UNOPS Cybersecurity Framework

Current status and future roadmap | December 2022

Table of Content

Abbreviations and acronyms

Abbreviation/Acronym	Meaning
APM	Application Portfolio Management
CERT	Computer Emergency Response Team
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
DLP	Data Loss Prevention
DTN	Digital and Technology Network (under HLCM)
EA	Enterprise Architecture
EAM	Enterprise Architecture Management
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning (system)
IAIG	Internal Audit and Investigations Group
ICT	Information Communication Technology
IdP	Identity Provider
IMAP	Internet Message Access Protocol
ITG	Information Technology Group (UNOPS)
IS	Information Security
NIST CSF	National Institute of Standards and Technology cybersecurity Framework
OD	Operational Directive
ORM	Obsolescence Risk Management
SaaS	System as a Service
SOC	Security Operations Centre
SWIFT	Society for Worldwide Interbank Financial Telecommunications
HLCM	High-Level Committee on Management
UNISSIG	United Nations Information Security Special Interest Group (under DTN)
UNOPS	United Nations Office for Project Services
ZT	Zero Trust

Executive summary

In response to JIU's recommendation no. 1 in its report on cybersecurity in the UN System Organizations (JIU/REP/2021/3) ,this report represents a comprehensive self-assessment of UNOPS' cybersecurity framework.

In a world of ever increasing cyberthreats, where any individual, organization or government can become desired targets, and motives might range from pure financial gain, reputational damage, or just simple malice, UNOPS acknowledges the responsibility to not put its partners, clients, personnel and vendors at risk by pursuing sufficient and appropriate cybersecurity capabilities.

The challenge of safeguarding all UNOPS systems, data, and devices is not trivial given the new ways of working for a distributed mobile workforce, plentiful and widespread operating locations and an ever increasing need for new software services, integrations and sharing of data. A challenge that UNOPS takes seriously and recognizes the importance of.
This is not only addressed from a technical perspective, but more importantly, through culture and training of personnel as UNOPS observe an increase in attempted attacks utilizing the human attack vector through phishing, spoofing or other email-based mechanisms. As such, cybersecurity in UNOPS is regarded as a joint effort where personnel is the first line of defense.

Over the last five years, great strides have been made with regards to the strategic goal of migrating the UNOPS IT landscape into the cloud and cementing a web-only approach to systems tools. UNOPS now has centralized digital identities and login, file repositories, critical business systems, collaboration tools, and has policies, processes and standards that carefully reviews and reduces proliferation of shadow IT.

This new landscape is not only more centralized and manageable from an operational perspective, but also regarded as a required foundation for further enhancement of cybersecurity in UNOPS as it enables centralized logging, monitoring, and corresponding effective detection and incident response.

Finally, UNOPS seek to further enhance its cybersecurity in 11 distinct focus areas; (1) Alignment with UN standards on cybersecurity, (2) Develop and implement UNOPS' Zero Trust architecture (3) establishing a UNOPS Security Operations Center, (4) enhancing our capabilities to prevent data loss, (5) further strengthening our device management, (6) introducing a stronger anti-malware capacity, (7) develop a more comprehensive security awareness training programme, (8) hardening UNOPS email communications systems, (9) increase the threat intelligence capabilities and capacity, (10) complete an internal security assessment across the core digital landscape, and finally (11) operationalize continued vulnerability scanning and penetration testing.

UNOPS cybersecurity - Today

UNOPS cybersecurity capacity and organization

UNOPS has historically treated cybersecurity as a natural extension of IT infrastructure operations, under the office of the CIO, without dedicated cybersecurity specialist positions. As the threat landscape, and UNOPS itself, is constantly growing, the need for strengthening cybersecurity is paramount. In February 2019 a dedicated Chief Information Security Officer position was established to refocus and coordinate UNOPS' information security efforts, such as information security awareness training and alignment with best practice frameworks and standards in the realm of cybersecurity.
The position did not come with a dedicated team, but relied on close collaboration with the IT group. As a result of this dedicated function, good strides have been made with regards to personnel training on information security awareness training, system hardening, vulnerability scans, policy updates on data classification and information inventory.

Today, the organization around cybersecurity in UNOPS consist of six key components:

1. **Personnel**
    a. All UNOPS personnel are trained to look for- and report any cybersecurity related incident to their local ICT focal point, ranging from suspicious emails, loss- or compromise of devices, to detected anomalies in systems they are using.

2. **Local ICT focal points**
    a. This is the first point of contact for UNOPS personnel with regards to reporting personal cybersecurity incidents. ICT focal points will ensure further escalation to ITG Infrastructure and/or CISO. There are ICT focal points in all regions and most offices where UNOPS operates, resulting in good capacity and timely response compared to a centralized similar function.

3. **ITG**
    a. ITG Operational Teams- Teams for hosting, monitoring and disaster recovery of UNOPS business applications.
    b. ITG Product and Platform Teams - Teams for development and management of UNOPS business applications. Responsible for secure development and adherence to established UNOPS standards. Assists in incident response.
    c. Headed by CIO

4. **Enterprise Architecture**
    a. Responsible for establishing technical IT security standards across the IT landscape, including best practices with regards to areas such as Identity and Access management, Multi Factor authentication, IT infrastructure hardening and other technical areas. Collaborates greatly with the CISO for alignment and shared roadmapping.
    b. Reports to CIO

