RIMAC

Dec. 11, 2023

# Information Security


Information Security
Vision and Oversight

# Information Security and Cybersecurity Strategy

RIMAC

## Threats

Cybercriminals

Insiders
Human
Error

Insiders
Internal
Fraud

## Strategy

External Security

Internal Security

## Controls

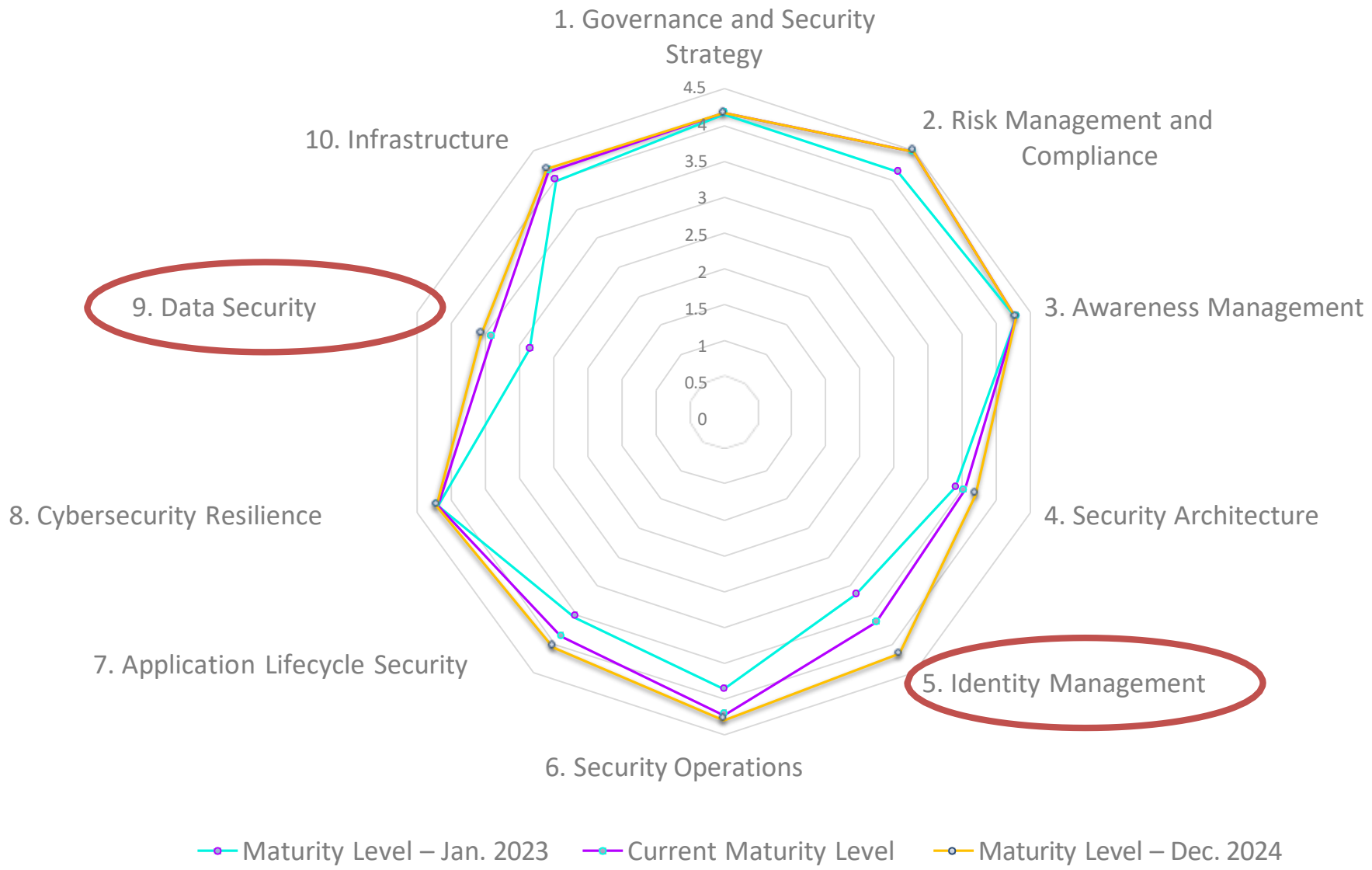
Cybersecurity Controls

Access to information according to user duties

Correct use of information

2024 focus

# Information Security Maturity Advances



# Indicators 2023

# Indicators

## Information Security Risks

Risk Inventory

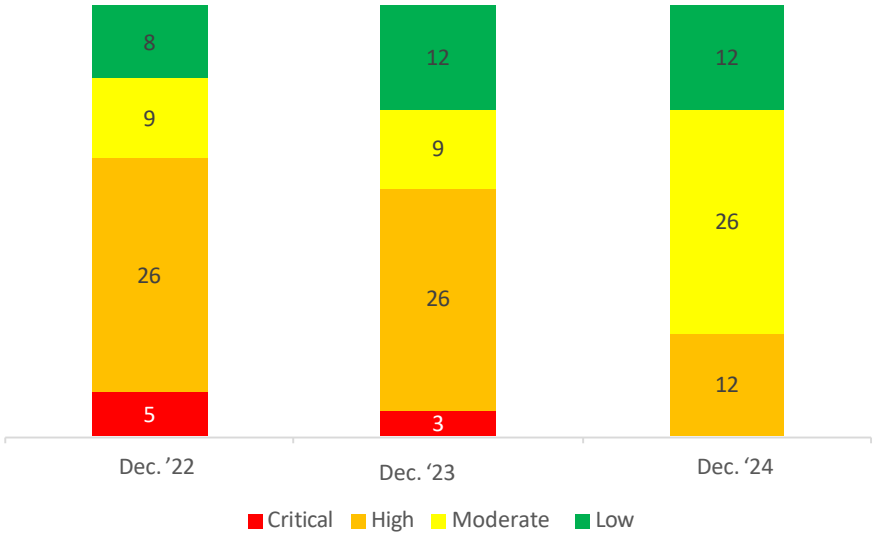
(50 risks)

