Software Development Plan

for

Multimodal Biometrics

Brian Tan

Davina Doran

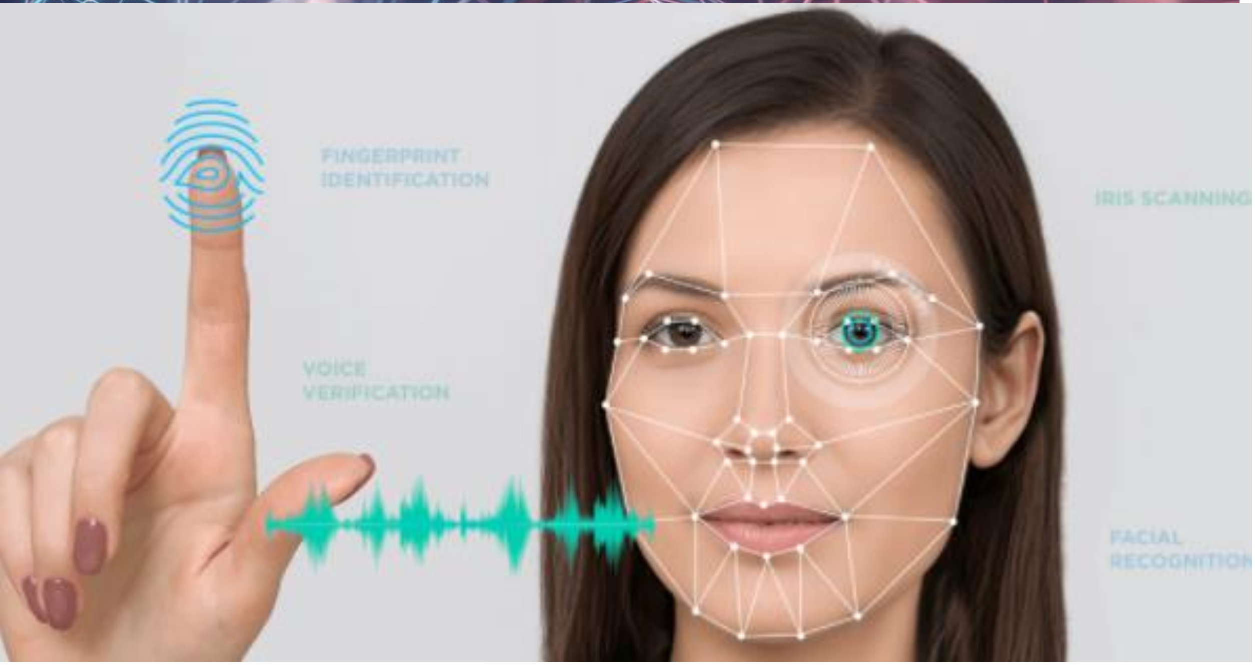
Fulya Kocaman

Konnor Gutierrez

California State Fullerton

CPSC 362 SOFTWARE ENGINEERING

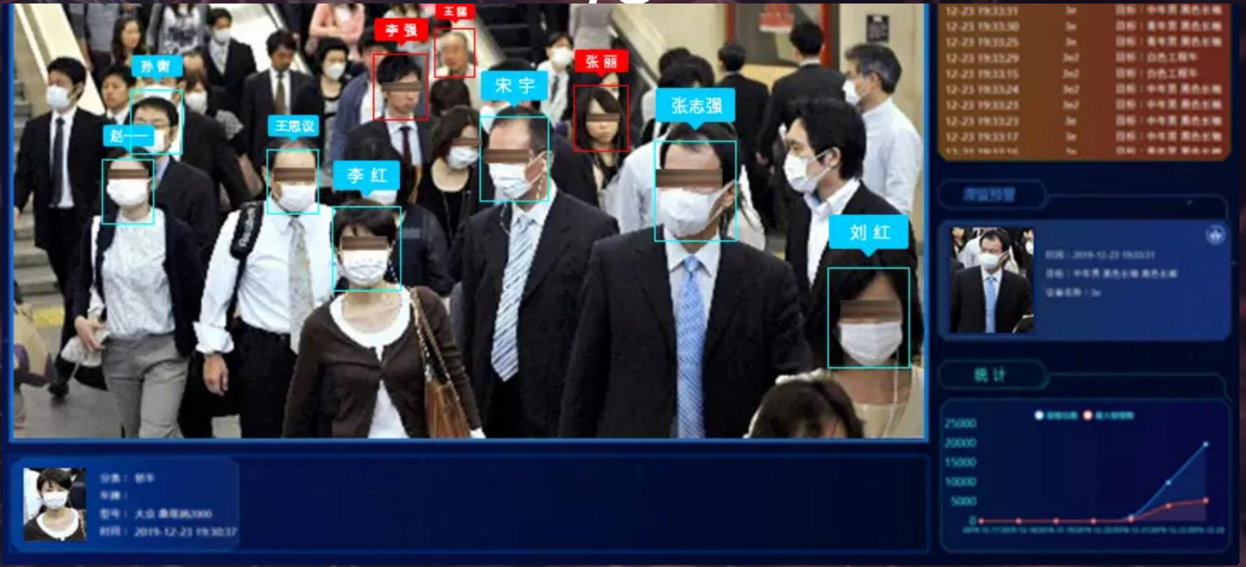
12/7/2020



Source: https://mobidev.biz/blog/multimodal-biometrics-verification-system-ai-machine-learning

Introduction - The Project Scope

- Develop a customized Multimodal Biometrics recognition system in conjunction with the CAC (Common Access Card) for the US Army
- Uses unique identifiers - retina, fingerprint, voice, face, palm
- Provide fast and accurate access to secure locations/rooms/systems for authorized personnel in military facilities to prevent fraud and abuse
- Give options to make Biometrics contactless for hygienic reasons due to the COVID-19 pandemic.
- Aim to make facial recognition technology more advanced by including masked face detection and recognition technology