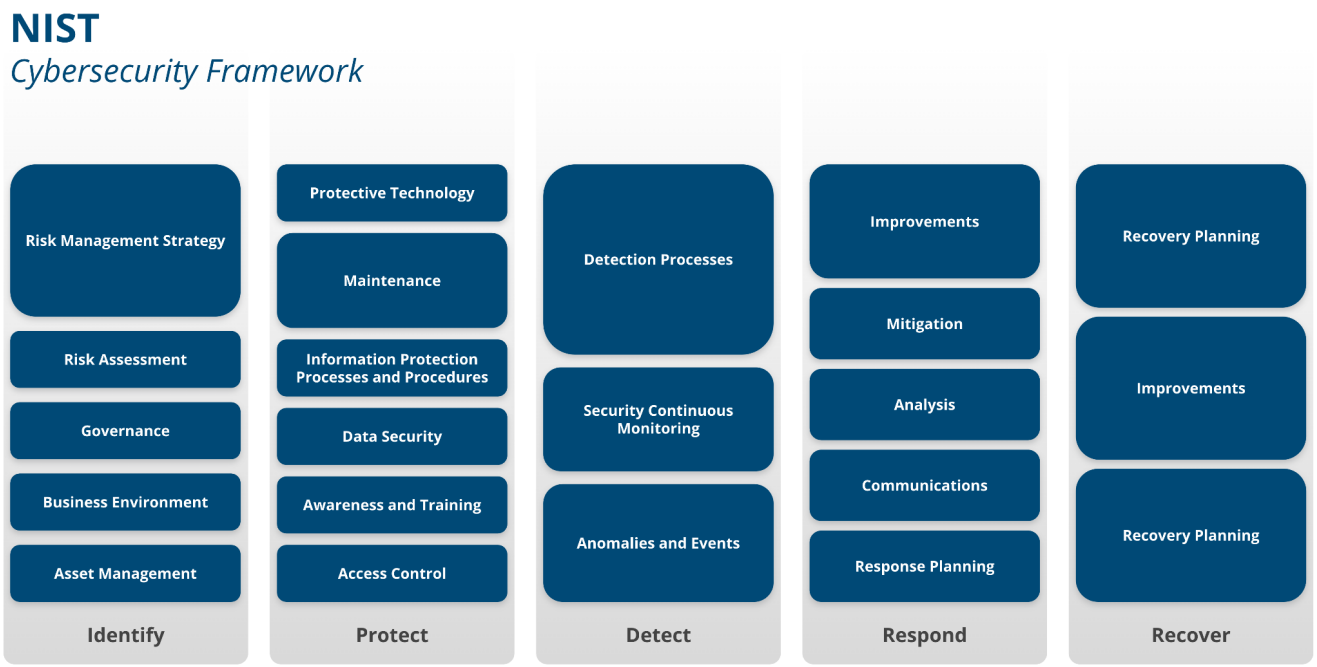
5. **Chief Information Security Officer**
    a. Accountable for information security. Develops and facilitates UNOPS-wide information security policies, standards, and guidelines to manage due care and respond to changes in the organization's operating environment.
    b. Reports to the CRO

6. **Office of the Chief Risk Officer**
    a. Ensures alignment of cybersecurity risks with the Risk Management framework and is responsible for periodic review of control effectiveness and overseeing progression. Additionally, the CRO Offices

supports UNOPS in evaluating and rolling out insurance solutions against cybersecurity exposures as and where feasible.

UNOPS cybersecurity functions

While UNOPS does not follow a specific standard cybersecurity framework in full, this chapter will be using the NIST cybersecurity Framework categorization of cybersecurity functions to describe the current state of cybersecurity in UNOPS within the five functional areas: Identify, Protect, Detect, Respond and Recover.



Identify

Risk management, internal controls and external assessments

cybersecurity risk management in UNOPS seeks to align with the overall Enterprise Risk Management framework, that are outlined in the following Policy Documents:

OPERATIONAL INSTRUCTION REF. OI.FG.2022.02 RISK MANAGEMENT:
https://content.unops.org/documents/libraries/policies-2020/operational-directives-and-instructions/risk-management/en/OD.FG-Risk-Management-2.pdf

Operational Directive Ref. OD.FG.2020.01Internal Control Framework:
https://content.unops.org/documents/libraries/policies-2020/operational-directives-and-instructions/internal-control-framework/en/OD.FG-Internal_Control_Framework.pdf

In short, cybersecurity risks are considered inherent to the business, its processes, its projects and third party relations. They are hence identified and analyzed as part of periodical and ad hoc risk assessments in the context of business planning, engagement acceptance, project planning, internal control, system development and access management. This is supported by including cybersecurity related themes in the risk taxonomy of the integrated oUP risk module and its Global Risk Library.

Beyond business and process implications, the technical assessment of cybersecurity risks are mainly done by the CISO, Enterprise Architecture, and the ITG function, but can also be identified and owned by individual projects if there are additional contextual information security parameters that contribute to risks..

Complementing the other risk assessment disciplines, UNOPS internal control framework supports ensuring the effectiveness and efficiency of day-to-day risk responses, and that appropriate oversight is in place.
In addition to this cross-functional internal control coordination and oversight by the dedicated team under the CRO, independent oversight and assurance is provided by IAIG.

As a SWIFT operator, UNOPS is also subject to annual attestation and external assessment on the security controls set forth in the SWIFT Customer Security Controls Framework, which is updated annually to align with industry best practices and standards on cybersecurity.

Excerpt from the Executive Summary of the 2022 version of the CSCF:

> *Launched in 2016 in response to the sophisticated cyber attacks on SWIFT users, the Customer Security Programme (CSP) seeks to pragmatically 'raise the bar' of cyber-security hygiene across all users, reduce the risk of cyber attacks and minimize the financial impact of fraudulent transactions. There has been a continued evolution since 2016, with SWIFT users facing attacks of increasing levels of sophistication. Modus operandi, the Tactics, Techniques, and Procedures (TTPs) have progressed and changed as institutions strengthen security measures. The persistence of such threats emphasizes the importance of remaining vigilant and proactive in the long term. While users are responsible for protecting their own environments and accesses to SWIFT, the CSP has been introduced to support customers and drive industry-wide collaboration in the fight against cyber fraud. The CSP establishes a common set of security controls known as the Customer Security Controls Framework (CSCF) which is designed to help customers to secure local environments and to foster a more secure financial ecosystem.*

UNOPS has already undertaken assessments in 2021 and 2022, where any observed recommendation automatically goes on the roadmap for timely implementation by respective teams and corresponding oversight through IAIG.

Application and system documentation

UNOPS maintains systems documentation for critical systems to facilitate knowledge transfer and ensure incident response teams are able to orient themselves and isolate potential compromised systems should lateral movement be possible (see the section on 'Network, environment, segmentation and micro segmentation' for further information on mitigations in place). Systems documentation is engrained in the UNOPS ICT team culture.

