it's both, disciplined improvement initiatives, marked by powerful leaps and breakthroughs. As the world's largest professional services firm, we help organizations build value and excellence by uncovering insights that create new futures and doing the hard work to improve performance.

Excelic's Profile - Overview

Excelic – specialist risk and compliance firm with expertise in IT risk management

Flexible "On Demand" Governance and Risk Consulting Services, Satellite presence in Middle East, India, Europe

Ex **Big 4 leadership** with combined 250+ years of professional services experience.

Risk and compliance expertise across industries, risk consulting services & operations; serving more than **100 clients across the globe**

15+ experts specialized in IT solutions with CISA, CISSP, ISO 27001, ISO 22301, OSCP certifications

15+	10+	15+
Seasoned Risk & Audit Professionals	IT Risk Management Professionals	Cyber Security Professionals

IT RISK MANAGEMENT TEAM

- Techno functional team to conduct application reviews.
- Pool of CISA, CISSP, CISM, OSCP, CEH, ISO27001 LA, CRISC and other relevant certified professionals
- Team with a good mix of industry and consultancy background
- Team with technical expertise in networks and infrastructure reviews
- Methodology aligned to the ISO 27001/ COBIT / ISF framework
- Large repository of technology risk and controls database
- Audit methodology and documentation practices aligned to the standards of international accounting bodies and industry best practices

A Snapshot of Our IT Risk Management Services

1 Cyber Risk and Security

- Cyber Risk Management
- Infra & App security assessments
- Enterprise security architecture review
- Secure SDLC review
- Identity & access management
- Cloud security and mobility security reviews

2 IT Governance and Compliance

- IT security policy & process review
- IT GRC (tools) review
- HITRUST, HIPAA, NIST, ISO alignment
- Data Governance
- GDPR & CCPA, SOX, SSAE16, PCI requirments

3 IT Risk Management

- ITRM framework design & rollout
- Third party InfoSec Reviews
- BCP & DR planning & implementation
- Software Asset Management

4 Forensic Investigation

- Evidence Acquisition
- Evidence Analysis
- Legal Documentation
- Forensic Data Reporting
- Legal Certification
- Court Depositions

5 Corporate fraud Prevention

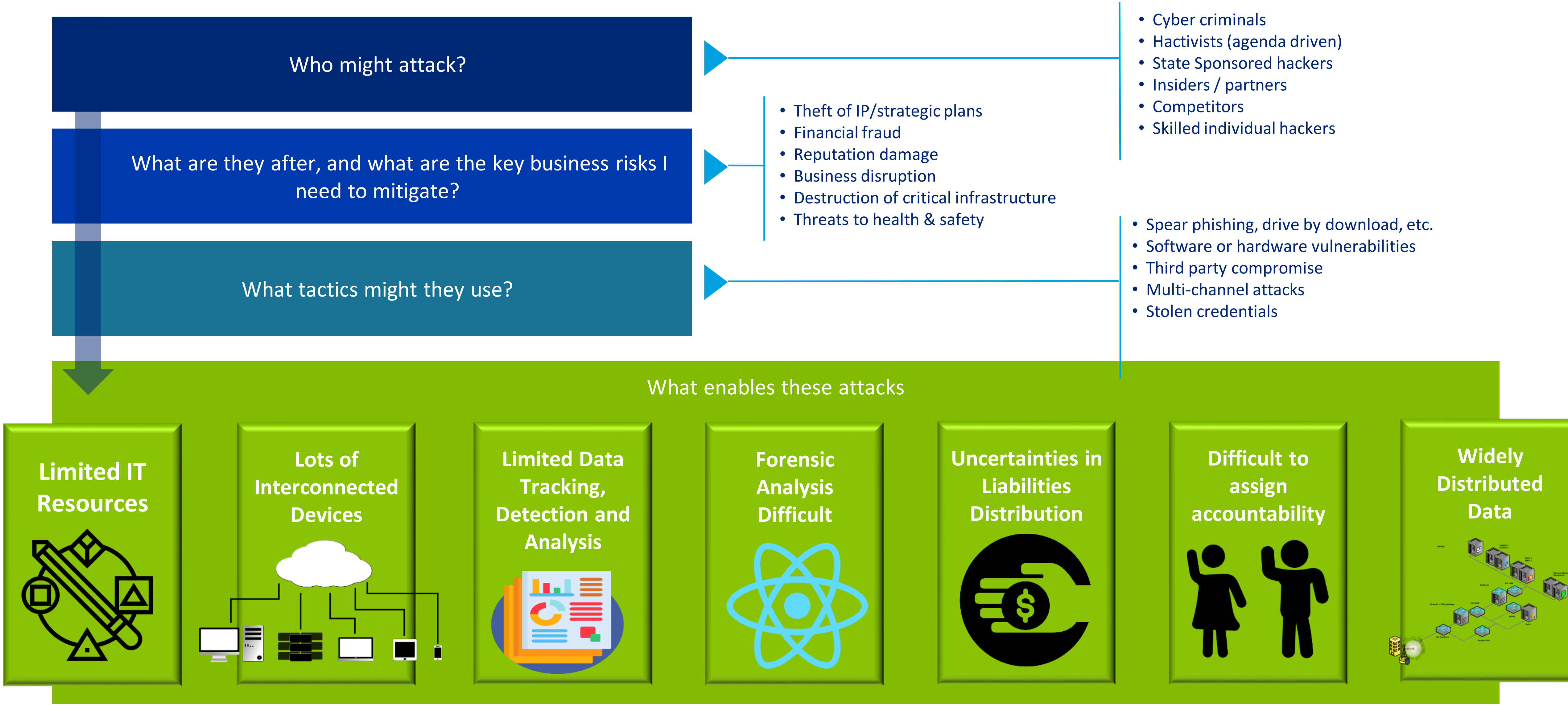
- Know your Employees
- Company Data Protection Policy
- Review IT Security Policies
- Data Protection Process
- Data Governance
- Legal Framework