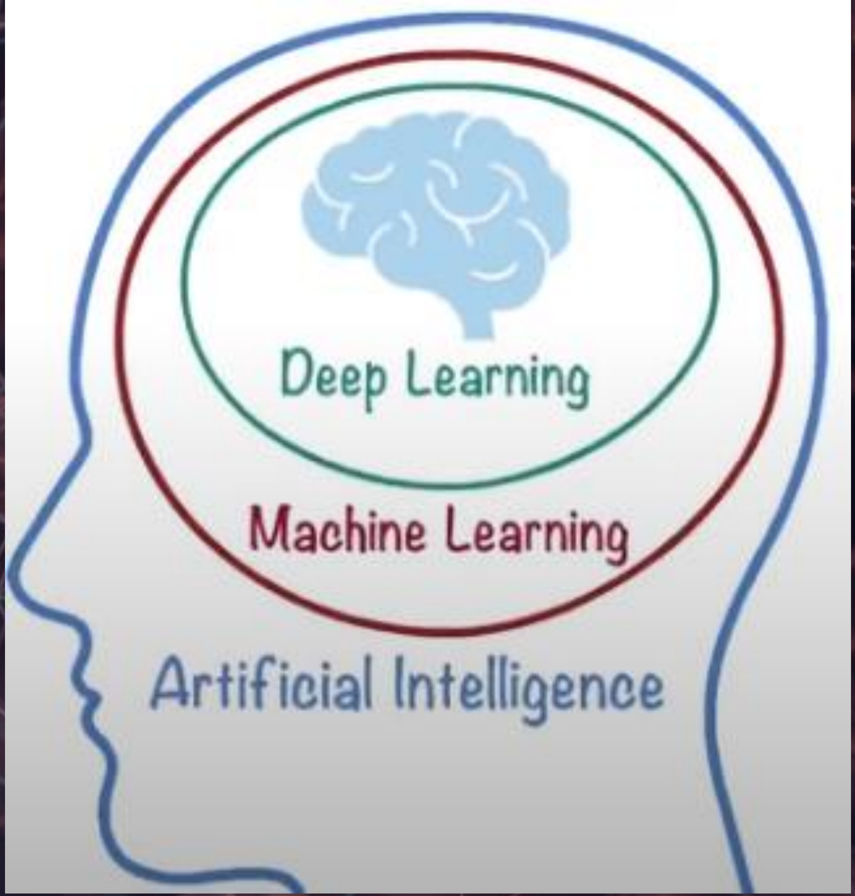


Source: https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/

Planning and Analysis

Our system

- Robust, flexible, modular, and extendable with the help of using object-oriented design
- Designed to handle the constant changes and improvements of the fast-growing industry
- Very difficult to spoof as compared to unimodal systems
- In case of a failed identifier, still provides security by employing the other identifier
- Secure and fast using efficient and accurate **Deep learning algorithms** that determines a person’s identity within *minimum margin of error*

