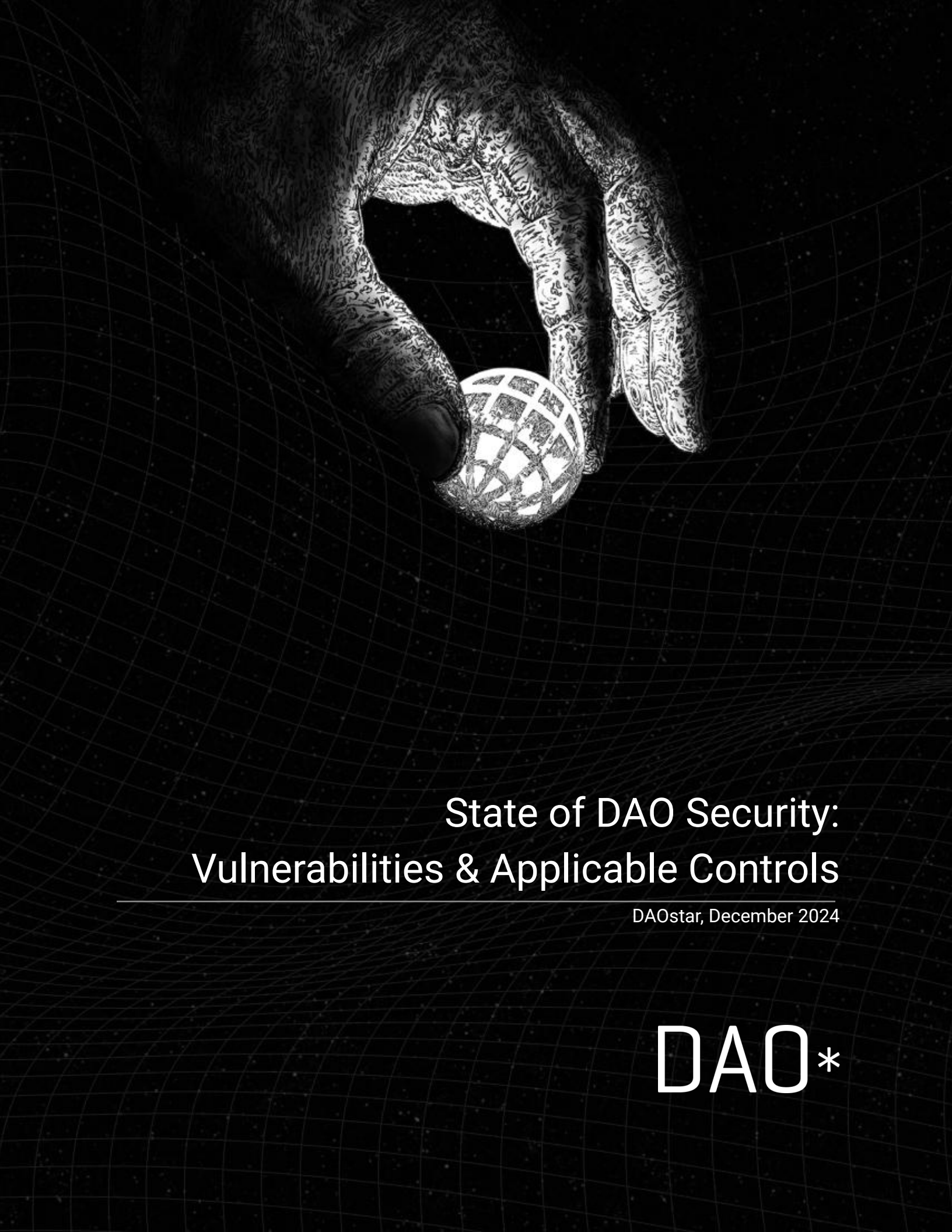

State of DAO Security: Vulnerabilities & Applicable Controls

DAOstar, December 2024

DAO*

Executive Summary

DAOIP-8, or *Recommended controls for DAOs*, is a comprehensive set of recommendations to improve DAO security. DAOIP-8 aims to establish a minimum viable security standard among DAOs, such that all DAOs, irrespective of their scale or governance design, have an easily accessible set of controls to follow as standard practice when it comes to security.

This report sits on top of DAOIP-8, which is short and concise, and provides more context on why certain controls are recommended and why some aren't. This report also explores common vulnerabilities among DAOs and aims to provide useful information on designing capture resistant DAOs.

The report starts with a walkthrough of common vulnerabilities including governance attacks, proposal safety, ineffective incident response & vulnerability management, management of external entities, and lack of security training for key entities. This is not a complete list, but rather some of the most critical vulnerabilities present. With the stage set, it continues to DAOIP-8, outlining two levels of controls - **[MANDATORY],** measures that are critical, and **[RECOMMENDED],** measures that mitigate second-order risks. Out of the 14 controls listed, 8 are applicable to all DAOs irrespective of their governance structure or size. The last 6 controls are for *Protocol DAOs,* DAOs that manage an onchain protocol through governance.

The overarching goal is to encourage DAOs to methodically assess their own risks, refine security strategies, and adopt better operational practices. The report then proceeds to community feedback, highlighting some of the constructive feedback DAOIP-8 has received so far. Note that the specification is fairly new, more feedback from the ecosystem is expected to follow in the coming weeks and months.