Critical Patient Health Data

Personally identifiable information (PII) and *protected health information (PHI)* are handled by almost every department in a hospital, in one or more health information system. All healthcare providers (e.g., physicians, physician assistants, nurses, pharmacists, technicians, dietitians, physical therapists) use electronic health records (EHR), e-Prescribing software, remote patient monitoring, and/or laboratory information systems; the billing office works with insurance and financial information through medical billing software; scheduling and administration departments work with clinical data on scheduling software, and the list continues. PII in a hospital setting, the data is highly sensitive and valuable, yet almost all departments handle it at least in some manner. Cybersecurity measures aim to protect PII and PHI by securing devices, electronic systems, networks, and data from attacks.

Cyber Attacks on Hospitals

To manage cyber risks appropriately organizations must set risk appetite, and drive focus on what matters. Our Cyber Risk Management framework starts by understanding who might attack, why, and how.



Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- State Sponsored hackers
- Insiders / partners
- Competitors
- Skilled individual hackers

What are they after, and what are the key business risks I need to mitigate?

- Theft of IP/strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety

What tactics might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials

What enables these attacks

- Limited IT Resources
- Lots of Interconnected Devices
- Limited Data Tracking, Detection and Analysis
- Forensic Analysis Difficult
- Uncertainties in Liabilities Distribution
- Difficult to assign accountability
- Widely Distributed Data

Impact of the Cyber Attacks

Critical Equipment Unavailability

- Blood-product refrigerators
- Imaging equipment
- Automated drug dispensers
- Electronic health records
- Critical systems such as heating, ventilation, and air conditioning (HVAC)

Irreversible Data

- Stolen credit card can be replaced
- Genetic and Health Info cannot be replaced
- Medical Data used in Identity Theft
- Data used in Medical Fraud

Dark Web Data Publishing

- Medical Data highly in Demand on Dark Web
- Sells 20-30 times more
- Health Info is significantly valued
- By Hackers

Disruption in Services

- WannaCry Attack of May 2017
- Hollywood Presbyterian Medical Center attack of February 2016
- Surgeries had to be delayed
- Patients diverted to nearby hospitals

EHR Integrity Compromised

- Encrypted in an attack, such as ransomware
- Lose access to critical information
- Example patient allergies, current medications, and comorbidities