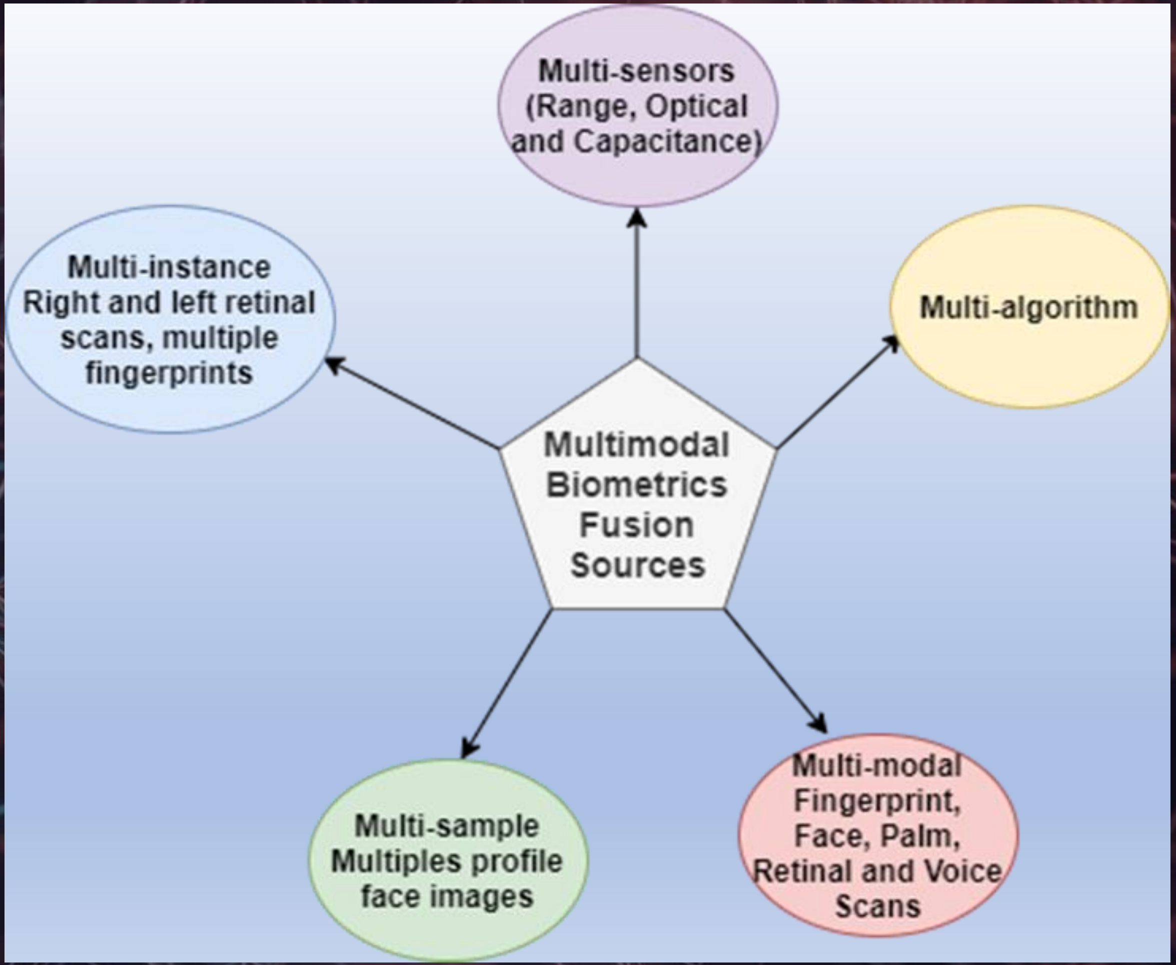


Source: https://bit.ly/SimplilearnDeepLearning

Program Design Approach

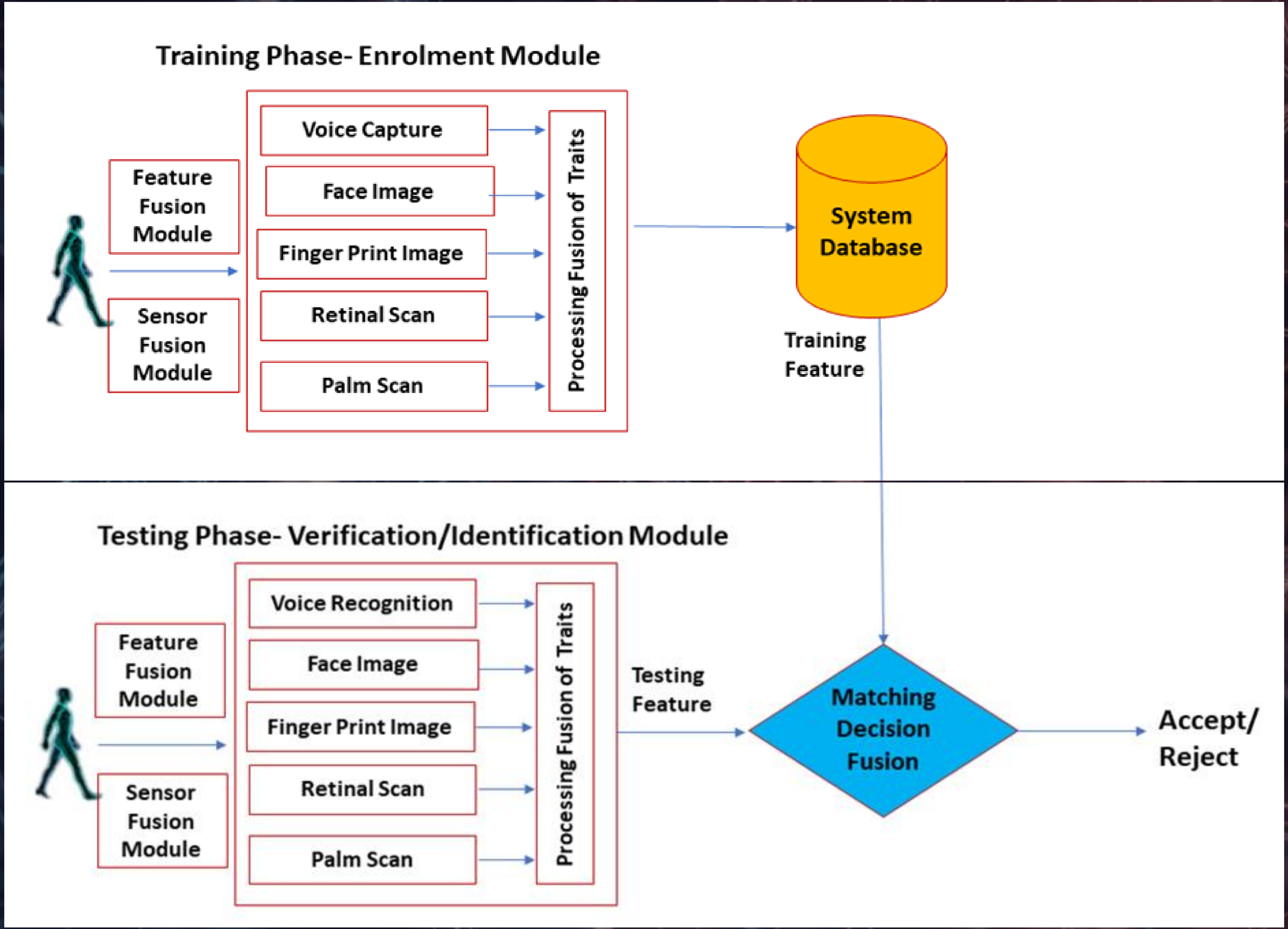
Architectual Design

- Multisensors: Used to capture the data
- Multiple algorithms: The same capture data are processed using different algorithms
- Multiple instances: Multiple instances of the same modality used
- Multisamples: Multiple samples of the same trait acquired
- Multimodal: Data from different modalities combined, such as face, fingerprint and palm, retina and voice.

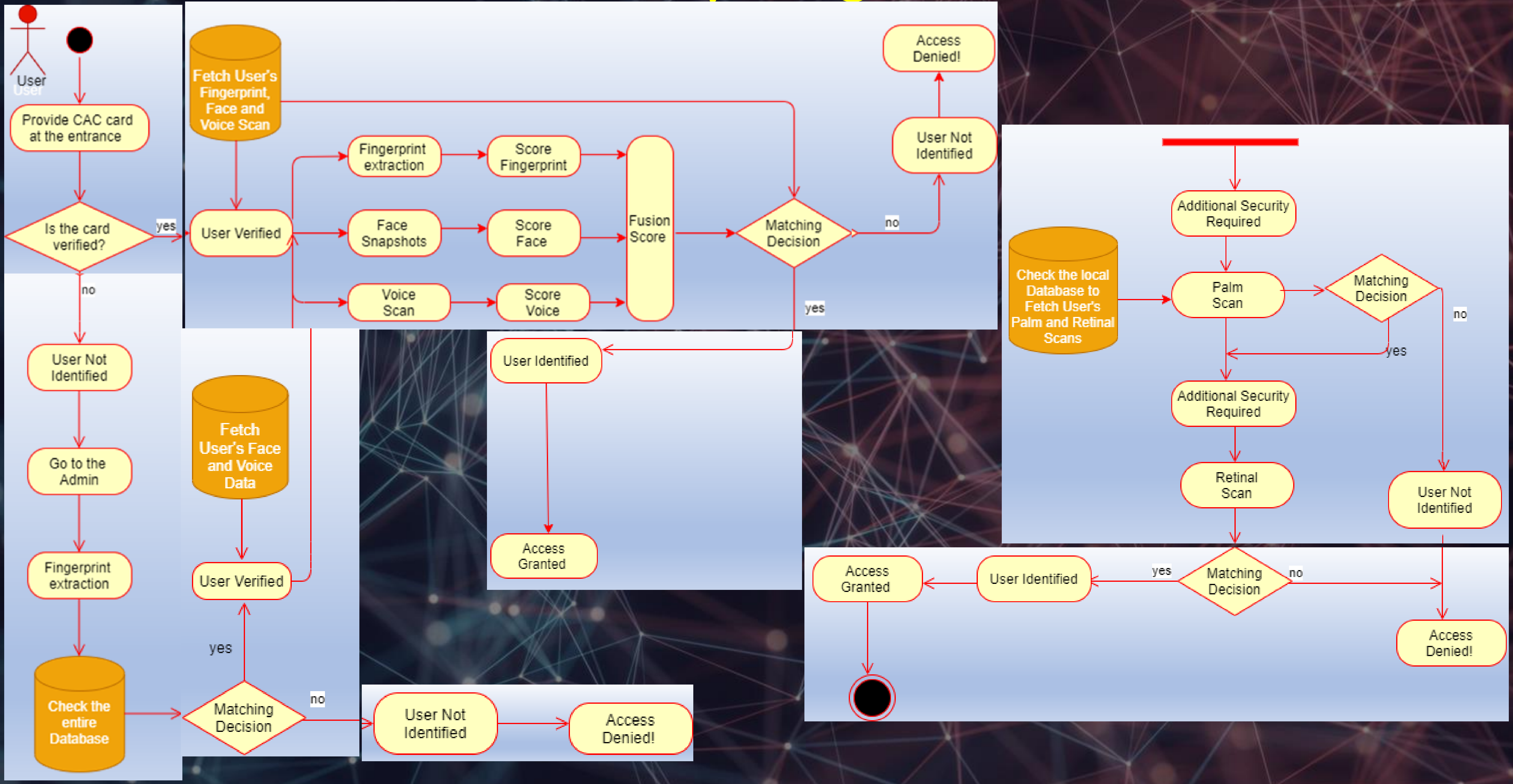

Multi-sensors (Range, Optical and Capacitance)
Multi-instance Right and left retinal scans, multiple fingerprints
Multi-algorithm
Multimodal Biometrics Fusion Sources
Multi-sample Multiples profile face images
Multi-modal Fingerprint, Face, Palm, Retinal and Voice Scans