All aspects of this work are open-source. You may use this report, as well as DAOIP-8, without prior permission from its authors or DAOstar, to improve the state of security in your DAO, facilitate discussions, or for other initiatives, provided you attribute DAOstar. DAOstar's Github and Slack are the two best channels for joining the discussion. You may also join this Telegram group if that is more convenient.

Disclaimer: The recommendations in this report are intended as general guidance and are meant to structure your security-related discussions, rather than dictate your security solutions. They may not address all specific risks or requirements of individual DAOs and should be adapted accordingly.

About the authors

Amandeep

Aman is the present *Strategy Lead* at DAOstar, and *Governance Facilitator* at Safe{DAO}. He is interested in designing systems for improving capture resistance, accountability, alignment, and resource allocation in DAOs.

Ben

Ben is a co-founder at eth.limo, a public good for dWebsite gateways using the Ethereum Name Service. Ben is interested in the cross section of decentralized governance and its overlap with Web2 technology assets.

Rafael Solari

Raf is a co-founder at Tally. Tally's mission is to make DAOs work. He spends lots of time thinking about how to help decentralized organizations succeed.

Outside of the three main authors mentioned above, this work has benefited from extensive feedback from numerous individuals and organizations. For a full list of contributors, please refer to the *Acknowledgements* page. This work was made possible by a grant from the Ethereum Foundation through the Ecosystem Support Program (ESP).

This report is a publication of DAOstar (or DAO*), the standards body for the DAO ecosystem.

Contents

Introduction to the DAO Security Landscape

DAOs, or decentralized autonomous organizations exist on a broad spectrum of organizational design. For the scope of this work, we have considered a DAO to be any organization that uses blockchain technology to decentralize the management of assets that may be held in onchain or offchain treasury. As this definition is quite broad and it does not distinguish between voting system, execution, tooling, delegation, as well as several other factors, the implementation of controls defined in DAOIP-8 may vary from DAO to DAO.

One of the core tenets of web3 security is trust abstraction using cryptographic guarantees and smart contracts. DAOs too are built on this foundation. Decentralizing decision making reduces the likelihood of a hostile takeover as governance power is distributed among a large number of participants(although to what extent varies from DAO to DAO). While governance power can often be bought by purchasing the governance tokens, there are often additional safeguards built against this in the form of security councils that can veto malicious proposals, or as permissioned sets of actors that can execute specific steps (for example, move a proposal to a vote, or execute a proposal). Active voting thresholds and quorum guardrails are also often employed, in order to specify a minimum participation baseline, ensuring that risks introduced by low voter turnout can be effectively mitigated. The long game of governance often acts as a practical filtering mechanism, which favors more active and committed actors to rise to prominence, for example, as the largest delegates.

However, decentralization also creates a principal agent problem that is unique to DAOs, making DAO security significantly different from securing web2 entities, or centralized blockchain protocols. While decentralization distributes governance power, it can also diffuse responsibility. This can create “no one’s job” scenarios, where critical tasks—like compliance, incident response, or code reviews—are neglected because no single party feels a mandate to act.

Similarly, due to the bootstrapped nature of the DAO ecosystem, formalized definitions do not exist for most relationships between a DAO and external entities. Add to this the still-early nature of regulation and compliance of DAOs - the usual forcing functions that dictate how vendors, service provider policies, and other key entities are to be managed, is largely non-existent. This can sometimes have a direct effect on security as in the case of DAOs some of these entities may hold keys to treasury smart contracts, or work on critical software upgrades.

This initiative aims to define controls unique to DAOs to address these systemic risks that are often overlooked. Below, we provide a short overview of common threats and vulnerabilities.

Common Threats & Vulnerabilities

This section highlights some of the most critical vulnerabilities faced by DAOs, setting a foundation for the controls outlined in DAOIP-8.

Governance Attacks

Governance attacks primarily relate to proposals with a malicious intent infiltrating a critical stage of the governance process, typically the voting stage. This can happen by accumulating governance tokens (via legitimate acquisition or flash-loans), slipping in a malicious proposal at the last minute or attaching a malicious detail to an otherwise safe proposal, oftentimes leveraging low voter turnout to push these harmful proposals through the governance process. This may lead to treasury drain, sabotage protocol upgrades and cause unrest within the DAO.

Lack of concentrated voting power, high voter turnout and high-quality governance participants, can make governance attacks impractical, and/or exponentially more expensive. Sub-DAOs and or working groups can provide meaningful guardrails through specific isolation mechanisms for governance. While we have not recommended these as explicit security measures, DAOs are recommended to invest resources into a stronger *social build*.

Proposal Safety:

Proposal safety refers to ensuring that proposals, especially ones that introduce new code/components to the DAO, do not proceed to voting with insufficient testing, simulation, or reviews as this may allow subtle, malicious logic to slip through. Inadequate audits, rushed deployments, and insufficient peer review of on-chain code can introduce vulnerabilities. Even subtle bugs in upgrade logic, governance modules, or treasury contracts can become catastrophic if not caught early. This may cause unintended smart contract behavior, drain assets, or alter critical parameters in a way that disadvantages the broader community.