Urgent Cases Derailed

- stealth malware can stay hidden in the system until conveniently activated

Doctor-Patient Trust Breach

- Following a Data Breach

Compliance in Healthcare

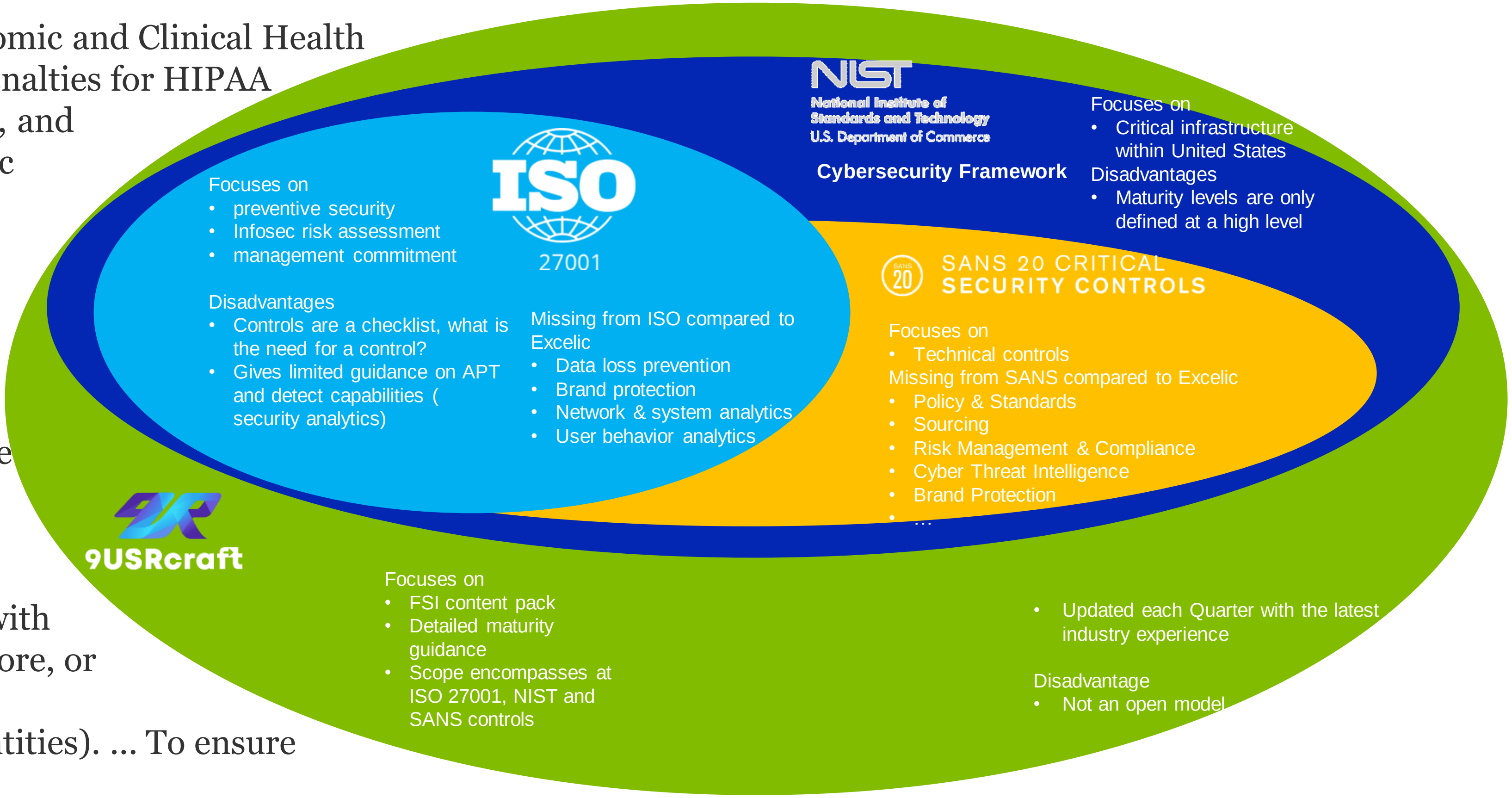
- In the United States (US), the Health Insurance Portability & Accountability Act (HIPAA) was passed in 1996; it enforced the protection of health information usage, disclosure, storage, and transmission

- Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, which increased penalties for HIPAA violations, strengthened breach notification, and encouraged the meaningful use of electronic health records

- Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, which increased penalties for HIPAA violations, strengthened breach notification, and encouraged the meaningful use of electronic health records

- In 2017, the FDA began mandating that medical device manufacturers show that their devices are able to have updates and security patches applied throughout their lifespan. As part of this same regulation, the FDA requires that a “bill of materials” be shared with buyers of a medical device.