Program Design Approach- Fusion Levels

System Architecture: Enrollment and Authentication Phases



Activity Diagram



Schedules and Milestones

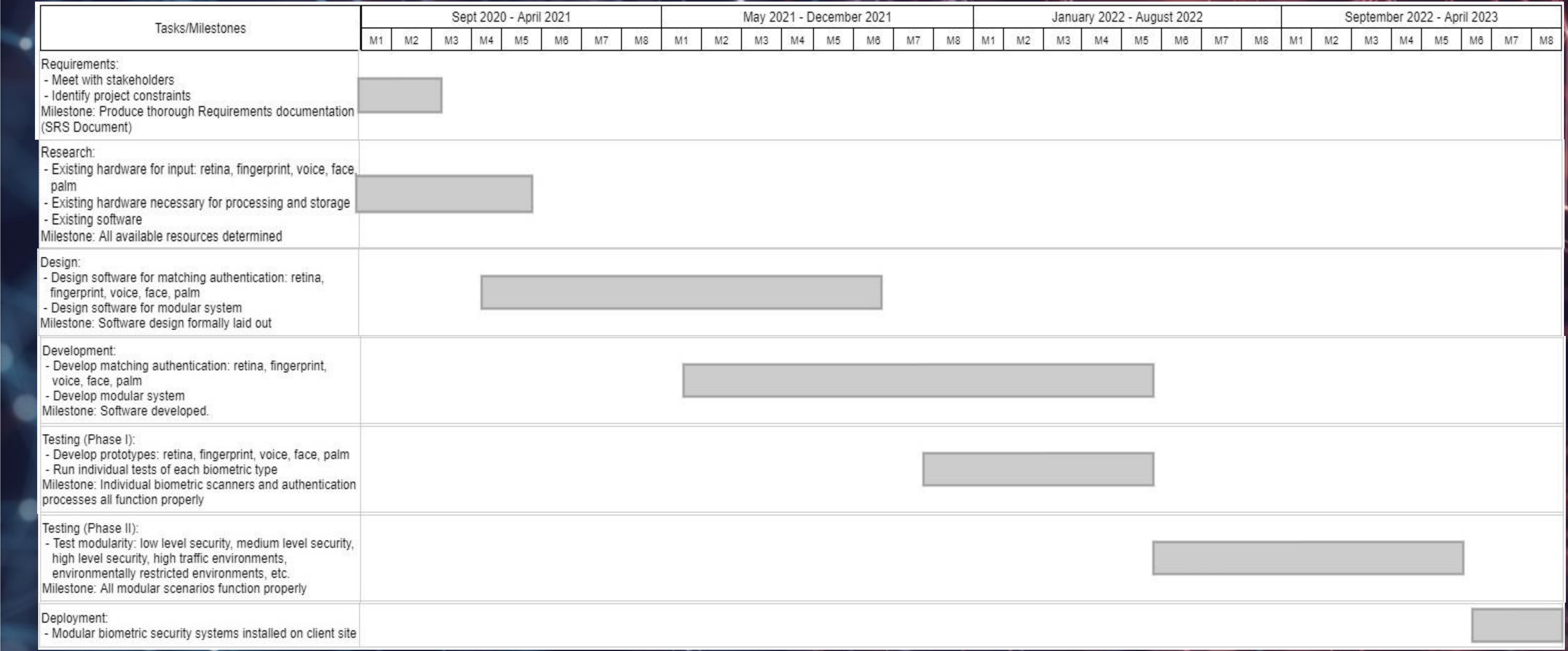
The Breakdown

- Requirements: meet with stakeholders, identify project constraints
- Research: existing hardware, software, & people
- Design: software for matching authentication & modular integration
- Development: software for matching authentication & modular integration
- Testing (Phase I): create and test prototype system for each biometric type
- Testing (Phase II): create and test systems with different levels of modular integration
- Deployment: installation of biometrics systems on site.

Initial Gantt Chart

Time Allocation (32 months)

- low coupling between each biometric system allows for phases of the schedule to begin before the previous phase completes



Tasks/Milestones	Sept 2020 - April 2021								May 2021 - December 2021								January 2022 - August 2022								September 2022 - April 2023							
	M1	M2	M3	M4	M5	M6	M7	M8	M1	M2	M3	M4	M5	M6	M7	M8	M1	M2	M3	M4	M5	M6	M7	M8	M1	M2	M3	M4	M5	M6	M7	M8
Requirements: - Meet with stakeholders - Identify project constraints Milestone: Produce thorough Requirements documentation (SRS Document)	▨	▨																														
Research: - Existing hardware for input: retina, fingerprint, voice, face, palm - Existing hardware necessary for processing and storage - Existing software Milestone: All available resources determined	▨	▨	▨	▨	▨																											
Design: - Design software for matching authentication: retina, fingerprint, voice, face, palm - Design software for modular system Milestone: Software design formally laid out				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																		
Development: - Develop matching authentication: retina, fingerprint, voice, face, palm - Develop modular system Milestone: Software developed.									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨											
Testing (Phase I): - Develop prototypes: retina, fingerprint, voice, face, palm - Run individual tests of each biometric type Milestone: Individual biometric scanners and authentication processes all function properly															▨	▨	▨	▨	▨	▨	▨											
Testing (Phase II): - Test modularity: low level security, medium level security, high level security, high traffic environments, environmentally restricted environments, etc. Milestone: All modular scenarios function properly																					▨	▨	▨	▨	▨	▨	▨	▨	▨			
Deployment: - Modular biometric security systems installed on client site																														▨	▨	▨

Cost Estimate

COCOMO Model

- Basic COCOMO Model estimation technique for organic project types, and an estimated 250K lines of code

Type	a	b	c	d
Organic	2.4	1.05	2.5	0.38

Effort:

$2.4(250)^{1.05} = 791$ Person-Months

Development Time:

$2.5(791)^{0.38} = 32$ Months

Avg. Staff Size:

$791 / 32 = 25$ Persons

Productivity:

$250 / 791 = 0.32$ KLOC / Person-Month

Cost Estimate

People Power Requirements (Approx. 25 people)

- Already filled roles: senior management team, project specialist, steering committee.
- To be hired: project manager, system administrator, system analyst, hardware engineers (team of 4 people), requirement analyst, technical clerk, software engineers (2 teams of 3 people, 6 people total), algorithm engineers (team of 3), database engineers (team of 3-4 people), technical support (5-8 people), QA manager.

Cost Estimate

Cost to develop/run the system:

- Based on current national averages, 40-hour work weeks for 30-32-months

- Project manager: 30-32 months, $50-60 hourly
  - life of project est. $240,000-$307,200
- System administrator: indefinitely, $25-$35 hourly
  - life of project est. $120,000-$179,200
  - yearly est. $48,000-$67,200
- System analyst: indefinitely, $25-$35 hourly
  - life of proect est. $120,000-$179,200
  - yearly est. $48,000-$67,200
- QA manager: 30-32 months, $50-$60 hourly
  - life of project est. $240,000-$307,200
- Technical clerk: indefinitely, $10-$20 hourly
  - life of project est. $48,000-$102,400
  - yearly est. $19,200-$38,400
- Software engineers: 6 people, 30-32 months, $30-$40 hourly
  - life of project est. $144,000- $204,800 per person = $864,000-$1,228,800
- Algorithm engineers: 3 people, 30-32 months, $55-$65 hourly
  - life of project est. $264,000-$322,800 per person = $1,584,000-$1,996,000
- Database engineers: 3-4 people, indefinitely, $25-$35 hourly
  - life of project est. $120,000-$179,200 per person = $360,000-$716,800
  - yearly est. $48,000-$67,200 = $144,000-$268,800
- Technical support: 5-8 people, indefinitely, $10-$20 hourly
  - life of project est. $48,000-$102,400 per person = $240,000-$819,000
  - yearly est. $19,200-$38,400 = $96,000-$307,200

- Estimated Total for the Software Development (30-32 months): $3,696,000-$5,836,800 (Average $4,766,400 total)

Cost Estimate

Hardware Cost Estimates:

- Cost varies per system implemented. ($10,000 – $2M, 1M Average)
    - Input Device Costs(per unit):
        - Voice: $500
        - Palm: $100
        - Fingerprint: $1,300
        - Facial: $25,800
        - Retinal: $50,000
    - Environmentally hardened scanners run at x2’s the rate
    - Processing/Storage Devices:
        - CPU: $200 - $400 per system
        - RAM: $30 - $50 per system
        - Database: $5000 – $10,000
    - Backup Power (UPS): $2,000-$5,000 per system

Cost Estimate

Management Reserve:

- Average MR rate of 5 – 15%
- Estimated cost to develop system: $ 6M
- Accounts for a MR of $6.3 - $6.9M