Slow, Uncoordinated, and Unplanned Incident Response and Vulnerability Management:

Without a well-defined emergency management plan, DAOs will be slow to respond to security incidents. Delayed reactions increase damage, whether it's a compromised DNS zone, OWASP common vulnerabilities, or a malicious proposal that slipped through.

Additionally due to the diffuse nature of DAO structures, there is often no agreed upon vulnerability management plan (VMP). Vulnerability management entails the evaluation, risk assessment and remediation of security weaknesses within technical assets, such as servers or applications. This is a proactive as well as retrospective process that requires coordination

between stakeholders and technical teams, creating a feedback loop of constant improvement. This would include processes such as dependency management and vulnerability scanning within codebases, monitoring of existing deployed artifacts, and agreed upon remediation timelines based on the severity of the discovered vulnerability.

It is important to to premeditate possible attack surfaces, and have plans with established responsibilities and a chain of command in the face of an emergency. These incident and vulnerability response plans should be wargammed at consistent intervals to ensure that participants are aware of the process and are able to identify any potential weaknesses or oversights that could decrease the efficacy of such contingencies.

Management of External Entities:

Note that every entity other than the DAO is in essence an external entity to the DAO. For day to day operations, DAOs often rely on a variety of external services (e.g., SaaS tools, off-chain oracles, auditing firms, dev shops) that may or may not be aligned with the DAO's security posture. The misalignment becomes more risky if some of these entities hold privileged positions within operations, including being multisig signers, or code contributors. While it will practically be difficult for token holders of a DAO to verify and vet external entities and how they follow these policies, these can still be used as best practices.

The same risk carries over when discussing technical asset ownership and management by key entities that may often be conflated as the DAO. An example of this would be the founding company having full responsibility for the management and operation of DNS names, front ends, core application code, gateways, and other supporting infrastructure. In such a scenario, there is little oversight or applicable governance avenues for stakeholders to in any way influence or otherwise encourage better security practices due to the lack of transparency and ownership roles. This creates a unique challenge, in such that the DAO itself actually has little to no governance power beyond that of the purse. While the power of the purse is indeed formidable, it is not sufficient in and of itself as a means of exercising administrative controls within the context of technical asset governance and ownership, particularly when a founding company is involved in core operations.

Lack of Security Training and Awareness for Delegates and Key Entities:

"Wrench attacks", or physical coercion or intimidation of keyholders is a real threat. Multiple crypto founders have been on the unfortunate side of these attacks, especially at conferences. Without proper guidelines and training, delegates, multisig signers, and core team members may inadvertently expose private keys, laptops, or other sensitive resources. DAOs should define mandatory policies to combat these attacks, and if resources permit, provide training material or sessions.

Several other attack surfaces, and common vulnerabilities exist within DAOs. There are data transparency gaps (especially around privileged roles, or incomplete listing of DAO assets, which can lead to confusion, and difficulty in pinpointing accountability); regulatory uncertainty (which may lead to regulatory penalties and reputational damages to participating entities, which may deter aligned entities from securing the DAO by participating in governance); community management risks (which can enable an attacker to spread misinformation or scam community members), and infrastructure vulnerabilities (off-chain infrastructure like forums, websites, or GitHub repositories can be compromised even if the on-chain code is secure).

DAOIP-8, detailed in the section below, will specify controls to combat these vulnerabilities.

DAOIP-8: Recommended controls for DAOs

Goal

DAOIP-8 aims to establish a minimum viable security standard among DAOs, such that all DAOs, irrespective of their scale or governance design, have an easily accessible set of controls to follow as standard practice when it comes to security. The specification in its current form considers:

- Data transparency
- Decentralized ownership
- Proposal safety
- Management of external entities
- Defense against governance attacks
- Physical security for key entities
- Community management best practices
- Compliance
- Code security
- Key management
- Subdomain versioning

It also benefits from a long list of controls in the background that did not make it to the final specification. While the absence of some of these controls, for example, a physical security policy for delegates, can lead to a critical security incident, others, say data transparency, may not have an immediate effect. Even so, every control defined in DAOIP-8 can have second-order effects. For example, low data transparency may lead to the loss of governance contributors, which reduces voter turnout and makes a governance takeover less costly. Hence, all DAOs are recommended to make their best effort to follow all controls outlined in DAOIP-8.

DAOIP-8 also intends to help DAOs establish the basic foundations of a Technical Governance Framework. The intention is to tackle the dilemma of technical governance as it relates to DAOs and their usage of services and technologies which are either directly or indirectly related to the DAO's operations, for example, hosted code repositories, cloud services, and other third-party providers. These external dependencies introduce novel complexities without clear boundaries relating to technical asset ownership and management. In addition to more traditional Web2 assets, DAOs also need to take on-chain assets into account when considering their security posture by defining and implementing specific controls around code security, vulnerability management, incident response, auditing, etc.

This guide encourages DAOs to ask the question: "If we can successfully govern a treasury, why can we not also govern our own technical footprint, operations, and security posture?" This resource aims to provide a starting point for DAOs to begin to answer this question.

While complete decentralization is the ultimate goal, it is important to recognize that the DAO ecosystem is still in its infancy and explicitly relies upon a myriad of centralized infrastructures and services in order to operate. These aforementioned dependencies are not typically taken into consideration when discussing DAO governance and thus present unique challenges to DAOs in terms of security and operational risks.