- HDPSA applies to businesses that work with companies that create, receive, transmit, store, or maintain protected health information (HIPAA business associates and covered entities). ... To ensure that you are adequately safeguarding PHI.



ISO
27001
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Cybersecurity Framework
SANS 20 CRITICAL SECURITY CONTROLS
9USRcraft

Focuses on
- preventive security
- Infosec risk assessment
- management commitment

Disadvantages
- Controls are a checklist, what is the need for a control?
- Gives limited guidance on APT and detect capabilities (security analytics)

Missing from ISO compared to Excelic
- Data loss prevention
- Brand protection
- Network & system analytics
- User behavior analytics

Focuses on
- Critical infrastructure within United States

Disadvantages
- Maturity levels are only defined at a high level

Focuses on
- Technical controls

Missing from SANS compared to Excelic
- Policy & Standards
- Sourcing
- Risk Management & Compliance
- Cyber Threat Intelligence
- Brand Protection
- …

Focuses on
- FSI content pack
- Detailed maturity guidance
- Scope encompasses at ISO 27001, NIST and SANS controls

- Updated each Quarter with the latest industry experience

Disadvantage
- Not an open model

Cyber Risk Case Studies

Lukaskrankenhaus Neuss (Germany)

public hospital founded in 1911 in Neuss, Germany with 537 beds and 1400 employees

Who

Impact

Needed to postpone high-risk procedures .

The hospital reported that its backup system was kept up-to-date and only a few hours of data were lost, but a backlog of handwritten records from when the computer systems were offline need to be integrated with the remainder of the EHR eventually

In February 2016, employees encountered various error messages from a ransomware attack initiated through a social-engineering tactic. In response, the hospital took servers and computer systems offline to assess and cleanse infected systems. In the meantime, staff resorted to using pen, paper, and fax machines to continue their work.

What Happened

While the hospital did not receive a direct demand for money, they were given an email address to contact for further instructions. No attempt was made to contact the attackers as recommended by local authorities

The hospital's spokesperson predicted it would take a few months before their workflow was back to the status quo. There was no evidence that patient data were breached.

Cyber Risk Case Studies

South-eastern Norway regional health authority (Norway)

a state-run organization of specialist hospitals and healthcare services created in 2002 alongside three other regional authorities

Who

Impact

The vulnerability is thought to have come from the legacy system, Windows XP .
While the organization had begun security measures to reduce the risks brought on by Windows XP along with a plan to phase it out, the attack took place before they could implement the security measures.

In January 2018, South-East RHF announced that the PHI and records of nearly 2.9 million people (more than half of the population of Norway) had been compromised. It is suspected that a sophisticated criminal group from a foreign spy or state agency led the attack targeting both patient health data and the health service's interaction with Norway's armed forces

What Happened

While this attack did not seem to pose risks to patient safety or delays in hospital operations, the event raised concerns about future attacks on health data for the purpose of political gain and served as a wake-up call for GDPR. Under GDPR, the organization would have had to notify those affected within 72 h, which it did not do.

Cyber Risk Case Studies

Hancock regional hospital (United States)

a small (71 beds) non-profit hospital in Greenfield, Indiana founded in 1951.

Who

Impact

It was discovered that the hackers had permanently corrupted components of the backup files from many systems, except the EMR backup files.
Attack was conducted using Microsoft's Remote Desktop Protocol as an entry point into the server and the hackers had compromised a hardware vendor's administrative account to initiate the attack.

What Happened

On January 11, 2018, Hancock Regional faced a ransomware attack by the malware SamSam [21]. The attack targeted a server in their emergency IT backup-system and spread through the electronic connection between the backup site, located miles from the main campus, and the server farm at the hospital.