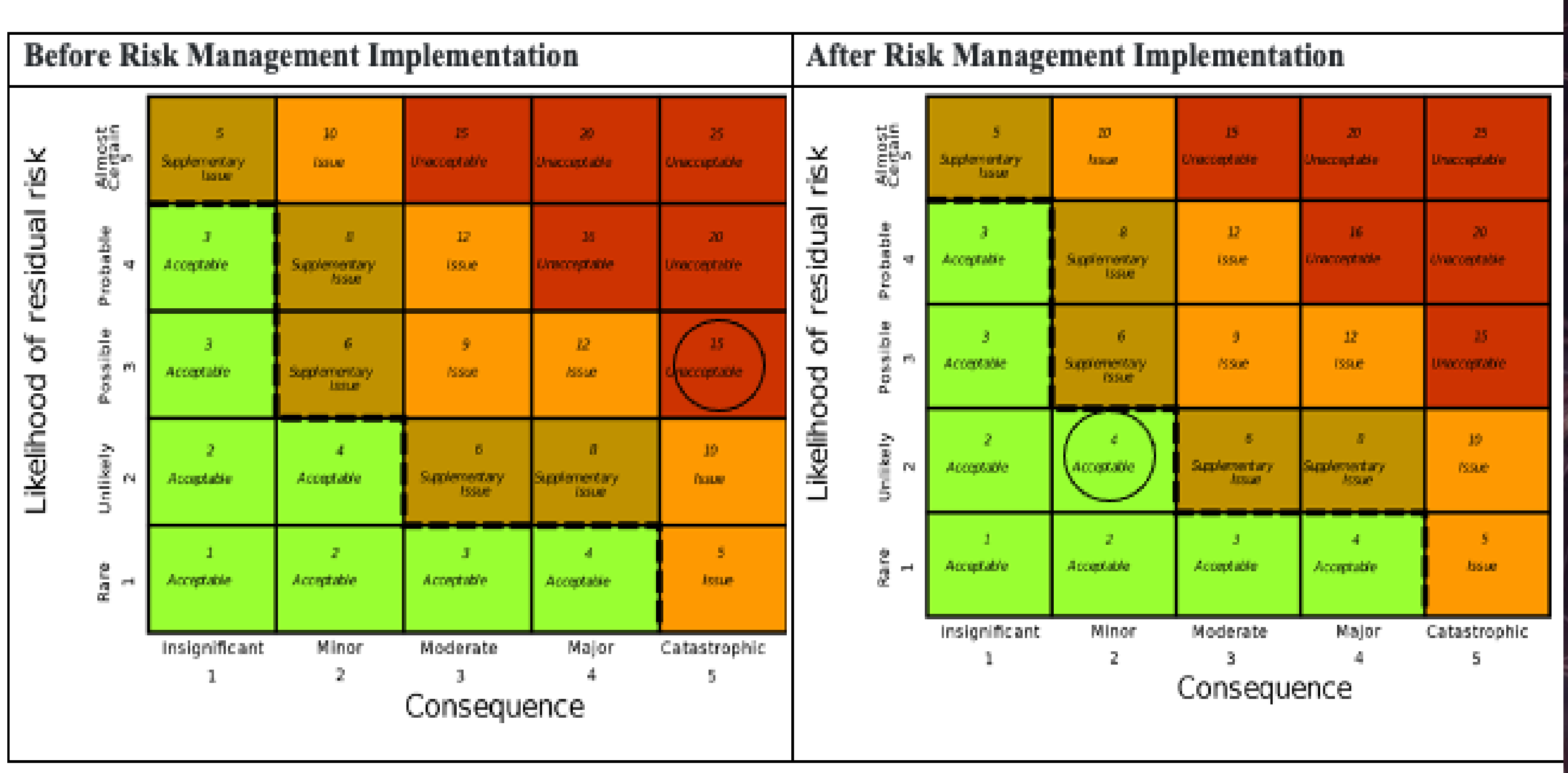
Risk Analysis

Identified Risks

- System Performance
- Rejection / Accepting Rates
- Spoofing Attacks
- Data Breaches

Risk Mitigation – System Performance

- Mitigating system failures
- Allow for CAC authorization and personnel verification
- Implement live backups and live rollbacks as needed
- Have rollback method built into BIOS, not OS



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

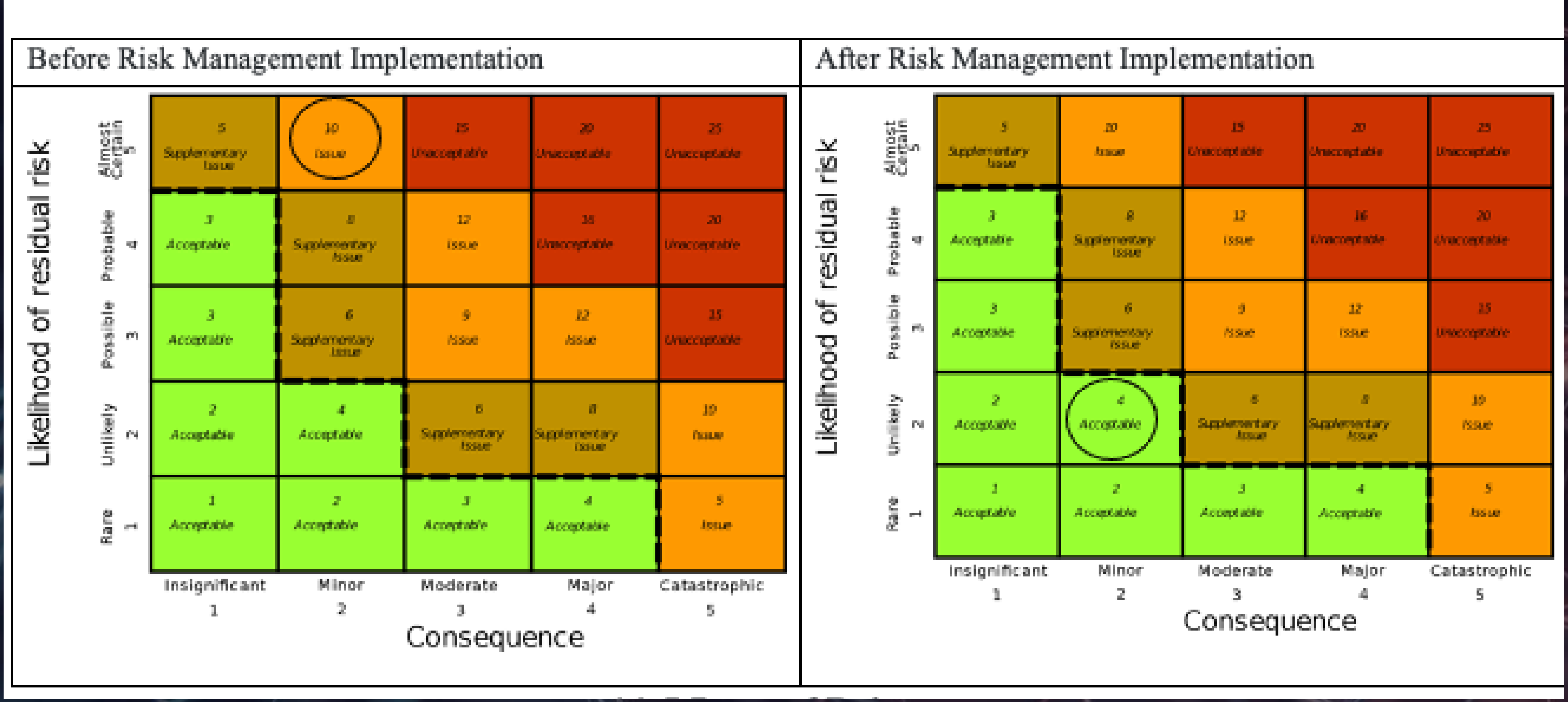
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	20 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Risk Mitigation – System Performance

- Handling individual scanner failures
- Have failover biometrics enabled
- Include built in self test and error correction upon boot/reboot
- Allow for failover to CAC card authentication when applicable.