Note that DAOIP-8 is a work in progress, and will evolve over time. As the industry matures, its minimum viable security standard will become more stringent. Hence, DAOIP-8 is expected to have more controls and narrower recommendations in the future. As it stands, several sections (for example, vendor management policy, or incident response) need to be polished to fit the design of your DAO. This guide is in no way exhaustive and does not explicitly focus on prescriptive implementation details, but rather defines and describes core precepts which can be further expounded upon by contributors and stakeholders.

Note that DAOIP-8 refrains from addressing common cybersecurity / software development / blockchain development security issues, as these are covered by Frameworks by SEAL in great detail. DAOIP-8 will instead focus on very DAO-specific vulnerabilities.

Categories of Controls

Controls are categorized into:

- **[MANDATORY]**: includes measures that are critical to ensuring DAO security.
- **[RECOMMENDED]**: includes measures that may not have an immediate effect, but can have second-order security effects.

We recommend following both categories of controls to ensure maximum security.

Note that controls below are split into two sections. The first section is applicable for all DAOs. The second section is for *protocol DAOs*, i.e., DAOs that control an on-chain protocol through governance. All DAOs, whether or not they are a *protocol DAO*, are advised to consider the controls detailed in the first section.

DAO Controls

1. Data Transparency

a. **[MANDATORY]** The DAO should publish an up to date resource, outlining the steps, scope and stakeholders involved in governance.

Data transparency contributes to improving DAO security by increasing the accountability of existing participants and making it easier for new participants to join the DAO. Inaccessible information can cause insider groups to form. This is disadvantageous as *elitist* groups within a DAO may enjoy higher trust than others, causing their proposals to go through less scrutiny or lead to the creation of unchecked single points of failure within the DAO.

By clearly defining the governance process, its scope, and entities that are responsible for in various stages, the DAO becomes conscious of its operational legos. This also makes it easy for DAO participants to add additional safeguards or make amendments to the existing governance process to maximize security.

Hence, this control finds a resource that outlines the steps, scope and stakeholders involved in governance as MANDATORY / CRITICAL. The resource should ideally include the following at the very least:

- Governance process, including timelines, mandatory steps such as temp checks, signalling, voting and execution.
- Operational details such as type of voting (ranked choice, single choice, first past the post, etc), quorum, duration, governance cycles, etc.
- A list of privileged roles including information pertaining to the powers delegated to said role, the addresses associated with each role, and the process of election and management of the said roles.

In order to ensure that such a resource is up to date, DAOIP-8 recognises the advantage of having a predefined entity(s) responsible for the resource's upkeep. Being able to accept feedback and commentary from the wider community can make updates easier, and timely.

b. **[RECOMMENDED]** The DAO should maintain a repository of all DAO-related artifacts.

The list of DAO-related artefacts stretches well beyond the governance-focused resource mentioned above. DAOs, even in the smaller scale, produce a large number of artefacts including transparency reports, financial reporting, protocol performance reports, outputs from various working groups, data on initiatives funded by the DAO, notes from substructures (committees, councils, etc.), and more.

Storage, and easy access to as much information as possible will lead toward maximum accountability within the DAO. Having historical data handy will also make post mortems and security process improvements easy.

To address this, DAOIP-8 RECOMMENDS DAOs to maintain a repository of all related artefacts Standards such as EIP-4824 can be used to facilitate the storage, management, and consumption of this data.

2. Ownership of Assets

a. **[MANDATORY]** The DAO should make public a list of all assets it owns and controls. The list could include crypto tokens, ENS names and other naming services, dApps, frontends, physical assets, etc.

It is important for DAO participants to understand what the DAO owns before it can be governed effectively. Assets owned by a DAO may include smart contracts that are part of a protocol owned and governed by the DAO; treasuries where the DAO's assets are stored; loaned, invested or stored assets presently in smart contracts not controlled by the DAO; ENS names; frontends of applications and community channels such as website and discussion forums; physical assets; and more.

Depending on the asset, its present control or management may reside with an external entity, and the entity may make decisions on behalf of the DAO. Depending on the size of the DAO, the number of such assets, the number of managers, and the number of dependencies increases. If there isn't a strict culture of publicly documenting a DAO's assets, along with its mode of management, and operational rules (including scope of management, and date when a new manager needs to be chosen if any), it will become a gargantuan task later on.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to maintain a public list of all assets owned by the DAO, along with necessary details on their management.

3. Self defense, incident response, auditing, and vulnerability management

Over the lifecycle of a DAO, there may be multiple security incidents and events which pose a risk to the core operations of a DAO or its technical assets. It is imperative to have a course of action or otherwise defensive capability for responding to security incidents. This includes things such as CVE remediation, DNS hijacking/infrastructure compromise, KPI definitions for security event monitoring and response. A template for inspiration is available here (not

Web3/DAO specific). While there are many overlapping security considerations with Web2 practices, it is important to take DAO specific concerns into account. Additionally, it is necessary to also consider proactive controls for things such as MFA requirements, IAM best practices and regular reviews/audits of permissions for developers or technical contributors.