Hospital's IT team shut down all network and desktop systems. Hospital operations continued within the confines of their downtime procedures. Patients were not diverted, and the hospital did not shut down. The hackers demanded four Bitcoins (55,000 USD) for the ransom, and the hospital paid. IT staff then spent the next three-and-a-half days decrypting files and trying to get the system to run normally. They found no evidence that patient data had been compromised.

Excelic Solutions for Cyber Safe Hospitals

IT Security Posture Assessment

- IT infrastructure with configuration management, change management, and logging and monitoring in place
- Configuration management boosts vulnerability and patch management
- Change management avoids unnecessary service downtime, also useful during a cyberattack
- An incident response plan can be a version of change management.
- Strict audit logs and monitoring of logging records are IT functions which are critical to quickly recognizing attacks and obtaining details on an attack

Internal Fraud Prevention

- Humans are the weakest link in cybersecurity
- End users, from clinicians to billing and scheduling staff, as well as patients and caregivers who connect their personal devices with the hospital network, can unintentionally threaten the cybersecurity of the health facility
- Relevant and effective trainings,
- Data Leak Protection Solutions
- Defined Policies or SOPs
- Legal Binding with NDA
- Random Forensic
- Endpoint Protection

Vulnerability Management

- Risk Assessment and VA/PT.
- Patch Management
- Configuration Hardening
- Endpoint Protection Solutions.
- Administrative and other user privileges and SOPs

