consult hyperion
consulting by fime

Fime Academy

Digital Identity

Biometrics Masterclass.

Governing biometric system selection and qualification strategy.

This comprehensive training course provides an end-to-end exploration of the global biometric landscape, from modality trends to the complexities of industrial standards and AI-powered threats. It delivers a structured approach for strategically evaluating and designing implementations utilizing biometric technologies that balance security with user experience.

Participants will gain the 360-degree insights necessary to navigate integration hurdles, ensure regulatory compliance, and mitigate risks in the age of deepfakes and automated fraud. By the end of this masterclass, stakeholders will be empowered to make data-driven analysis and introduce reliable, inclusive, and next-generation biometric deployments.

Objectives

- Identify best practices and evaluate potential risks and threats inherent to biometric technologies.
- Strategically evaluate and select appropriate biometric modalities.
- Design, implement, and qualify biometric solutions effectively.
- Master industrial qualification and compliance frameworks.
- Anticipate and mitigate common hurdles during biometric integration.

Key topics

- Market trends and emerging biometric modalities.
- Strategic considerations for biometric implementations.
- Biometrics in the age of AI - navigating threats and opportunities.
- Qualification metrics and global industrial standards.

Audience

This masterclass is designed for Business Leaders, Decision Makers, Product/Project Managers, and Quality Assurance teams across all industries.

Price

Visit our website for more information about our training offer. For any specific requests, please contact us.

Duration	Location	Language
1.5 days (on site) or 4 online sessions (~2.5 hours each)	Customer premises Online delivery Available worldwide	English Local language options may be available.

Masterclass program

On site **1.5 days.**

M1. **Market overview.**

This module introduces the essentials of biometrics, covering what they are, the main modalities, and why organizations choose to use them. It includes brief examples of sector use cases and highlights how regulations shape responsible deployment. The session concludes with a concise look at key market trends influencing current adoption and innovation.

M2. **Considerations.**

The module reviews core factors behind effective biometric implementations, including key design pillars and the difference between identification and authentication. It highlights major risks such as presentation attacks and AI driven threats like deepfakes. Interoperability needs, user journey design, and the importance of inclusive performance across demographics are also addressed in a streamlined way.

M3. **Good practice guidelines.**

This session focuses on practical guidance for deploying biometrics successfully. It outlines best practice expectations across the project lifecycle, from requirements and data capture to deployment and ongoing monitoring, and includes recommendations for strengthening systems against AI enabled fraud.

M4. **Testing and qualification measurements.**

The module explains why thorough testing is essential and outlines how to define an appropriate testing strategy. It introduces key testing categories, including performance evaluation, presentation attack detection, and injection attack detection. Practical preparation tips help ensure testing conditions support meaningful and representative results.

M5. **Standards and compliance.**

This module provides a concise overview of standards and certification frameworks relevant to biometric systems. It distinguishes between standards and certification and presents the major programs available. The content helps participants identify which compliance routes best align with operational needs and implementation goals.

Online **4 sessions.**

Session 1 | 2.5 hours

M1. Market overview
- Introduction.
- Use cases.
- Regulation requirements.
- Market trends.

Session 2 | 2.5 hours

M2. Considerations
- Risks and vulnerabilities.
- Interoperability and user journey.
- Impact of AI and deepfakes.

M3. Good practice guideline
- Good practices of project phases.
- Defense in AI-powered fraud.

Session 3 | 2.5 hours

M4 Testing and qualification measurements
- Biometric system qualification.
- Define testing strategy.
- Types of testing.
- Test preparation considerations.

Session 4 | 2.5 hours

M5 Standards and compliance
- Standard vs. certification.
- NIST program overview.
- FIDO biometric component.
- FIDO Identity Verification (ID&V).
- Major platform requirements.
- Payment network programs.
- Critical distinctions and nuances.

Contact

fimeacademy@fime.com

Americas
fimeinsidesalesnalac@fime.com

APAC
fimeinsidesalesap@fime.com

China
fimeinsidesaleschina@fime.com

EMEA
fimeinsidesalesemea@fime.com

India
fimeinsidesalessa@fime.com

Japan
fimeinsidesalesjapan@fime.com

Korea
fimeinsidesaleskorea@fime.com

Making innovation possible.
Making the world work.

Consulting | Test Platforms | Testing Services

F-TRAIN-BIOMETRICS
Biometrics Masterclass