The intention here is to prompt the creation of a plan - no critical details need to be public. As decentralization may sometimes make it difficult for the DAO to “trust”, or fund a security consultant’s emergency management plan that cannot not be inspected by all voters, it may need to delegate this responsibility to a trusted third party like the core team, Foundation, or a high-context working group.

a. **[MANDATORY]** The DAO must publish a self-defense and emergency management plan.

DAOs can greatly reduce the mean time to respond (MTTR) by preemptively creating various incident and emergency response playbooks in order to better react to malicious or adversarial events. In addition to providing step by step remediation strategies, self-defense and incident response templates provoke a thorough risk-assessment of various key systems and operational security risks. This has the added side effect of better informing stakeholders of potential blindspots or weaknesses, leading to more robust technical and administrative outcomes through iterative improvement efforts.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to have a self-defence and emergency management plan. Note that as mentioned above, no critical detail of the plan needs to be public.

b. **[RECOMMENDED]** The DAO should publish a vulnerability management plan. Sample template (not Web3/DAO specific).

Software vulnerabilities exist within a multitude of systems and applications, often going unnoticed until they have already been exploited or have introduced specific defects. By employing various dependency management analysis tools and creating a well defined internal standard for identifying, tracking, and remediating vulnerable packages, DAOs can greatly reduce attack surface and the likelihood of triggering a security incident. A vulnerability management plan includes automated testing suites and their usage, as well as well defined severity categories and their respective remediation timelines. For example, a DAO may want to ensure that any CVE with a severity of 7 or higher is remediated within 48 hours. Early detection and inventories of deployed applications are necessary for rapid response.

To address this, DAOIP-8 RECOMMENDS DAOs to publish a vulnerability management plan. To set expectations, it may define expected timelines by when fixes, post-mortems and or any other detail is published. As above, DAOIP-8 does not expect any critical detail of this plan to be public.

4. Vendor/service provider management Policy

a. **[MANDATORY]** The DAO should publish a list of vendors/service providers it relies upon.

Given the opaque nature of DAO composition and the relationships between founding companies, foundations and the DAO itself, it is imperative to track and manage vendor and service provider dependencies. Similarly to how the governance process benefits from transparency and broad participation, vendor and service provider relationships can likewise benefit from a similar scheme.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to have a public list of vendors that the DAO relies on. This data set can be extended to include yearly cost, outputs, impact over the years, and other details so that it may also help token holders assess vendors and service providers more effectively through governance.

b. **[RECOMMENDED]** The DAO should publish a vendor management policy. Inspiration here.

Vendors include all 3rd party service providers that provide a good or service to the DAO, including software services that are not paid by the DAO, but used for operations, governance or other avenues. Per the security alliance framework recommendations on vendor selection, DAOs should evaluate and select relevant vendors based on areas of expertise and security posture. A set of vendor security and operational requirements streamline the DAOs vendor selection process and provide a baseline of criteria which can continuously be expounded upon as the needs of the DAO evolve over time.

To address this, DAOIP-8 RECOMMENDS DAOs to publish a vendor management policy, specifying expectations when it comes to the vendor's security posture.

5. Proposal safety

a. **[RECOMMENDED]** It is recommended to:

1. Use a timelock before upgrading protocols that hold assets.
2. Simulate proposals before executing them.
3. Perform automated checks on proposals for common attacks.
4. Quorum threshold definitions for core governance changes.
5. Auditing and review of governance mutating transactions by qualified contributors to ensure expected outcomes match voter preferences.

DAO proposals can execute arbitrary code. It's important that anyone approving proposals or affected by them understand what the code will do. Traditional software development has a lot of best practices that also apply here: invariant testing, code review, and test suites all have analogies for DAO proposals. Taken together, these proposed safety recommendations aim to give stakeholders enough time and information to judge whether a change is safe and will work as intended. Importantly, these checks need to be visible to everyone. Someone making a proposal should have the tools to understand that it will work as they intend, AND people who are approving that proposal should have the same tools to verify that it will work as described.

In DAOs where governance is offchain signalling and execution is a trusted setup like a multisig (for example, Snapshot + Safe), the responsibility to evaluate proposal safety often falls on the multi-sig signers. In cases where the signers are non-technical (which has been the case in several DAOs DAOIP-8 authors looked at), this presents a critical attack surface.

To address this, DAOIP-8 RECOMMENDS DAOs to employ the series of tests mentioned above to ensure proposal safety. It is ideal to have these tests as standard practice, and in cases where the proposal execution happens outside of governance, independent of the entities responsible for final execution.

6. Physical security training

a. **[MANDATORY]** The DAO should publish a physical security recommendation and provide training to combat wrench attacks.

The DAO is recommended to focus on educational content that describes measures to be taken by key delegates, multisig signers, members of the foundation, and other important stakeholders to ensure security while traveling to conferences and other events. Inspiration taken from here. Key recommendations could include the following:

1. Hardware wallet management.
2. Laptop security.
3. Usage of public WiFi.
4. Social engineering defense.
5. AirBnB/hotel security.