Before Risk Management Implementation

Likelihood of residual risk

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

After Risk Management Implementation

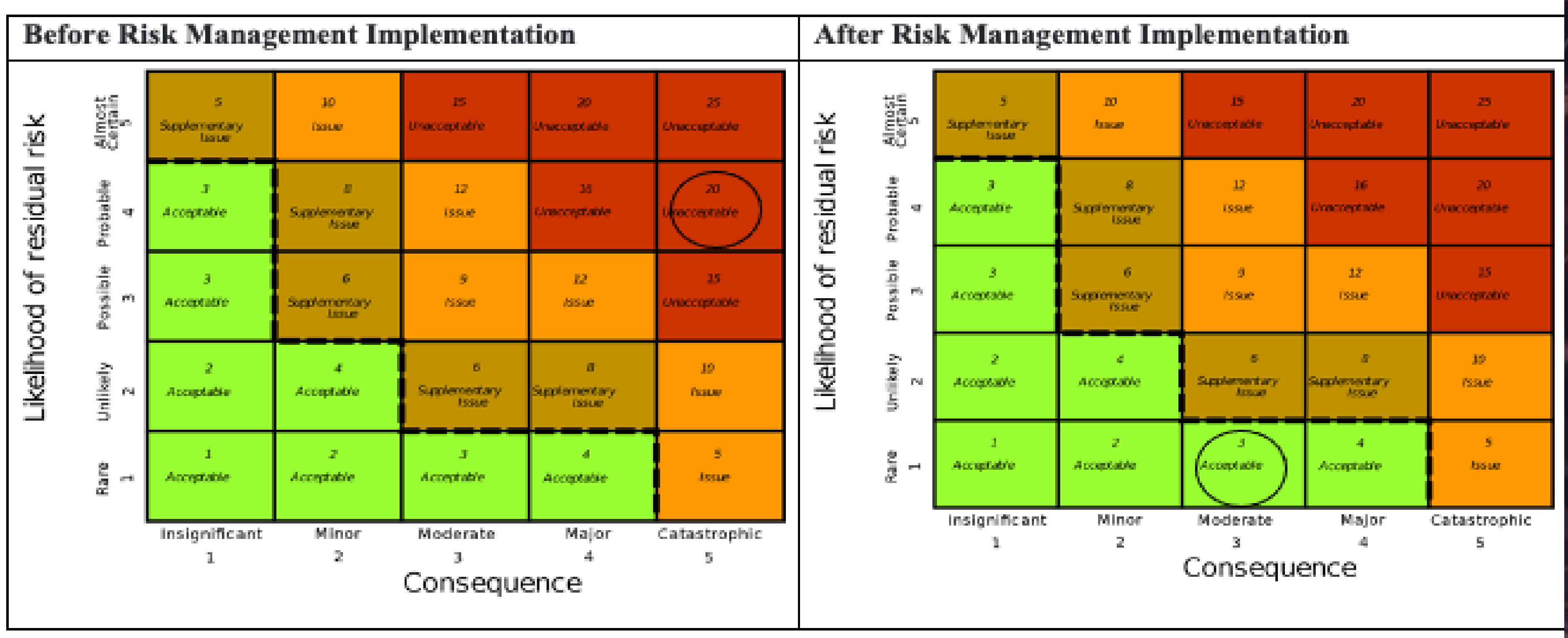
Likelihood of residual risk

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	20 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Risk Mitigation – False Rejection/Accept Rates

- Type I -Tolerance increased during multifactor authentication - Not applicable in mandatory max security checks.
- Type II - Tolerance lowered when using single authentication factor.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

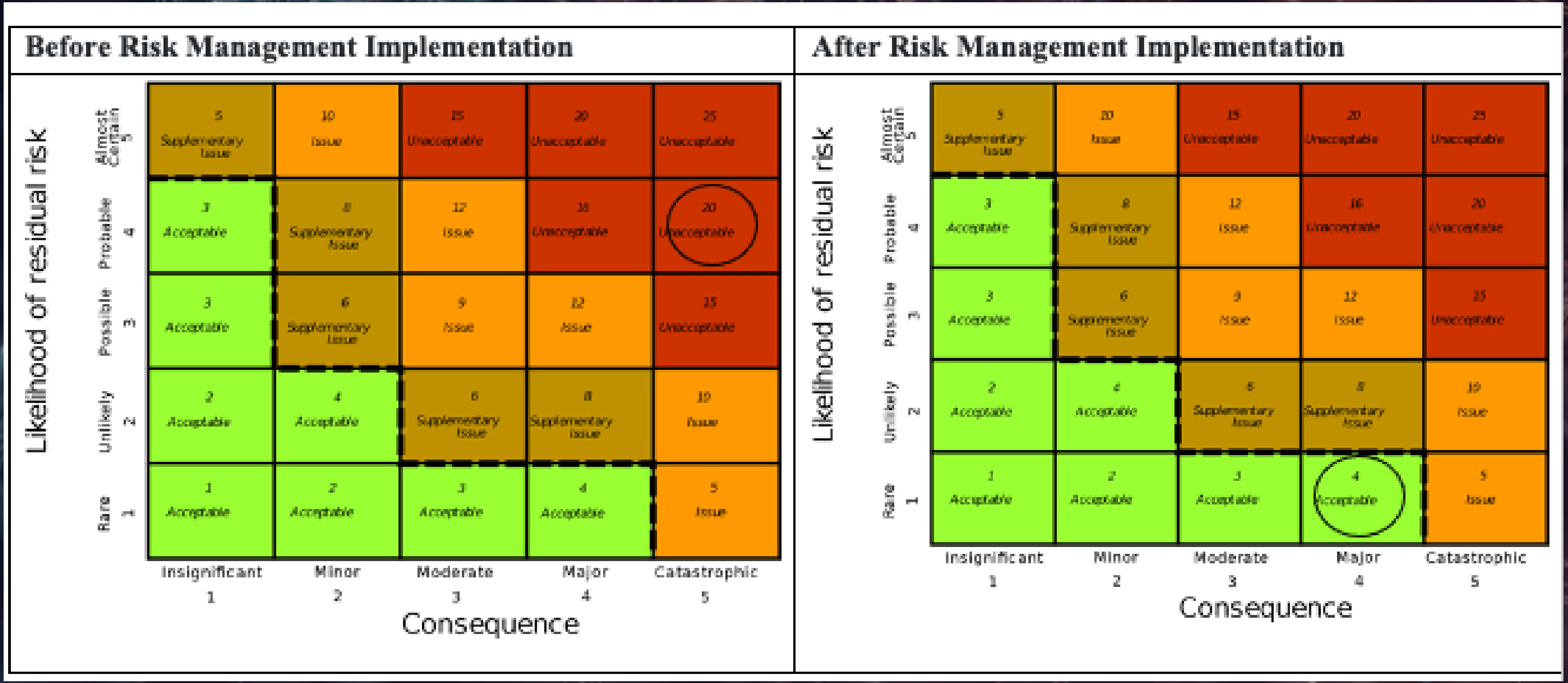
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	20 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Risk Mitigation – Spoofing Attacks