UNOPS is actively creating an enhanced blueprint of the ICT landscape by employing an Enterprise Architecture Management (EAM) platform in which inventories, such as, 'Application Portfolio Management' (APM), 'Obsolescence Risk Management' (ORM) are used to plan, coordinate and track existing, and future landscape changes. The activities are important to understand the total footprint of UNOPS ICT operations and system interdependencies, which in return leads to understanding critical junctions where security is impacted.

Data inventory and classification

UNOPS follows a 4-level classification scheme for data:

1. Public
2. Unclassified
3. Confidential
4. Strictly confidential

Their definition and more details can be found at

Executive Office Instruction Ref. EOI.IAIG.2019.02
Information Classification
https://content.unops.org/documents/libraries/policies-2020/executive-office-directives-and-instructions/privacy-and-information-security/en/EOI.IAIG-Information-Classification.pdf

Today, all offices are required to fill out, and review, data inventory spreadsheets with their corresponding data classification. While this ticks the box from a pure compliance perspective, it does not meet UNOPS' ambition for effective global data loss prevention mechanisms. Please see the Future Roadmap for the plan on this, where automated classification and corresponding data loss prevention measures are discussed.

Device inventory

UNOPS ' primary application delivery vehicle is the Chrome browser as all applications are web-based. The browser is used to access all UNOPS business applications and will detect when UNOPS credentials (@unops.org) are used and request personnel link their browser instance to the UNOPS credentials. This in turn allows UNOPS to enforce a set of browser configuration settings, key among them an 'endpoint verification' extension which facilitates UNOPS device inventory and device compliance status. In addition to the Chrome browser extension all mobile devices connecting to the UNOPS productivity suite are also included in the device inventory.

The device inventory facilitates lightweight device management capabilities such as (1) device blocking in case of an incident, (2) device compliance monitoring in areas such as disk encryption, screen lock, etc., (3) device credential expiration to ensure new login and policies are adhered to.

In addition, UNOPS have managed Windows devices that are registered and managed in UNOPS LAN based Microsoft Active Directory. These have however become a small minority as they are costly and slow to deploy and maintain. The controls afforded by Active Directory management are gradually being shifted to cloud native platforms enabling management away from the office LAN and to enable remote enrollment.

As such, UNOPS is shifting to a cloud native device management strategy as part of the current UNOPS IT strategy that runs to 2025. This stems from the realization that a modern workforce needs to be mobile, flexible and rapidly deployed, in return they expect to be able to access required systems from anywhere, anytime. Be it from their UNOPS issued computer or their personal devices.

Protect

Authentication and access methods

Any access to UNOPS internal applications requires, in accordance with the official UNOPS policy, an individual assigned account that is issued as part of the onboarding process. No shared accounts are allowed.

In terms of account lifecycle management, the scripted accounts creation requires a registered- and approved contract record in the UNOPS ERP (including for retainers and external affiliates), where the corresponding contract start- and end-dates control the state of the account (enabled/disabled).
While the creation is today a partly-manual process performed by the ICT focal points, due to group membership assignment and Organizational Unit (OU) placement, the task of disabling accounts is automated by a daily job that checks the contract in the ERP and acts accordingly. This ensures that there is no prolonged access for personnel without a valid contract.

UNOPS still relies on Microsoft Active Directory to hold the accounts for certain legacy purposes, including backend access to systems, devices and applications that relies on Windows Authentication, but is gradually shifting towards Google Workspace Directory as the single identity provider (IdP).

Today, all internal UNOPS applications that are user facing, are pre-authenticated with Google login, using the OAuth 2.0 protocol. For the legacy-, Windows based applications this is made possible by performing an authentication protocol transition, where the Google OAuth token is converted to a Windows Kerberos token on the UNOPS Network Load Balancers (NLB). This is seamless to the user and there are no connections from the client to Microsoft Active Directory.

As there is no application access that is granted through Microsoft Active Directory, but where it only acts as a repository, it allows us to focus any access security enhancement efforts on a single IDP; Google Workspace Directory. This includes password complexity, password rotation, number of failed login attempts, and Multi-Factor Authentication.

Today, UNOPS is enforcing MFA for all users, and while it is currently permissible to use code generators and push messaging, Short Message Text (SMS) and email has been centrally disabled, due to their inherent security flaws.
For accounts with privileged access (administrative accounts), there is a requirement of physical hardware tokens due to superior security.

For System as a Service (SaaS) applications used in UNOPS, there is a set of minimum technical requirements, including Single-Sign-On (SSO). That ensures that any access to non-UNOPS hosted applications, must redirect to the UNOPS IDP for authentication. The result is that any access to these applications are subject to the same security methods as for our internal application, and that the account lifecycle management process only needs to consider the single account when disabling access across the application.

For access to data in UNOPS' cloud-based reporting platform (Google BigQuery), there is a structured Role Based Access Control framework that begins with defined business-oriented roles in the ERP. Further to this, data access policies are established and maintained, based on data classification, by the data steward in the corresponding policy unit for the data segment in question (HR, Finance, Procurement, etc.).
The approved- and assigned business roles in the ERP are then used in combination with the data access policies applied to the underlying data (dataset-, table-, column- level today) for traceable identity-based access to the data.

Physical IT security

Physical security for UNOPS systems is to a large extent handled by the cloud provider (Google Cloud) for both the productivity suite (Workspace) and for hosted business applications (Google Cloud Platform). This means that the physical security goes far beyond what UNOPS would be able to facilitate with on-premise data centers. To highlight a few of the physical security characteristics of Google Cloud 6 layer security model the below list is included:

- 24/7 surveillance with on-duty guards
- Data replication and sharding across multiple zones and regions
- Strict data storage device asset tracking and access control in addition to encryption at rest
- Building security checkpoints
- Personnel background
- Any many more

UNOPS is migrating away from operating applications on the LAN (on-premises). As of this writing all critical applications have been relocated to Google Cloud and only a few non-sensitive applications remain on-premises and are all scheduled for sunsetting. This enabled UNOPS to treat their networks in a completely different way as all network traffic is encrypted end to end and local networks merely become data carriers without any risk of information leakage. While UNOPS network traffic might not be at risk the physical security of network access and distribution equipment is still secured. UNOPS mandates physical security and access restriction on network infrastructure rooms wherein equipment such as routers and switches are installed. This ensures a high degree of network stability avoiding accidental or malicious equipment tampering.