Apart from wrench attacks, DAO stakeholders, voters, delegates, etc. are also at risk of non-targeted attacks. Incidents such as a stolen laptop, malicious WiFi snooping at a cafe, or even stolen smartphones can pose an existential risk to the organization as a whole. By adopting a set of best practices and providing recurring annual training, DAOs can greatly minimize the damage that can be inflicted by a single member becoming compromised. Part of

this training should also be integrated into the DAOs key management efforts, particularly in regards to hardware wallet physical security for participants.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to provide physical security training for key entities. Similar to the Vendor Management Policy recommended above, it may be good practice to also define minimum expectations from all individuals responsible for various roles within the DAO. While enforcing is difficult, the DAO can mandate all potential candidates while elections happen, to attest to following the outlined recommendations.

7. Community management

a. **[MANDATORY]** The DAO should follow secure community management processes, to secure community accounts on Twitter, Discord, Telegram, and other applications. Template (recommendations by the Security Alliance) here.

Securing social media accounts is a critical component in not only protecting the DAO itself (reputationally, operationally) but also protecting its users and governance participants. This section is intended to be a companion to the incident response and emergency management recommendations. For example, a defined process for responding to and remediating a compromised social media account. By mandating secure best practices such as multi-factor authentication, restricted chat roles, only using vetted 3rd party integrations for platforms like Discord, etc., risk of compromise can be greatly diminished. Additionally, phishing awareness and training is paramount to combat social media account compromise.

In many cases, platforms utilized by the DAO, for example, a forum that hosts governance proposal discussion, may not be owned or controlled by the DAO. This is partly because it is inconvenient and difficult to control offchain platforms through governance. Regardless of ownership, it is important to ensure that these platforms are secure, and that there are dedicated personnel to prevent spam, and maintain security standards.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to follow secure community management processes. While not critical, DAOs are also advised to consider archiving important information, like discussions, particularly those that contributed to decision making, in case platforms get taken down, or the entity that currently owns it runs into unforeseen circumstances.

8. Compliance

a. **[MANDATORY]** The DAO must keep a record of its compliance efforts, including policies, procedures, and audit results. It should make its best efforts to comply with the regulatory frameworks applicable to its areas of incorporation.

While the regulatory landscape is always shifting, DAOs are by no means exempt from complying with regulatory regimes, depending upon the types of services offered and the geographic location of their users. For example, GDPR applies to all EU citizens, regardless of where the hosted service resides. This can introduce additional liabilities on founding companies and service providers. As a result, it is critical that applicable regulations are complied with. Further complicating matters is that DAOs can often put their own stakeholders at risk as in the case of OokiDAO, by failing to adhere to regulatory and administrative requirements. A full list of recommendations and applicable compliance frameworks can be found here.

Note that regardless of DAO jurisdiction or its regulatory standing, assets such as websites, frontends, forums, etc. can be subject to various data privacy laws. It is recommended to make a concerted effort to adhere to regulatory obligations to prevent future burdens or headaches such as “DSARs” and “Right to be forgotten” requests.

To address this, DAOIP-8 identifies that it is MANDATORY / CRITICAL to make its best efforts to comply with applicable regulatory frameworks, and keep a record of its compliance efforts .

Protocol DAO Controls

The following set of controls are authored for protocol DAOs, i.e DAOs that control an on-chain protocol. All DAOs, irrespective of whether they are a protocol DAO, are advised to follow the controls detailed in the previous section.

1. Data transparency

a. **[MANDATORY]** Code that the DAO governs should be available somewhere publicly.

A protocol DAO governs protocol smart contracts. The DAO might have authority to change parameters or even the authority to fully upgrade or replace the protocol smart contracts. The source code of the protocol should be publicly available, so that DAO stakeholders can see what

governance is authorized to do and evaluate proposals to change the protocol. Note that code governed by the DAO need not specifically be open-source.

b. **[RECOMMENDED]** There should be publicly accessible documentation on the protocol components, along with flow diagrams, design choices, dependencies and a record of critical privileged roles. All DAO related smart contracts including protocol, token, governance and treasury related smart contracts, should be documented, as well as verified on block explorers (if the provision exists).

Additional documentation makes it easier for stakeholders to understand the system and its governance. Block explorers make smart contracts much more accessible. Publishing smart contract code on block explorers makes it easier and safer for stakeholders to inspect and interact with the protocol and governance.

2. Code security

a. **[MANDATORY]** Protocol code MUST be audited, and a comprehensive report detailing vulnerabilities and suggested improvements should be publicly available for the latest protocol version.

Code auditing is a pillar of transparency when designing a protocol or implementing core upgrades. Similar to the benefits that Open Source Software (OSS) provide, code audits and vulnerability transparency provide a crowd sourced means to properly assess risks and identify potential exploits before they can take place. Auditing is a multi-faceted endeavor, requiring teams to employ well known evaluation tools early in the development process, and engaging high-quality security firms that possess the expertise necessary to properly review and test code. Code security is also an integrated component in vulnerability management, and as such there will be considerable overlap between these two areas of concern. For example, front end code may require less stringent auditing and code security efforts as opposed to a new on-chain protocol architecture as evaluated by risk scoring within a vulnerability management plan.

The following Security Framework recommendations should be considered:

- Security testing
- Secure software development
- External security reviews

3. Bug Bounty

a. **[RECOMMENDED]** Bug bounty program. The DAO is recommended to operate a bug bounty program.