Critical: 3

- Unauthorized access: 3

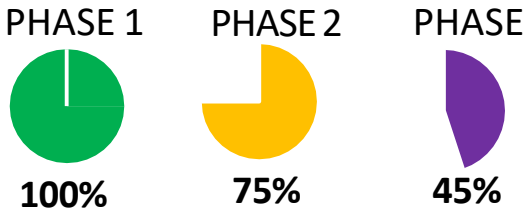
High: 26

- Integrity: 1
- Regulatory violations: 1
- Unauthorized access: 9
- Data leak: 8
- Unavailability: 7



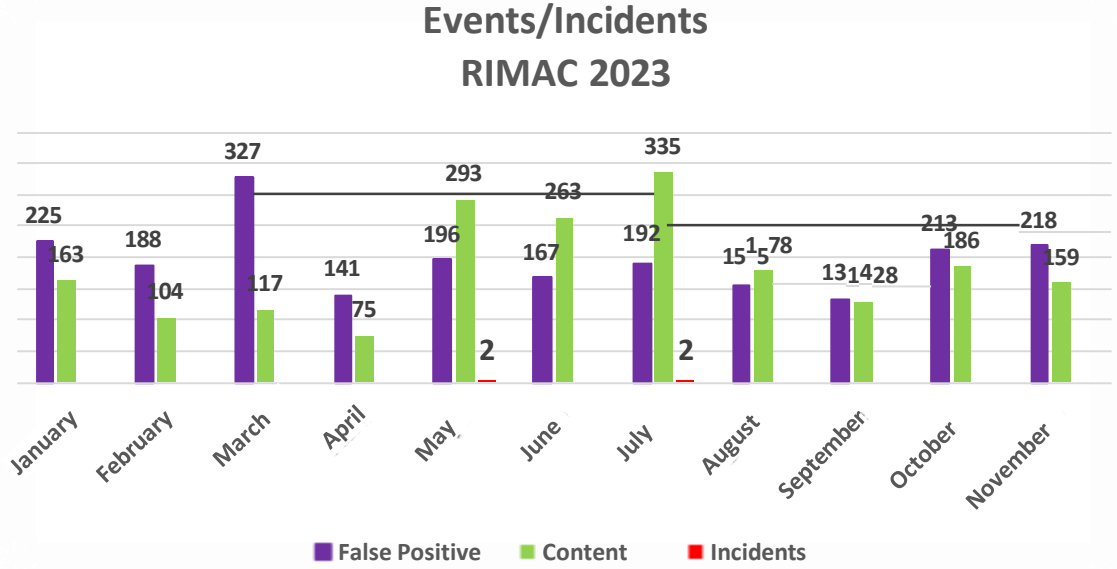

- All risks are continually monitored.

## Strategic Information Security Plan




## Information Security Maturity

| Close 2022 | Current | Close 2023 |
|---|---|---|
| 3.93 | 4.06 | 4.1 |



# Key Achievements 2023

# Achievements 2023

| | |
|---|---|
| **1. Security Governance and Strategy** | • Security evaluation of 30 critical suppliers (impact on business continuity, IT, and Royal contract). |
| **2. Risk and Compliance Management** | • Definition of the User Risks indicator, based on knowledge and behavior of team member.<br>• Mitigation of three critical risks.<br>• Risk assessment and information classification in Business Insurance and Personal Insurance Divisions.<br>• PCI recertification. |
| **3. Awareness Management** | • Strengthening of culture program:<br>  • Salesforce participation in “Mission Possible.”<br>  • Dissemination of awareness-raising videos on information protection.<br>• Information Security Week with talks and office activities. |
| **4. Security Architecture** | • Three new baselines were created, and seven were updated.<br>• Four new security guidelines were created, and 10 were updated. |
| **5. Identity Management** | • control monitoring (high, low, changes, privileged users, access recertification for core applications).<br>• Implement of IT control tools for the management of local user administrators (PCs) and privileged server users (150 critical servers).<br>• Conflict resolution for functional separation in three processes and drawdown of four additional processes. |

# Achievements 2023

| | |
|---|---|
| **6. Security Operations** | • Increased CyberSOC coverage and capacities.<br>• Discovery of cloud and on-premise assets for vulnerability management.<br>• Implementation of baseline monitoring capacity in cloud environments. |
| **7. Application Lifecycle Security** | • Increase in the coverage of projects evaluated by IS from 44% in January to 82% of projects in November. |
| **8. Cybersecurity Resilience** | • Reduction in the number of incidents by 50% compared to 2022 (from 10 inc. to 5 inc.). |
| **9. Data Security** | • Implementation of information classification tool in 1,000 pieces of user equipment.<br>• Implementation of data loss prevention (DLP) tool in PCs and cloud, and configuration of policies to restrict outgoing confidential information via noncorporate means.<br>• Implementation of device control tool to limit information leaving Rimac on personal mobile devices. |
| **10. Infrastructure** | • Implementation of cloud cybersecurity monitoring (CASB).<br>• Implementation of endpoint navigation control (SWG). |

# Key Risks and Threats

# Key Risks and Threats

**Critical Risks**

- Unauthorized access to applications by third parties when such access is not included in their job position profile.
- Unauthorized access to critical application options by team members when such access is not included in their job position profile.
- Effects on information confidentiality due to a lack of two-factor mechanisms implemented in internet-facing portals.

**Threats**

- Information leaks due to inappropriate use of Gen AI tools.

Thank You

RIMAC