

CAPABILITY OVERVIEW

ACH Solutions

Independent IT/OT Cybersecurity Consulting

Securing manufacturing IT and OT environments with practical, vendor-neutral advisory. Based in Bengaluru, India, serving clients across India and international markets.

https://achsol.com

services@achsol.com

ACH | SOLUTIONS

THE CHALLENGE

Connected manufacturing creates risk that needs independent eyes

Interconnected plant and enterprise systems

Industrial networks, SCADA, PLCs, MES platforms, industrial servers, connected devices and enterprise applications now operate as one linked ecosystem.

Efficiency arrives with operational exposure

Greater connectivity improves visibility and throughput, while introducing risks to production continuity, operational resilience, business information and industrial operations.

Built around manufacturing realities

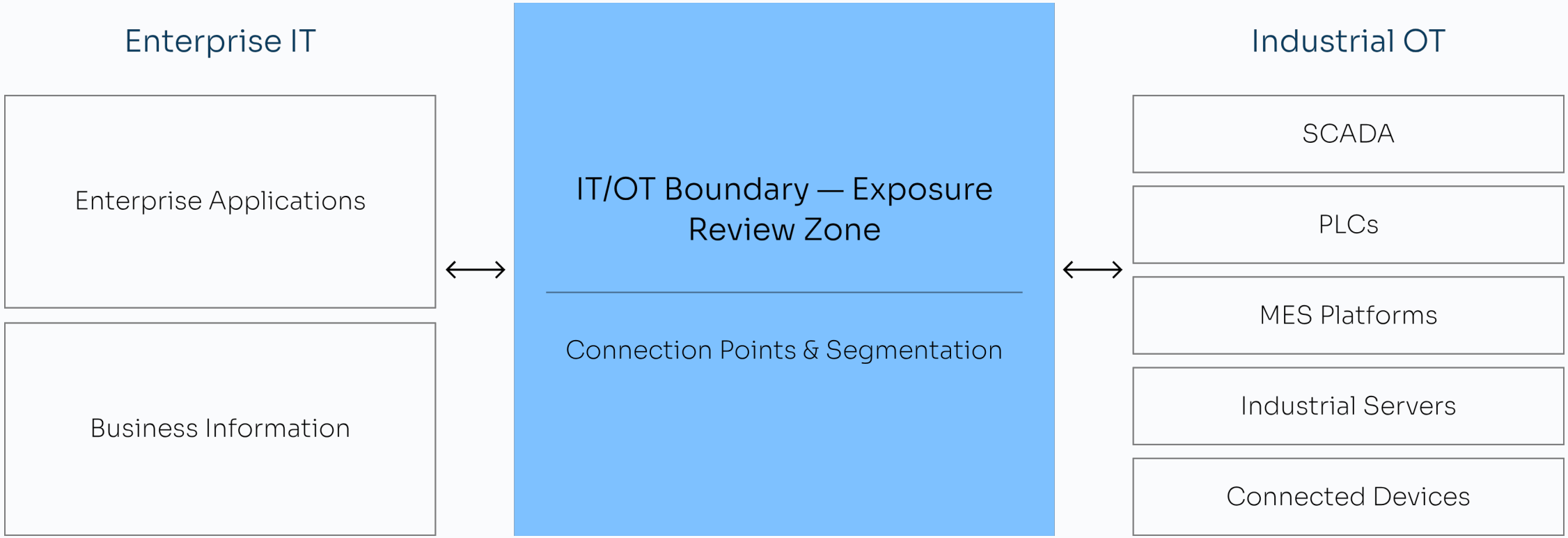
ACH Solutions delivers independent, vendor-neutral assessments and advisory grounded in how plants actually run.



IT/OT CONVERGENCE

Where IT and OT converge, exposure follows

Links between corporate networks and plant-floor systems create shared pathways that require structured boundary review.





OUR APPROACH

Practical, risk-based, vendor-neutral

Every engagement progresses from operational context to achievable action.

1. **Understand the environment.** Map business priorities, plant operations, systems and constraints before evaluating controls.
2. **Identify security weaknesses.** Uncover critical architecture, access, asset and governance gaps across IT and OT.
3. **Assess business impact.** Evaluate findings against production continuity, safety, resilience and commercial exposure.
4. **Recommend achievable improvements.** Define realistic, prioritised actions without unnecessary technology investments.

ACH | SOLUTIONS

CORE SERVICES

Two services, two distinct jobs

Engage ACH Solutions to establish clear risk visibility first, or to build sustained governance and remediation discipline.

SERVICE 01

Manufacturing IT/OT Cybersecurity Risk Assessment

Designed to establish an objective baseline of your industrial cybersecurity posture.