A bug bounty program (BPP) provides a powerful incentive for threat hunting professionals to contribute to the security posture of a DAO. However, careful consideration should be taken into account when designing and implementing a robust program. For example, compensation must be carefully balanced against risk thresholds, a process for reviewing submissions and filtering out false positives must be devised, and careful consideration of in and out of scope assets.

b. **[RECOMMENDED]** The DAO is recommended to execute a white hat Safe Harbor agreement.

Safe Harbor Agreement empowers whitehats to act immediately during an exploit, offering a swift and structured recovery process without needing to pause the protocol. This agreement applies only to critical situations where responsible disclosure procedures would not save funds due to the urgency of the exploit, and it is not intended for routine security testing or vulnerability reporting. Under the terms of the Safe Harbor, whitehats are required to return all rescued assets to a pre-designated recovery address controlled by the protocol within 72 hours of recovering them. This ensures that recovered funds are quickly secured, preventing delay or potential loss. Whitehats are rewarded with a percentage of the recovered assets, up to a predefined cap, for their successful interventions. For more details, refer to this Safe Harbor adoption proposal on Uniswap.

To adopt Safe Harbor, DAOs need to register an agreement in the Safe Harbor Registry. This ensures transparency and immutability, and is fairly easy as it does not require a legal entity like the core team or Foundation to draw up a traditional agreement on behalf of the DAO.

4. Key management

a. **[MANDATORY]** Isolated and purpose specific hardware wallets should be used by multisig key holders and delegates of a DAO. SAFEs or other account abstraction implementations should also be deployed in all operational areas.

Key management is perhaps one of the most critical aspects of a DAOs security posture. Not only is proper key management essential to maintaining the integrity of DAO operations, it is also crucial for protecting its stakeholders and governance participants at an individual level. While there is no one-size fits all approach, there are several best practices that should be employed where applicable, such as:

- Advise stakeholders and participants not to publicly brag or advertise specific token holdings or privileges which might be associated with a particular private key.
- Avoid custodial and software wallets wherever possible.
- Utilize physical security controls such as a floor mounted safe for storing private key material such as seed phrase backups. Additionally, hardware wallets should also be physically secured when traveling or away from your place of residence or work.
- Multisig SAFEs should be used with reasonable threshold signature requirements for DAO governance or asset management.

Key management implementations and practices should be regularly reviewed by qualified participants and careful consideration should be taken into account when designing new governance primitives or product features.

5. Operational security policy for key entities

a. **[RECOMMENDED]** The DAO should require entities, including its foundation, founding company, or service providers with a long-term service agreement, to publish and adhere to an operational security policy.

A detailed template of various components that can possibly go into the security policy is detailed here. As above, the intention is to prompt operational security for all stakeholders and not to publish critical information publicly.

The policies can be as strict and prescriptive as the DAO wishes. For example, the DAO can put forth requirements around internal policies for granting and revoking permissions and role memberships; vulnerability management, data classification, privacy policy; incident reporting; disaster recovery; log retention and other angles.

6. Subdomains for contracts and dApps

a. **[RECOMMENDED]** It is recommended to provide all contracts with ENS names. dApps should enforce ENS subdomain versioning schemas (v1, v2, etc) as mentioned here.

Using an on-chain naming service provides several benefits to DAOs, namely it can assign human readable names to smart contracts and dApps as well as serve as a hierarchical management structure for organizing sub-DAOs or working groups with unique roles and permissions. By leveraging subnames, it therefore becomes possible to implement immutable versioning by assigning the semantic versioning schema to other on-chain artifacts. For the

purposes of this particular recommendation, we chose the Ethereum Name Service specifically because of its robust integrations and near universal client support. While specifically using ENS is not required, it is recommended, although any other sufficiently developed on-chain naming service can be deployed.

This is a best practice for future management of organizational units when delegating responsibilities to working groups or other sub-organizations within the DAO. Additionally this provision helps ensure that versioning remains immutable and easy to understand.

Addressing Community Feedback

Given the importance of the topic, DAOIP-8 has garnered constructive feedback from numerous entities in a short time (a full list of collaborators can be found in the *Acknowledgements* section of this report). Below, we address some of the key community feedback and outline how DAOIP-8 can be refined moving forward. Note that the responses below are perspectives of the authors of this report, and may divert from

1. Decentralization as the Foundational Principle / Control:

Multiple reviewers noted that DAOIP-8 would benefit from explicitly framing decentralization as the guiding principle and as one of the key controls. This sentiment makes sense, especially since the “D” in DAO stands for decentralization. In fact, we went back and forth several times on how to include decentralization in DAOIP-8.

The reason why optimizing for decentralization does not appear explicitly in DAOIP-8 is because we concluded that this specification should operate as the foundation for enabling decentralization, rather than mentioning it as ‘just another control’. In that sense, DAOIP-8 is the complete set of legos that makes decentralization work from a security perspective. All 14 controls, whether mandatory or recommended, ultimately align with the broader aim of enhancing decentralization. Improving data transparency, fortifying relationships with external entities, documenting assets, and prioritizing proposal safety are all preparatory steps required for DAOs to effectively decentralize.