- Implement custom in-house anti-spoof algorithm
  - Considered high priority for security ops team
  - Algorithm constantly updated to prevent reverse engineering
  - Rework done upon major discovery in algorithm cracking



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

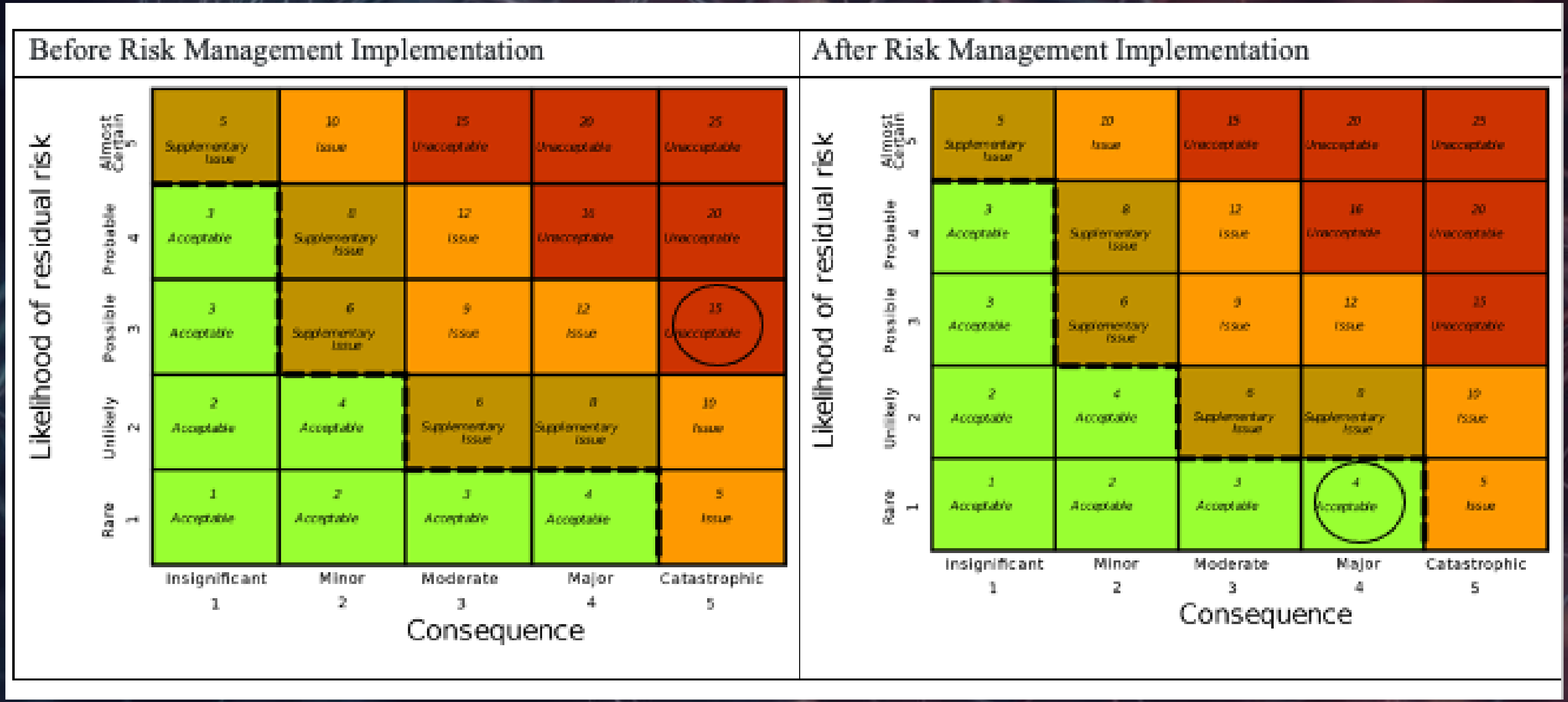
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Risk Mitigation – Data Breaches

- No data storage done on local scanner
- Biometric enrollment must be done manually
- Databases aren’t connected to internet/external network
  - Network connection works via approved MAC addresses
- Communications done through AES encryption