Network environment

UNOPS applications are web-based to ensure that deployment and reachability for UNOPS personnel remains unobstructed no matter which location or device is available.
UNOPS implements a strict policy on network traffic inside and across the internal- and external border of UNOPS networks:

- All data in transit must be encrypted disregarding network type or data sensitivity

This means that UNOPS does not take into consideration the nature of the data being transmitted, nor on which network the data is being transmitted. All data is encrypted and authenticated at source and destination to mitigate data loss and tampering while in transit.

The network environment greatly reflects this across the various network architecture dimensions:

End user client device networks

All UNOPS networks for which client devices connect are considered “dirty” and therefore not to be implicitly trusted. No applications are thus hosted in the user network segments. To further secure the client network from cross device pollination attacks ‘private VLAN’ or similar technologies are deployed to prevent client devices from connecting latereally to each other. Thus network traffic is only allowed to designated network services or business applications with strict firewall segmentation and logging.

VPN remote access

UNOPS does not operate a VPN gateway solution and client devices are thus not able to connect remotely to UNOPS networked resources. VPN gateways are often implemented to grant broad network level access to sensitive internal networks and it is UNOPS opinion (aligning with industry consensus on “zero trust”) that all networks are to be treated as assumed compromised. While this might pose a problem “traditional” network architectures as applications would be hosted on a network adjacent to client devices, it does not constitute a problem as UNOPS applications are accessible securely via the public internet without the need for a network tunneling. For other remote access scenarios see the section on Remote access.

Application networks
All UNOPS applications (servers and related infrastructure) are cloud hosted and published securely on the public internet. Across the hosting environment microsegmentation (also known as “host isolation”) is implemented to ensure no lateral movement is possible for advanced persistent threat actors. Logging of all network traffic is implemented as well as regular network traffic policy reviews.

Ransomware mitigation

While UNOPS has yet to be a victim of a successful ransomware attack, UNOPS remains very aware of the rise in ransomware attacks and considers it a matter of time before a malicious attempt will be made using this attack vector.
As such, a number of mitigating efforts have been made in order to reduce the risk and potential impact.

1. **User training**
    a. As part of the Information Security Awareness training and UNOPS guidance, users are trained to be on the lookout for, and report, suspicious behavior and anomalies. Once identified they are to halt all activity and contact their ICT focal point for further assistance. This includes emails, a prime delivery vehicle for ransomware. See the section on Communication security for further details on this.

2. **Discontinued use of file servers**
    a. UNOPS used to have a large number of file servers, both in HQ and field offices which would be a prime target for ransomware attacks. These document repositories have been replaced with online storage in Google Drive (Enterprise plus), where traditional ransomware attacks would not be successful. All upload/download of binary files to Google Drive is subject to centralized malware scan.

3. **Shift away from binary file types**
    a. UNOPS embraces the cloud-native document types that exist today. These files only exist online and should-, and cannot be downloaded, transferred, and more importantly: encrypted using normal methods.

4. **No local desktop software or files**
    a. UNOPS follows a web-only principle in terms of application availability, which ensures that any client device compromised with ransomware should not hold documents or critical software. As always, there will be the need for exceptions, and these are subject to review and approval from the Enterprise Architecture and Platforms review board that is chaired by the CIO, where the risks and mitigation efforts are properly coordinated.

5. **Complete daily backup**
    ○ Servers, databases, and other UNOPS-hosted IT components and artifacts, are subject to daily backup and are a vital part of disaster recovery planning and testing.

Remote access

Remote access is defined as the process of connecting to a UNOPS system, outside of the normal web based connectivity paths for UNOPS applications. An example would be to connect to a shell or desktop session on a system hosted within the UNOPS secured network perimeter.

Remote access for UNOPS systems are divided in two distinct categories. Namely (1) end user remote support access and (2) privileged account remote access.

Common among both types of remote access is the following security requirements:

- Network traffic must be encrypted in transit.
- Authentication must be performed using UNOPS official identity provider and be subject to enforced MFA.
- Only approved remote access software and agents can be used.

End user remote support access
In addition to the common requirements the following controls are required by policy for end user remote support access:

- Remote support access scenarios (wherein a support representative connects to another end user's active or passive desktop session) must be with consent and approved in real time.

Privileged account remote access
In addition to the common requirements the following are required by policy for end user remote access:

- Only the approved and official administrative remote access facilities are approved and must be subject to strict audit logging.

Communication security

As many organizations, UNOPS relies heavily on its ability to communicate in a safe, reliable and trustworthy manner with internal as well as external stakeholders. To ensure UNOPS communications are secure and robust the following communication security provisions are in place:

Email
To protect email communication (both inbound and outbound) UNOPS imploys a wide range of industry standard security practices. To protect UNOPS end users from fraudulent emails UNOPS email system utilizes Google's high ranking email protection to detect, quarantine and warn end users of known and suspicious emails. Detations include, but are not limited to, (1) spoofing organization personnel names and domain names (2) detect unauthenticated email senders, (3) detect emails with malware content, (4) detect dubious wording, (5) crowdsourced and AI/ML detected SPAM, and many other detection dimensions.

UNOPS operations personnel get instant notifications in case of incidents that require a human intervention and have dashboards, reports and investigation tools to help track and facilitate incident response. This includes phishing attempts and spam alerts that can either be detected from a system perspective, reported by colleagues, or reported by external parties.

To further enhance email security, UNOPS is enforcing which emails clients personnel can use to retrieve emails with. UNOPS is no longer allowing email desktop clients such as, but not limited to, Microsoft Outlook/Apple Mail/Mozilla Thunderbird to retrieve and store emails on desktop environments. This prevents both data exfiltration as well as data loss in the event of a compromised unsecured desktop endpoint. Furthermore mobile device email clients are restricted to require device screen lock. IMAP has been blocked centrally.

Full email journaling is enabled for all internal and external email communications to facilitate incident investigations, and all events are stored in immutable logs.