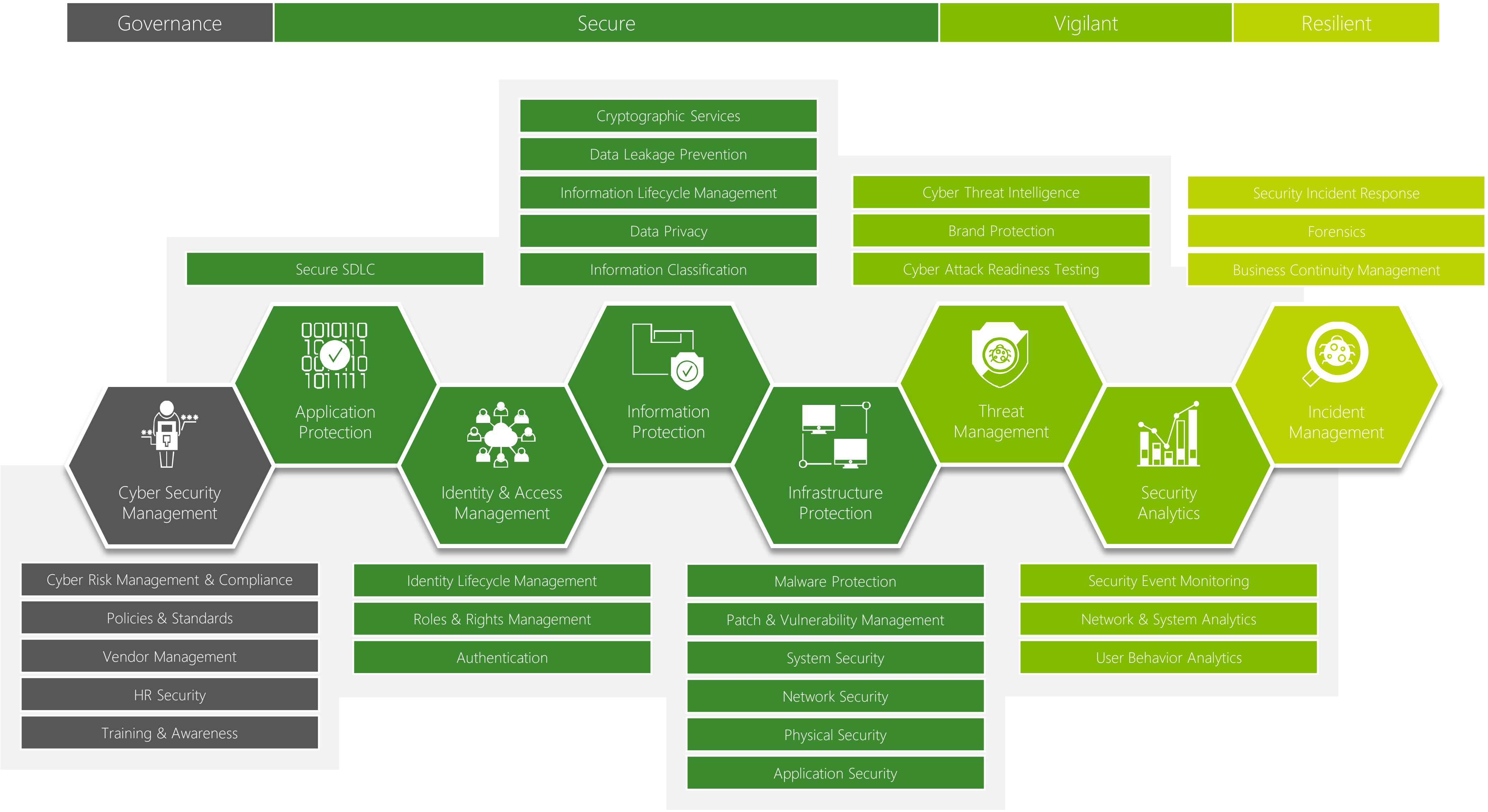
Vendor Risk Assessment

- Audit against a checklist
- Collaborating with the Management and IT
- Evidence Gathering and Documentation
- Policy Documentation if available
- Process Documentation if available

Audit and Compliance

- NIST Complaince
- ISO 270001 compliance
- Security Audit.
- HIPAA Compliance

Excelic's Cyber Security Framework & Services



Governance | Secure | Vigilant | Resilient

Cyber Security Management
- Cyber Risk Management & Compliance
- Policies & Standards
- Vendor Management
- HR Security
- Training & Awareness

Application Protection
- Secure SDLC

Identity & Access Management
- Identity Lifecycle Management
- Roles & Rights Management
- Authentication

Information Protection
- Cryptographic Services
- Data Leakage Prevention
- Information Lifecycle Management
- Data Privacy
- Information Classification

Infrastructure Protection
- Malware Protection
- Patch & Vulnerability Management
- System Security
- Network Security
- Physical Security
- Application Security

Threat Management
- Cyber Threat Intelligence
- Brand Protection
- Cyber Attack Readiness Testing

Security Analytics
- Security Event Monitoring
- Network & System Analytics
- User Behavior Analytics

Incident Management
- Security Incident Response
- Forensics
- Business Continuity Management

Corporate & Government Ties

INDIA
INDUSTRY IMPARTIALITY INTEGRITY

प्रवर्तन निदेशालय
सत्यमेव जयते

महाराष्ट्र पोलीस

GREATER MUMBAI POLICE

Cyber Crime Investigation Cell

देशसेवार्थ करसंग्रह

TATA
TATA MOTORS

teltronic
a Hytera company

ADITYA BIRLA GROUP

LARSEN & TOUBRO

Kawasaki

ALSTOM
• mobility by nature •

NSE
NSEIT

DAMM
Critical communication made easy

هيئة كهرباء ومياه الشارقة
Sharjah Electricity & Water Authority

Edelweiss
Ideas create, values protect

CRRC

GT20
CANADA

EURO T20 SLAM

राष्ट्रीय सेवा योजना
NATIONAL SERVICE SCHEME

SKF®

LOVELY PROFESSIONAL UNIVERSITY
PUNJAB (INDIA)

MANDATLY
Privacy Compliance Software

BCH™
BOMBAY COFFEE HOUSE
BANDRA | FORT

destek

DhakDhak™
India ke Dil ki Dhadkan

ARYANS
GROUP OF COLLEGES

D Y PATIL
UNIVERSITY

JBCN
International School

BKC
Your Growth Our Mission

RP
RAM PRIYANKA
Media Entertainments

KUAUSMEDIA
ENTERTAINMENT
FILM PRODUCTION, PR, CELEBRITY, EVENT & TALENT MANAGEMENT

Polaron TECHNOLOGIES PVT. LTD.®

LEGAL NEXTT

Thank You