

Enterprise Security Architect - IAM

Job ID
REQ-10075772

4月 14, 2026

Spain

摘要

Location: Barcelona, Spain;
#LI-Hybrid

Internal job title: Assoc. Dir. DDIT ISC Enterprise Security Architecture - IAM

The Enterprise Security Architecture team is looking for an IAM Enterprise Security Architect. This role will play an essential role in shaping and driving the architecture and design of various IAM platforms. This includes defining and adopting standards for their use, as well as acceptable implementation patterns, in alignment with Novartis information security standards and industry best practices. The individual will lead technology selection processes, manage vendor relationships, and guide cross-functional teams to execute and implement the IAM change strategy. This strategy aims to transform the way the company manages digital identities and their access to systems. They will also provide technical leadership for IAM transformation projects, ensuring that IAM applications are effectively security tested throughout their development and lifecycle.

About the Role

Key responsibilities:

- Drive definition of IAM standards and architecture patterns and contribution to the overall Novartis technology strategy in collaboration with Novartis Enterprise Architecture/Governance; contribute to the development of overall Novartis technology strategies, designs, standards, and procedures that support business strategies
- Review, approve and control technology variants to the agreed enterprise IAM standards
- Lead IAM technology selection process including in-depth IAM products evaluation and vendor relationship management
- Drive senior management sessions on IAM risk management, solution proposals, technology adoption
- Provide technical leadership for various IAM transformation projects, throughout the project lifecycle, including evaluating business requirements and security technologies, planning technology deployment, aligning with security engineering and solution architecture teams
- Proactively share knowledge of technology risks with business domain, while partnering with delivery leadership to ensure continuous improvement of IT services, application rationalization and efficient management of existing systems and operations
- Effectively liaise with other teams in information security & risk management, infrastructure & architecture management as well as business functions
- Ensure IAM applications are effectively security tested, according to their criticality, throughout development and lifecycle
- Ensure that project and development teams gain a sufficient level of IT security awareness for designing new services, technology, and source code to gain an effective and sustainable IT security improvement and lower risk to the organization when projects are handed over to operations
- Drive performance KPIs and metrics for IAM architecture outcomes, measure performance against architecture strategy and operational goals; ensure industry network in IAM domain and identify innovation opportunities

Essential Requirements:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- 10+ years of working experience in Identity and Access Management domain; minimum 5+ years in architecture capacity; 5+ years of IAM project experience and leading technical design, product comparison and selection
- Demonstrated security architecture conceptual skills, roadmap definition, and technology selection and decision making, incorporating sound security principles
- Prior experience in IAM policy, standards, guidelines, and patterns definition and in depth understanding of the IAM domain including strong knowledge of:
 - Identity governance and administration (IGA) architecture and solutions design and implementation
 - Role and attribute-based access control
 - IAM governance processes definition
 - Azure AD security technologies
 - IAM capabilities of major cloud providers such as AWS, Azure, Salesforce, Workday,

- ServiceNow, SAP, etc.
- Privileged Access Management
- AD architecture and key concepts
- API security and best practices for authentication/authorization
- Automation and integration related to IAM systems
- Experience in reporting to and communicating with senior level management (with and without IT background), with and without in-depth risk management background on information risk topics, and excellent written and verbal communication and presentation skills; interpersonal and collaborative skills.
- Proven experience to initiate and manage projects that will affect other divisions, departments, and functions, as well as the corporate environment, delivery focused with keen attention to detail and good decision-making ability function with/without supervision to deliver in time and at expected quality.
- Experience working in a multi-vendor, global environment and leading technical teams

Desirable:

- Professional information security certification, such as CISSP, CCSP, CISM is preferred.
- Professional (information system) risk or audit certification such as CIA, CISA or CRISC is preferred

Commitment to Diversity and Inclusion:

Novartis is committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

Why Novartis: Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? <https://www.novartis.com/about/strategy/people-and-culture>

Join our Novartis Network: Not the right Novartis role for you? Sign up to our talent community to stay connected and learn about suitable career opportunities as soon as they come up: <https://talentnetwork.novartis.com/network>

Benefits and Rewards: Read our handbook to learn about all the ways we'll help you thrive personally and professionally: <https://www.novartis.com/careers/benefits-rewards>

Why Novartis: Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? <https://www.novartis.com/about/strategy/people-and-culture>

Benefits and Rewards: Learn about all the ways we'll help you thrive personally and professionally. [Read our handbook \(PDF 30 MB\)](#)

部门

Operations

Business Unit

Information Technology

地点

Spain

站点

Barcelona Gran V í a

Company / Legal Entity

ES06 (FCRS = ES006) Novartis Farmac é utica, S.A.

Functional Area

Technology Transformation

Job Type

Full time

Employment Type

Regular

Shift Work

No

Job ID
REQ-10075772

Enterprise Security Architect - IAM

[Apply to Job](#)



Job ID
REQ-10075772

Enterprise Security Architect - IAM

[Apply to Job](#)

Source URL:

<https://www.novartis.com.cn/careers/career-search/job/details/req-10075772-enterprise-security-architect-iam>

List of links present in page

1. <https://www.novartis.com/about/strategy/people-and-culture>
2. <https://talentnetwork.novartis.com/network>
3. <https://www.novartis.com/careers/benefits-rewards>
4. <https://www.novartis.com/about/strategy/people-and-culture>
5. <https://www.novartis.com/sites/novartis.com/files/novartis-life-handbook.pdf>
6. <https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Enterprise-Security-Architect---IAMREQ-10075772>
7. <https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Enterprise-Security-Architect---IAMREQ-10075772>