Instant Messaging and VoIP
To facilitate personnel having instant text based communication, UNOPS deploy an organization wide instant messaging client which allows all personnel to lookup, contact and communicate with all colleagues. This effectively drives organization conversations into a secured messaging environment for which traffic is secured while in transit and fully authenticated. In addition to the text based channel the client also supports VoIP enabling UNOPS personnel to partake in end-to-end encrypted "voice calls".

In the event of a critical incident or for sensitive communications, where regular UNOPS instant messaging is unavailable or unsuitable, UNOPS has standardized on the use of the Signal application for end-to-end encrypted communication, in alignment with UN guidelines.

User training

UNOPS recognizes properly trained personnel as the most valuable first line of defense against a number of threats, such as phishing attacks, social engineering, and other cyberthreats that follow the human attack vector.
Today, all UNOPS personnel are offered courses in Information Security Awareness as part of their onboarding process. These self-paced courses are delivered online through the UNOPS eLearning portal and can be accessed globally.

Enterprise Architecture standards and guidelines

In addition to the operational teams, security technologies and cybersecurity processes UNOPS embeds the strategic and forward planning activities of cybersecurity within the 'Enterprise Architecture' function. The enterprise architecture function is responsible for developing cybersecurity roadmaps of related maturity enhancements across the entire application landscape, in coordination with the CISO, CRO, and CIO. In addition the Enterprise Architecture function performs forward-looking industry trend tracking to help UNOPS understand developing threats that are coordinated with the Enterprise Risk Management- and Internal Controls framework, as well as maintain a catalog of mitigation strategies to be considered for implementation.

Furthermore the Enterprise Architecture function has a critical role in publishing UNOPS mandatory standards and related guidelines on cybersecurity, in alignment with the CISO, for operational and product teams to implement and by subject to compliance checks on.

Threat simulations

UNOPS strives to perform an annual simulation of user-facing attacks. Phishing campaigns being the most frequently used approach.

It should be noted that after UNOPS transitioned away from self-hosting email services (Microsoft Exchange Server) in 2018, there has been a drastic decrease in delivered spam and phishing emails. As all emails are subject to Google's malware detection algorithms (see Communication security section), it has actually proven difficult to run the simulation campaigns as it requires a number of steps to successfully deliver a suspicious email. These steps include whitelisting and bypassing certain security features for specific sender domains in order to facilitate the security awareness and readiness level of the organization.

Nonetheless, the simulations are still regarded as a vital component in Information Security Awareness training, as UNOPS observes that phishing attempts are becoming more intelligent and that the work/private borders are becoming more blurry. As such, a colleague might be targeted on their private communication platforms where UNOPS information is being phished for. So having a robust workforce that is able to detect malicious emails is paramount.

Detect

UNOPS detection capabilities cover a range of vectors in regards to malware detection as well as system uptime and performance. This chapter will break them down and detail them.

System monitoring

For UNOPS hosted applications a performance and uptime monitoring solution (SolarWinds) is in place to ensure systems are running according to established baselines. Performance and uptime deviations from baselines are investigated to ascertain the root cause and likelihood of malicious actions against UNOPS systems.

Vulnerability Scanning

UNOPS hosted applications and servers are subject to vulnerability scanning to detect if any system misconfiguration and known compromised software are present and exploitable. The scans include potential lateral movement attack vectors, such as open server ports, but also application-level areas like at-risk or legacy libraries and frameworks.

Collaboration suite monitoring

Google Workspace (formerly "G Suite") implements a range of advanced detection mechanisms. Email phishing, spoofing and malware attachments are identified as well as fraudulent login attempts. These incidents are recorded in the central 'Workspace Security Center' for incident response personnel within ITG to action.

Malware detection

In regards to malware detection UNOPS has a limited deployment of malware detection agents (BitDefender) on managed Windows device endpoints. Malware incidents are reported to a central console for incident response. In addition, and to cover for endpoints without agent based detection, Google Drive (the primary document and file repository) supports malware scanning on uploaded and downloaded files. In addition for end users which have opted into Google's 'Advanced Protection Program' the Chrome browser will also protect against malicious downloaded content by warning or blocking downloads.

User incident reporting process

In addition to system detection capabilities UNOPS have instructed personnel (as part of security awareness training) to be vigilant and report any suspicious application or IT behaviors observed during the normal course of business. This can either be through the UNOPS email system (phishing or spam) that has dedicated functionality for reporting, or through user generated reports that are funneled through the ICT focal points for further investigation and actions. The latter includes loss/theft of devices, observed spoofing and other non-automated incidents.

Respond

Once an IT security incident has been detected, be it from system monitoring, internal ITG personnel, manually detected and reported by employees or external parties, the incident response(s) begins. There is today a split between personal- and system incident handling:

For minor, personal local IT security events, such as laptop/mobile theft/loss, the local ICT focal points will take immediate steps to mitigate potential further impact.
Once these mitigating steps have been performed, an incident report is submitted to the CISO for review and potential follow up. In certain cases, follow up steps could be to look for suspicious activity (large volume of downloads, logins from atypical locations and IP addresses). The CISO works with relevant stakeholders such as, but not limited to, ITG, Legal, Communications and external authorities if required.
In addition to the internal flow for these types of incidents, a report is also submitted to UNDSS and relevant local authorities.

For major, corporate- and external wide incident response related to systems, these are today triaged and initiated by UNOPS ITG and cover all types of incidents that cause disruptions to business systems and/or data. This includes incidents caused by bugs, hosting performance issues, malicious acts, etc..

Once the incident has been categorized and given a priority, a Major Incident coordinator is identified and a dedicated Incident Response Team is assembled.
Depending on the nature of the incident the incident response team may consist of members from ITG, business teams, CISO, or any other relevant stakeholders that combined can make required decisions and take appropriate actions and ensure diligent documentation and reporting.

Recover

Data and system recovery

UNOPS recovery capabilities are centered around post-incident data and system restore. In the event that data was lost by accident or by malicious intent UNOPS will, as part of the Major Incident Process, instigate recovery steps based on an approval workflow. Lost data will be restored from backup and relevant stakeholders informed.