- Understand your current IT and OT exposure
- Identify critical architecture, asset, access and control gaps
- Prioritise remediation by likelihood and business impact

SERVICE 02

Cybersecurity Governance and Remediation Advisory

Designed to turn assessment findings into durable operational discipline.

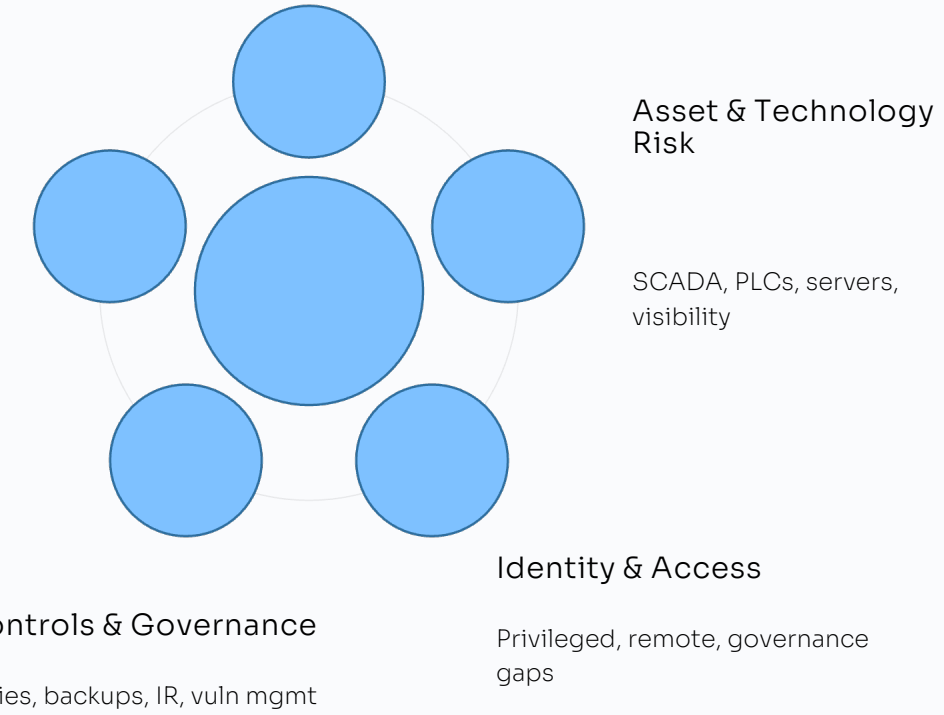
- Move from identified gaps to structured, sustainable improvement
- Establish clear ownership, policies and remediation tracking
- Support framework alignment and ongoing leadership reporting

ACH | SOLUTIONS

SERVICE 01 · ASSESSMENT SCOPE

Understand your industrial cybersecurity exposure

Five assessment scope areas establish an objective baseline across manufacturing IT and OT environments.



Service 01 deliverables lead to a prioritised plan

Posture assessment and architecture observations

A clear view of current security posture alongside critical asset and IT/OT architecture observations.

Security gaps and risk register

Documented weaknesses structured into a risk register, prioritised by likelihood and business impact.

Executive report and remediation roadmap

An executive assessment report paired with a practical, sequenced remediation roadmap.

Management presentation and walkthrough

A dedicated findings walkthrough with leadership to align on risk decisions and next steps.

CLIENT OUTCOME

Better visibility of industrial cybersecurity risks, informed leadership decisions and a prioritised plan to improve manufacturing resilience.

SERVICE 02 · GOVERNANCE & REMEDIATION ADVISORY

From identified gaps to sustainable improvement



Governance

Structures, ownership, policy and control improvements aligned to business needs.



Risk and remediation

Prioritise risks, plan and track corrective actions, and support risk acceptance decisions.



Framework advisory

ISO 27001, NIST CSF, ISA/IEC 62443-oriented OT governance and audit readiness.