Before Risk Management Implementation

Likelihood of residual risk

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

After Risk Management Implementation

Likelihood of residual risk

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

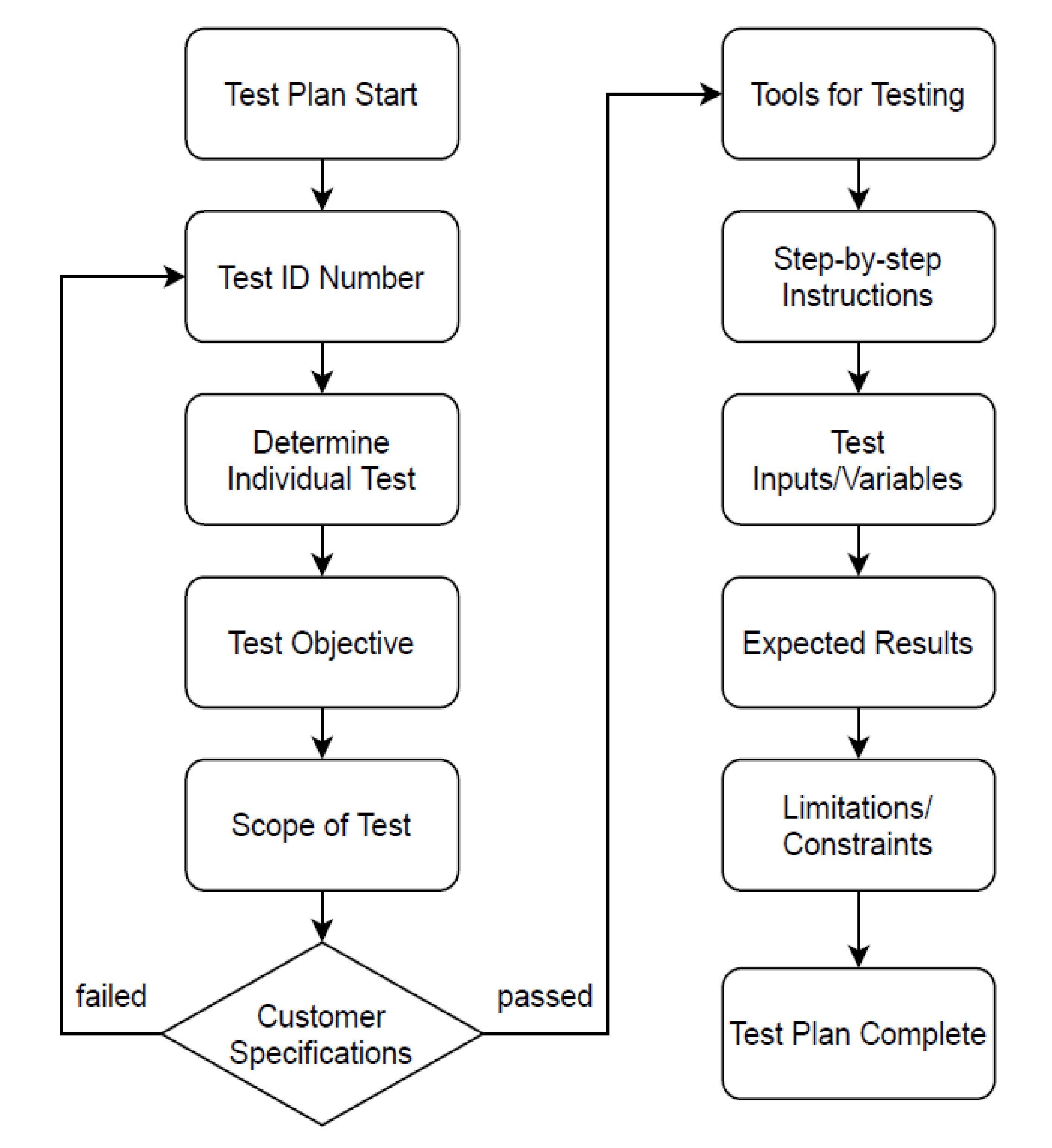
Consequence

Testing

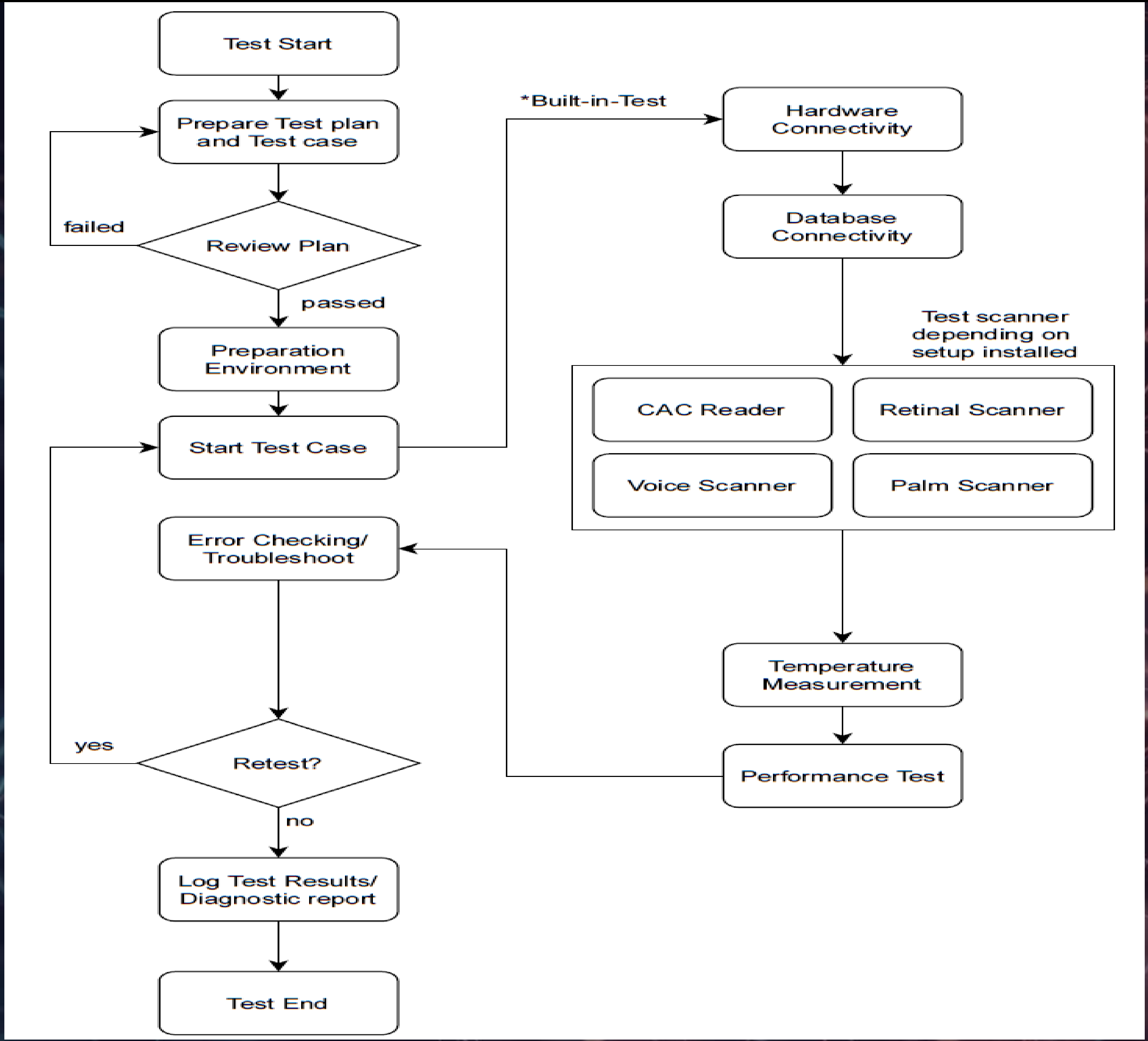
- Fast – ideally 30-45sec
- Independent – no reliance on any specific conditions
- Reusable – ability to repeat on any environment; local or server
- Self-Validating – shows pass/fails immediately
- Timely – tests should be ready with main code production

Testing

- Test Plan



- Test



Test Start

Prepare Test plan and Test case

Review Plan

failed

passed

Preparation Environment

Start Test Case

*Built-in-Test

Hardware Connectivity

Database Connectivity

Test scanner depending on setup installed

CAC Reader

Retinal Scanner

Voice Scanner

Palm Scanner

Temperature Measurement

Performance Test

Error Checking/ Troubleshoot

Retest?

yes

no

Log Test Results/ Diagnostic report

Test End

Deployment

- Deployment Schedule

Target Deployment and Sequence	Scheduled Release Dates	Resource Requirements
Bldg 76, Main Entrance, Fort Bragg, NC	12/01/2020	1 software developer + 1 hardware tech
Bldg 360, Room A, Fort Bragg, NC	12/02/2020	1 software developer + 1 hardware tech
Bldg 81, Room J, Joint Base Lewis-Mcchord, WA	12/7/2020	1 software developer + 1 hardware tech

- Technology Considerations

Target	Technology/Infrastructure Requirements	Support Requirements
Bldg 76, Main Entrance, Fort Bragg, NC	Outdoor system install. CAC and voice scanners only.	Contact site POC upon arrival for access
Bldg 360, Room A, Fort Bragg, NC	All-scanners install.	Access to site requires military police escort
Bldg 81, Room J, Joint Base Lewis-Mcchord, WA	CAC, retinal, hand scanners only.	Access to site requires military police escort

- Personnel Training

Site	Scheduled Dates	Trainer	Materials
Stimson Hall, Fort Bragg, NC	12/3/2020	Software developer	System manual
Waller Hall, Joint Base Lewis-Mcchord, WA	12/8/2020	Software developer	System manual

Maintenance

Software Maintenance

Component Releases

- Major component releases delivered once a year, December
- Minor component releases delivered as needed per month, dependent on customer feedback
- Emergency releases immediate-priority
- Monthly scheduled systems check and maintenance

Support Plan

- User Support
  - 24/7 helpdesk technician via phone or email

  - On-site technical services may be scheduled

- Incident Resolution
  - Primary goal is to restore system functionality ASAP

  - Incident reports available for customer records