UNOPS maintains a system inventory with relevant data protection(s) capabilities in place and related RPO/RTO.

The restore capability is tested on an annual basis and covers the full set of data restore capability as well as reestablishing production grade systems availability in the event that systems were impacted to a level that system availability were impacted.

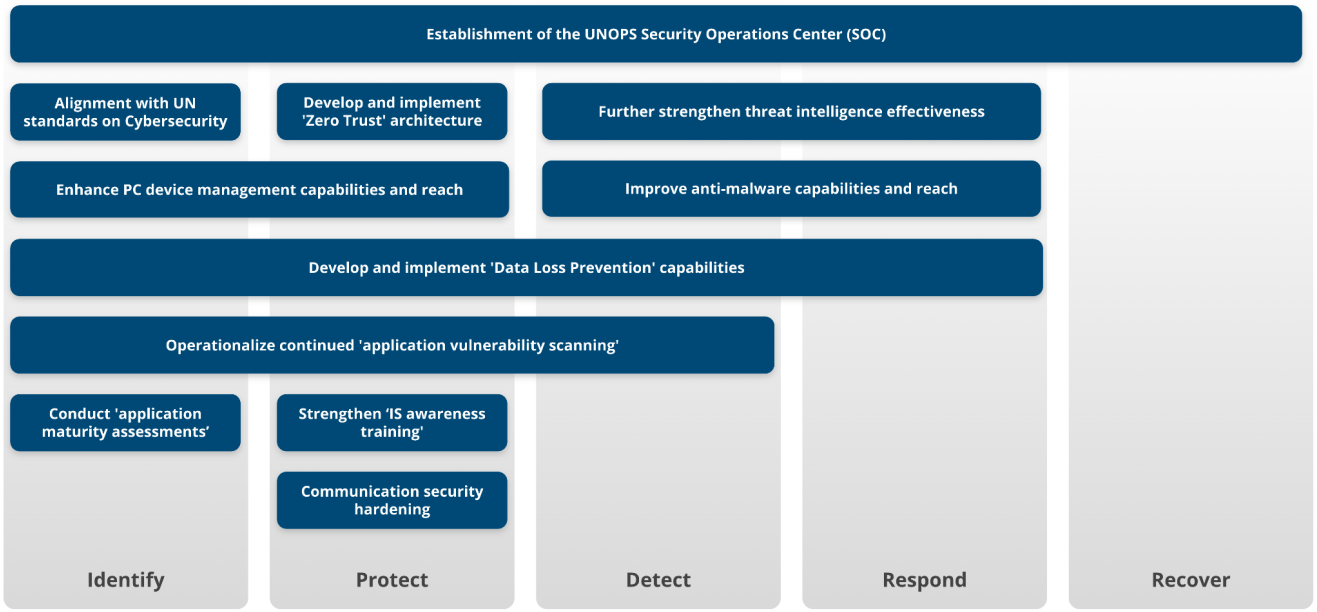
In addition to the disaster recovery capabilities UNOPS operational teams also provision “snapshot technology” to allow for granular operational recovery points as part of application development and deployment. These also serve as a valuable reverie point for potential incidents.

UNOPS cybersecurity - Future roadmap

While UNOPS' existing cybersecurity capabilities remain meaningful in the current operating context, a number of areas lend themselves not only to enhancement, automation and optimization, but also discovery and innovation. UNOPS will seek to mature these cybersecurity capabilities during the period 2023-2026, subject to available funding.

UNOPS Cybersecurity Future Enhancement Roadmap (2023+)

Augmenting existing capabilities



Alignment with UN standards on Cybersecurity

As identified by United Nations Information Security Special Interest Group (UNISSIG) and promulgated through HLCM-DTN, UNOPS is pursuing full alignment with the Minimum Baseline Standards as defined in section 5.4 in Digital & Technology Network (DTN) Session Report - Virtual Session, 20-21 October 2021

Current status on this alignment as of November 2022:

Baseline Standard Item	Sub-item	Compliance Status
Implement and enable Multi-Factor Authentication (MFA) to the maximum extent possible; all accounts that access systems via the internet should be configured with MFA.		Fully implemented
Mainstream basic cybersecurity best practices:		-
A	Maintaining an inventory of organization-owned devices and systems;	Fully implemented
B	Ensuring organization-owned devices and systems are regularly updated;	Under development
C	Decommissioning systems that no longer add value	Under development
D	Implementing access control to non-public resources, and ensure all users receive regular information security awareness training	Fully implemented
Perform regular penetration and/or security assessment tests (i.e. at least once a year);		Under development
Ensure cybersecurity risks are adequately included in enterprise risk management processes		Under development

UNOPS is a member of the High-Level Committee on Management (HLCM), the Digital Technology Network (DTN) subgroup and UNISSIG and will continue to support and pursue further alignment as agreed in the broader UN community.

Develop and implement 'Zero Trust' architecture

In order to better protect UNOPS information systems a continued pursuit of a “Zero Trust” (ZT) system architecture will be pursued with additional system level “zero trust” capabilities. UNOPS will enhance its current implementation of a “zero trust” architecture introducing device state assessment to validate system access decisions. UNOPS follows the published definition and recommendation of “zero trust” implementation as proposed by the ‘Digital & Technology Network’ (DTN) ‘United Nations Information Security Special Interest Group’ (UNISSIG) ‘Working Group on Zero Trust’.

The proposed “zero trust” definition outlines a comprehensive security architecture taking into account the following dimensions:

1. **Data**
2. **Identity**
3. **Endpoint devices (client devices)**
4. **Infrastructure**
5. **Network**
6. **Applications**

UNOPS has been on their ‘zero trust’ journey for multiple years which is reflected in the current related capability as described in the section UNOPS cybersecurity - Today. To continue the “zero trust” maturity journey UNOPS will focus on strengthening the capabilities within the following dimension:

(1) Data

UNOPS continuously strives to understand, and classify its information assets to assess which data must be subject to additional security measures for safeguarding. As such UNOPS is undertaking data classification exercises, via existing dedicated data governance panels, but also through a near-term dedicated project , which in turns enables UNOPS to enforce control on the individual data objects channels (such as documents, email, or transaction record) or wholesale on the custodian application/system. Appropriate data classification is foundational for UNOPS’ ability to restrict, harden or warn on data access requests in real time. (see section on DLP),
UNOPS is also very cognizant of the fact that the classification and corresponding data loss prevention measures need to follow the data across systems and channels. It is a fallacy to rely solely on central server protection when daily processes and communications require the information to be shared, presented and modified in collaboration tools.