Executive reporting and ongoing advisory

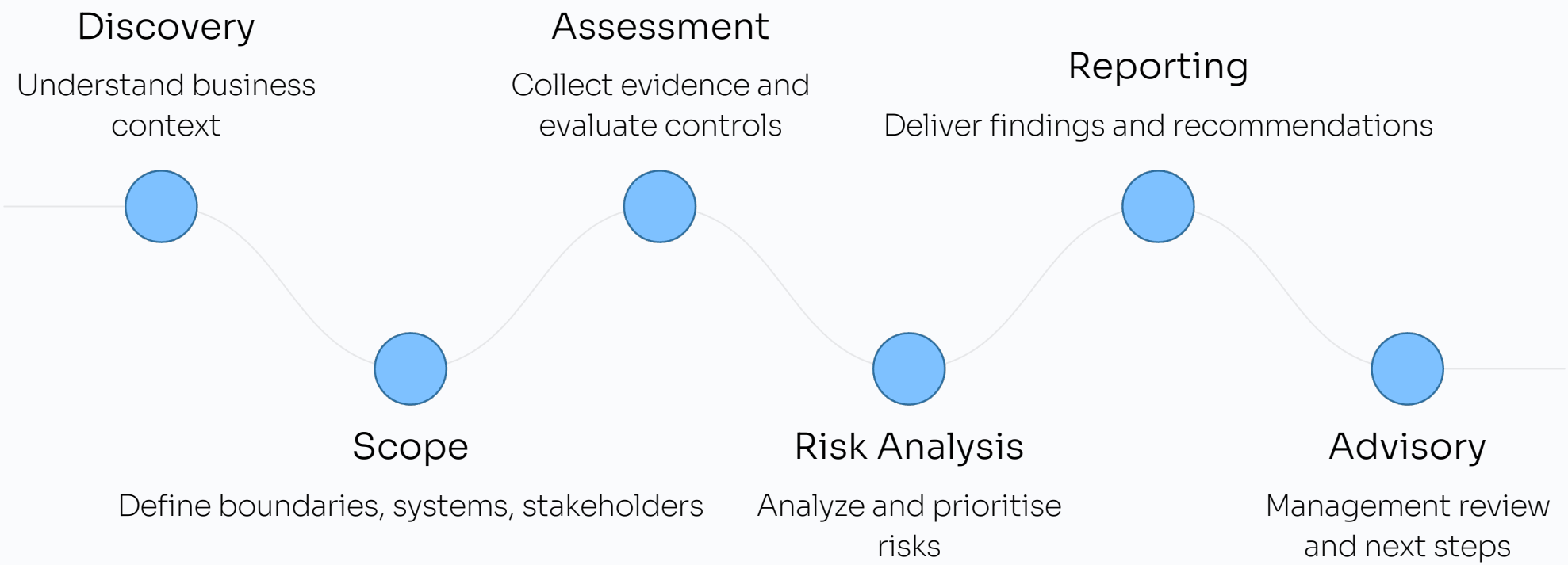
Periodic posture reviews, independent review of proposed improvements, incident preparedness support and advice to IT, OT and business leaders.

Outcome & deliverables: Stronger ownership, better risk visibility, structured remediation and sustainable governance, supported by improvement recommendations, a tracking framework, a prioritised plan, management reporting and periodic reviews where included.

DELIVERY METHODOLOGY

A six-step delivery approach

Every engagement moves systematically from business context and clear scope through to management review.



OPERATING PRINCIPLES

Five principles guide every engagement

01 Independent and vendor-neutral

No product sales or vendor affiliations, ensuring objective advice.

02 Manufacturing-aware

Respects production availability and real operational constraints.

03 Risk-based

Focuses on the risks that matter most, not long lists of low-value observations.

04 Practical

Delivers achievable controls and realistic implementation plans.

05 Management-focused

Translates technical findings into clear business risks and decisions.

Consistent standards across every assessment and advisory mandate.

ACH | SOLUTIONS

LEADERSHIP

Led by Abhijeet Chaubey

Founder and Independent IT/OT Cybersecurity Consultant

Over 18 years of experience

Across enterprise IT operations, cybersecurity, technology risk, audits, governance and manufacturing technology, spanning global manufacturing, banking and regulated environments.

- Connected manufacturing and MES governance across global plants
- SCADA and industrial connectivity; NIST CSF and ISO 27001 advisory
- Global IT, OT and cybersecurity audit leadership; ITSM, ISMS and operational resilience

Certifications: CISSP, CCSK, ISO 27001 Lead Auditor, ISO 20000 Lead Auditor, CSSLP, ITIL, CCNA, CCSA

> Controls that are technically appropriate, operationally practical and aligned with business priorities.



Who we serve and how we engage

Sectors we serve

- Automotive and component manufacturing
- Battery and energy storage
- Industrial machinery and automation
- Aerospace and defence suppliers
- Electronics, electrical equipment and connected industrial businesses

Key stakeholders

Founders, CEOs, MDs, CIOs, CTOs, CISOs, IT directors, and plant, engineering and OT heads.

Engagement formats

Work is structured as a defined assessment, multi-location assessment, governance programme or periodic advisory.

Scope, timelines, responsibilities, deliverables and commercial terms are agreed before work begins.

Specialist scope: Penetration testing, specialist technical testing, implementation and certification are included only when explicitly agreed and supported by appropriate delivery capability.

START WITH A CONVERSATION

Understand Your Risks. Prioritise Your Security. Protect Your Operations.

Does your organisation have sufficient visibility into the cybersecurity risks affecting its manufacturing and industrial environments?

ACH SOLUTIONS | WWW.ACHSOL.COM | SERVICES@ACHSOL.COM