2. Prescriptive Measures vs. Recommended Measures:

Many of the terms used in DAOIP-8 are taken directly from IETF standards. Consequently, the key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document should be interpreted as described in RFC 2119.

DAOs often move slowly when adopting standards, but the cost of postponing security considerations can be catastrophic. We’ve therefore introduced some prescriptive language to serve as a forcing function, pushing DAOs to address critical security measures sooner rather than later. While a DAO may initially choose to ignore most of DAOIP-8, given enough time and stakeholders committed to building a secure DAO, it’s likely they will ultimately consider and implement many, if not all, of the controls defined in DAOIP-8.

3. Presence of a *Ratings Body*:

As DAOs vary widely in maturity, scale, and structure, some controls may not be immediately feasible or relevant for newer DAOs. For more established organizations—particularly those

governing critical on-chain protocols—it's important to understand why certain recommended controls aren't being followed.

An industry-wide forcing function, in the form of an unbiased and credibly neutral ratings body, could help address this. Similar to how L2Beat analyzes layer-2 networks, such an entity could issue a "score" for each DAO based on its performance against DAOIP-8. We will consider adding optional metrics, benchmarks, or tools to enable this ratings body to evaluate DAO compliance and progress effectively.

4. Tangibility of Controls:

While discussing DAOIP-8 with multiple large DAOs, including LIDO, Arbitrum, Optimism, and others, we understood that some of the defined controls leave plenty of room for interpretation. For instance, an active delegate may perceive the DAO's data transparency on governance processes, assets, privileged roles, and protocol architecture as high, whereas a newer delegate might have a vastly different experience.

The same applies to other controls as well, where DAOIP-8 prompts the creation of an artifact, but it is open to interpretation how 'adequate' that artifact is. Without the presence of a centralized ratings system (which doesn't exist in DAOIP-8 for now), it is difficult to objectively measure how well a DAO has adopted these controls.

Even then, we are confident that a DAO can satisfactorily adopt all controls in DAOIP-8 if each control is presented for public discourse and contribution, rather than assuming that the control is already adequately met.

Conclusion

A key observation while authoring DAOIP-8 was how a lot of trust in DAOs is still placed in the goodwill of different entities. While we as an ecosystem advocate for 'trustlessness,' it does not exist in DAOs outside of the governance smart contract <> treasury {<> protocol} junctions, which are often the final step in the decision-making process. Given how customizable DAO tooling is getting, complete 'trustlessness' might be achievable by overengineering DAOs (and possibly making them less efficient as organizational structures). But, we do not think it should be something we strive for in itself. However, what is surprising—and rather worrying—is the lack of clear expectations.

While social norms may work for some time, all it takes is one core team member, a large delegate, a security consultant, or a few signers deviating from expected behavior to vaporize billions of dollars and erode trust. We believe that DAOs have reached a threshold of professionalism where it is no longer acceptable to neglect vendor management, internal safety policies for key entities, data transparency, vulnerability management, or the other controls specified above.

While this report and the accompanying DAOIP represent a necessary and pertinent step toward improving the overall security posture of the DAO ecosystem, it is still an embryonic process. Continuous, iterative improvements are necessary, alongside diverse collaboration with existing DAOs to better understand and address potential weaknesses. The aim of this DAOIP is to be informative and descriptive, not necessarily prescriptive. Given the diverse nature of the DAO landscape, the controls specified in DAOIP-8 serve as a starting point that can be adapted to the specific needs of individual DAOs.

The authors of this work and DAOstar are excited about the opportunity to present DAOIP-8 to DAOs across the ecosystem, collect constructive feedback, and modify the specification as necessary to fit various DAOs. As this is open-source work, we invite contributions from everyone—whether you are a security professional, DAO voter, significant delegate, or governance enthusiast. DAOstar's Github and Slack are the two best channels for joining the discussion. You may also join this Telegram group if that is more convenient.

Acknowledgements

This work would not have been possible without the invaluable support and feedback from numerous individuals and organizations. The project officially began over eight months ago, and throughout this time, many contributors have played a significant role in shaping the current version of DAOIP-8. We are deeply grateful for their insights and efforts.

The following individuals and organizations deserve special recognition. Kindly accept our apologies if your name has been inadvertently omitted:

Fredrik Svantes, Riely Chen (Ethereum Foundation)
Joshua Tan, Fernando Mendes (DAOstar / Metagov)
Eugene Levanthal (Scroll / Metagov)
Michael Lewellen (OpenZeppelin)
Mehdi Zerouali (Sigma Prime)
Matta, Sebastian (The Red Guild)
Michael Morami, Mooly Sagiv (Certora)
Eric (LIDO)
Krzysztof Urbanski (L2Beat)
Raam Chandrasekharan (Arbitrum Foundation)
Nikhil Suri (Wormhole Foundation)
Jan Brezina (How to DAO)
Spencer Graham (Hats Protocol)

DAOIP-8 was presented at multiple events during ETH CC Brussels 2024 and Devcon Bangkok 2024, where several DAO contributors provided constructive feedback. We are grateful to the wonderful sponsors of these events, as well as their participants, for making the sessions productive. Additionally, several DAO tooling providers, who are members of the DAOstar Roundtable, have offered valuable feedback, for which we are deeply grateful.