(3) Endpoint devices

Additional realtime device level checks will be put in place on UNOPS hosted applications to ensure that device compliance is validated prior to application or data access. Compliance checks include (A) disk level encryption status, (B) anti-malware status, (C) OS patch and version status, (D) Device approval status, in addition to other metrics such as geographical location, user identity and time of day.
This means that UNOPS will be able to prevent access from client endpoint devices that are not compliant with the corresponding ruleset. As an example, UNOPS could prevent access from a BYOD device to the ERP system, but still allow access to the absence management system from the same device depending on the level of device security compliance.
Additionally an enhancement to the device inventory practice will introduce an additional level of device segmentation around BYOD vs organization owned devices. This again enables UNOPS to make concrete access and feature availability decisions depending on the device status.

For additional enhancements see see sections on Device management and Anti-malware)

(4) Network

All business network traffic in UNOPS is subject to strict encryption requirements and as such no business application or service can operate within UNOPS without enforcing encryption and authentication. As a cornerstone principle within “zero trust” this allows UNOPS to operate on networks which might not be deemed to be fully secure. While UNOPS employs a range of network security measures on its office networks UNOPS does not at any point rely on the security of the network. Rather UNOPS networks are operated as “internet cafe’s” optimized for reliability and speed while fully ensuring that traffic is encrypted and authenticated end to end to fully mitigate data compromise as a result of a break in the chain of custody. In addition this application architecture allows UNOPS applications to be accessible irrespective of the network medium used for connectivity safeguarding personnel, information assets and allowing UNOPS workforce to be agile and connected at all times.

The remaining dimensions: (2) Identity, (5) Network and (6) Applications are matured to an acceptable or even leading level, and will be a second priority.

Establishment of the UNOPS Security Operations Center (SOC)

While there are operational IT security and IS capabilities in place in UNOPS today, they need to be resized to reflect the size of the organization. This includes dedicated personnel with responsibilities in monitoring and incident response, rather than relying on additional roles and functions attached to existing IT personnel.

UNOPS has therefore begun the process of establishing a SOC with buy-in and support from senior management. Current status as of November 2022 is that UNOPS is finalizing the procurement of consultancy services for a deeper review of UNOPS IT security needs and functions, with respect to the business context and IT landscape, and assistance for constructing the initial capacity and capabilities of the SOC.

Responsibilities include:

- Live monitoring of systems, data and events to detect anomalies and threats with supporting tooling for SIEM and XDR.
- Ensure timely and structured incident response coordination
- Provide reports and statistics on threats and incidents
- Drive the automation effort on incident detection and response, including automated playbooks for known events, as well as AI for DLP as an example.
- Perform- and assist in vulnerability scans and penetration tests of systems
- Assist UNOPS ITG development- and IT hosting functions in aligning with best-practise standards and practices on IT security.

It is expected that that contracting will be concluded in 2022, the review performed early 2023 and that the initial SOC in UNOPS will be fully operative by H2 2023, where the capacity and responsibilities will be further assessed for potential adjustments.

Develop and implement 'Data Loss Prevention' capabilities

As a result of the migration away from local file servers and email-based collaboration to a singular cloud-native collaboration platform, the centralization has provided UNOPS IT/IS with a much deeper understanding and visibility of its data that is being shared on a daily basis. While it has become easier to share and collaborate, it also puts how and what is shared in the spotlight. Something that was previously not possible to monitor and act upon effectively, as the decentralized nature of the organization and then corresponding IT infrastructure lent itself to local efforts for data loss protection. While traditional efforts focused on the protection of the source business systems, such as the ERP and project management systems, the reality is that people often need to download, augment, prepare or present the data in collaboration tools such as emails, spreadsheets, documents or presentations. The classification of the data, and the risk attached is no less, just because it is a local copy.

As any organization, UNOPS is sharing a substantive ammount of information and data with external parties, basically reflecting what used to be distributed through attached files in emails historically, but now very visible through the centralized nature of the platform that provides overview through logs and reports on all UNOPS document events, including access and sharing.
The volume and potential sensitivity does indeed require a dedicated mitigation effort to reduce the risk of either accidental- or intentional wrongful data sharing or exfiltration.

With the new centralized, cloud-based collaboration platform in UNOPS comes the opportunity and commitment to establish a corporate data loss prevention framework. This includes content sensitivity classification, either manual or automated based on AI, that subsequently will be used in platform system policies that notify, prevent or take other actions based on the content, context and policy in question.

UNOPS is also evaluating tooling for automated unsharing of documents on the same platform, which would address accidental sharing.

UNOPS has begun the foundational work in terms of technical data classification prerequisites and identified the required tooling and will conduct a pilot H1 2023.

Enhance PC device management capabilities and reach

UNOPS depends largely on unmanaged devices accessing UNOPS applications and information systems. While this strategy has proven well suited to UNOPS rapid project and global physical deployments, new realities of the cybersecurity environment dictate that further emphasis is put on endpoint device security and thus device management or compliance assessment. UNOPS will not seek to include all devices used for official UNOPS business into full device management as this would limit UNOPS ability to rapidly deploy personnel, but will rather be introducing a range of additional device level checks (see section on Zero Trust) on personnel connecting from unmanaged devices. Devices which do not meet minimal compliance standards for connecting to UNOPS systems can be barred, based on policy, from application access taking into account device compliance level in addition to the information classification of the specific application being accessed.

UNOPS will allow for non-compliant devices to self-enroll into device management or to mitigate compliance shortcomings locally on device in order to pass device compliance check and gain application access. This will greatly limit the need for centralized device management and associated delays in device deployment and thus allow for fast employee onboarding and productivity while maintaining a high level of device security and compliance.

Improve anti-malware capabilities and reach

In regards to anti-malware UNOPS will introduce/enhance its capabilities in the following meaningful ways:

Endpoint anti-malware

UNOPS endpoint device level anti-malware agent is only deployed on a subset of devices used to access UNOPS applications and information systems. With the introduction of a “zero trust” security architecture (see section on Zero Trust) UNOPS will gain the capability to block application access based on device compliance level (see section on Device management). To that end UNOPS will transition from its current legacy LAN based device anti-malware agent deployment to a cloud native endpoint security agent which can be deployed and operated independent of device location or connectivity. This will ensure relevant endpoint device malware protections are available and enforced for all devices used to access critical applications or information systems based on configured policy.

System level anti-malware

In addition to the endpoint device level anti-malware, UNOPS will pursue on-access scanning of documents in business applications, including SaaS and legacy applications.

This will ensure that documents stored in these systems are checked both at the initial upload into the systems and well as potentially years later when they are retrieved. This is important as documents uploaded in year one might not be flagged as infected until a later stage at which the anti-malware community has become aware of a malicious virus.

Strengthen 'information security awareness training' programme

As previously mentioned, UNOPS personnel are the first line of defense against human-vectored attacks, and proper training and awareness training provides the best value possible in this strategy. While UNOPS today, and going forward, have courses and security bulletins on email and Intranet, there are already approved, dedicated budgets for 2022/2023, with corresponding procurement activities that are already initiated to further strengthen this area. This includes best-of-breed training that is updated regularly and reflects the current threat landscape at all times.
While UNOPS have performed the regular simulations on Phishing in the past, there will also be a fresh take to see what vectors are most relevant to train on going forward (dropped USB stick in the parking lot, social engineering, etc.)

Communication security hardening

While UNOPS maintains a very secure communications environment, a range of identified improvements will be assessed and potentially implemented.

Message Transfer Agent - Strict Transport Security (MTA-STS)

UNOPS will assess the feasibility of enforcing strict encryption compliance for inbound emails as it relates to current statistics of partners ability to provide encryption as part of the message transfer to UNOPS. Currently UNOPS does not enforce encryption due to prior examples of lack of encryption capabilities on behalf of external partners' email systems. However the last assessment of these capabilities and associated impact assessment was done in 2019. A 2023 assessment will reveal the extent to which UNOPS will be able to require encrypted email communications with external partners.

'Domain-based Message Authentication, Reporting and Conformance' (DMARC)

In addition to MTA-STS policy review, UNOPS will also assess the feasibility of implementing DMARC policies to instruct external domains how to handle "unauthenticated" messages from UNOPS. UNOPS will gradually migrate to a full "reject" policy upon failed DMARC check for all domains under UNOPS' control and brand. As with the MTA-STS assessment an impact analysis will be completed to ascertain the practicability and timeline of implementing the DMARC compliance policy for UNOPS.

S/MIME

UNOPS will assess the need for 'end to end' email encryption in the organization and, should the need be identified, provision S/MIME encryption capabilities to specific personnel along with relevant training.

Email confidential mode

UNOPS email platform supports a special "confidential mode" in which the message body is not transmitted over normal SMTP. Confidential mode works by sending a special message instructing the recipient to view the message on a secured web site for a limited period of time. This mode will be enabled for UNOPS personnel during 2023 along with training on its use. Its important to know that while the message is not transmitted to the external recipient's email system UNOPS trains journaling capabilities and insight into the transmitted message.

Anti-malware

A range of extended malware protections and detactions are available in UNOPS' email platform. During 2023 UNOPS will review the practicality of enabling the extended malware protections to further secure the email platform from malicious content and block dangerous content from being delivered to UNOPS recipients.

Further strengthen threat intelligence effectiveness

While UNOPS today has an established external network for IT and information security related matters, including national CERTs, ISPs, vendors, and other UN agencies through the UNISSIG working group and key individuals, there is still an identified need to enhance and ideally automate the response to new threat intelligence. Today it is mainly a human-driven process, where a notification around a detected vulnerability normally requires a person to read the correspondence and manually initiate the remediation process. While this qualitative interaction is very valuable and will be supported- and extended going forward, the ambition is to also pursue automated measures, shifting the focus from reactive to preventive. Automated scanning throughout the CI/CD application lifecycle management processes as an example.

Conduct 'application maturity assessments across core digital landscape

As part of further Application Portfolio Management (APM) activities UNOPS will assess the maturity of its "core" applications developed in-house. Each application will be scores on its maturity in regards to the application architecture and operational practices. A full maturity assessment matrix and maturity gap analysis will be produced

for IT leadership to facilitate application risk profiling and prioritize any identified maturity gaps necessitating remediation.

Operationalize continued 'application vulnerability scanning'

While UNOPS currently performs vulnerability scanning, the regularity and scope can be strengthened. UNOPS will seek to onboard additional vulnerability scanning capabilities and ensure scanning, testing and remediation is part of a structured recurrent process at each development and deployment cycle.

Appendix I - UNOPS Minimum Technical Requirements

Requirement	Description
SSO	*Applications must support SSO via* *(1) 'Google Login' (OAuth2 w.OpenID Connect OIDC)* *(2) SAML* *(3) OAuth2*
User provisioning	*Application must support automatic user provisioning via one of or multiple methods:* *(1) SCIM 2.0,* *(2) R/W API,* *(3) Just-In-Time SSO-based provisioning*
Data confidentiality and classification	*Ensure that all information stored and processed by the application is classified and that the application is subject to relevant compliance requirements thereof.*
Billing delegation	*Application must be able to set a custom recipient for invoice and billing handling*
System administration delegation	*System configuration must be able to be delegated to a specific or group of individuals*
Security Event Logging [Audit trail]	*Application must record user access and action for incident and investigation purposes*
License administration delegation	*User licenses must be centrally managed and license management must be able to be delegated to a specific or group of individuals*
Application hosting	*Application must be delivered as SaaS (Software as a service)*
Application delivery	*Application must be delivered purely via Google Chrome, as a web application, and must not require any desktop installation- or storage.*
Application integration	*Applications must provide API's to facilitate system to system integrations as well as business process automations to avoid redundant "human intervention" and low data quality.*