Continuous Integration / Continuous Deployment	Vorbedingung	Get-Request	Response	Bedingung	Überprüfung möglich ja/nein	Anmerkung	Dokumentation

1. Workflows Should Not Be Allowed To Approve Pull Requests	n/a	GET /orgs/{org}/actions/permissions/workflow	`{`
			`  "default_workflow_permissions": "read",`
			`  "can_approve_pull_request_reviews": false`
			`}`
				`"can_approve_pull_request_reviews" == false`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-default-workflow-permissions-for-an-organization

2. GitHub Actions Should Be Restricted To Selected Repositories	n/a	GET /orgs/{org}/actions/permissions	`{`
			`  "enabled_repositories": "selected",`
			`  "allowed_actions": "all"`
			`}`
				`"enabled_repositories" == "selected"`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-github-actions-permissions-for-an-organization

3. GitHub Actions Should Be Limited To Verified or Explicitly Trusted Actions	n/a	GET /orgs/{org}/actions/permissions	`{`
			`  "enabled_repositories": "all",`
			`  "allowed_actions": "selected",`
			`  "selected_actions_url":`
			`"https://api.github.com/organizations/42/actions/permissions/selected-actions"`
			`}`
				`"allowed_actions" == "selected"`	j	Zunächst gilt es zu prüfen, ob "allowed_actions" = "selected" gilt.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-github-actions-permissions-for-an-organization

	"allowed_actions" = "selected",	GET /orgs/{org}/actions/permissions/selected-actions	`{`
			`  "github_owned_allowed": true,`
			`  "patterns_allowed": [],`
			`  "verified_allowed": true`
			`}`
				`"github_owned_allowed" == true && "verified_allowed" == true`	j	Wenn vorheriger Request allowed_actions = "selected" ausgibt, gilt es mit diesem Get-Request zu überprüfen, ob verifizierte oder explizit benannten GitHub-Actions vertraut wird.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-allowed-actions-and-reusable-workflows-for-an-organization

4. Default Workflow Token Permission Should Be Read Only	n/a	GET /orgs/{org}/actions/permissions/workflow	`{`
			`  "default_workflow_permissions": "read",`
			`  "can_approve_pull_request_reviews": false`
			`}`
				`"default_workflow_permissions" == "read"`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-default-workflow-permissions-for-an-organization

	n/a	GET /repos/{owner}/{repo}/actions/permissions/workflow	`{`
			`  "default_workflow_permissions": "read",`
			`  "can_approve_pull_request_reviews": true`
			`}`
				`"default_workflow_permissions" == "read"`	j	Eine Überprüfung ist darüber hinaus auch auf Repository-Ebene zu vollziehen, da diese Einstellung auf durch Repositories überschrieben werden kann.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-default-workflow-permissions-for-a-repository

5. Runner Group Should Be Limited to Private Repositories	n/a	GET /orgs/{org}/actions/runner-groups	`{`
			`  "total_count": 1,`
			`  "runner_groups": [`
			`    {`
			`      "id": 1,`
			`      "name": "Default",`
			`      "visibility": "all",`
			`      "default": true,`
			`      "runners_url": "https://api.github.com/orgs/octo-org/actions/runner_groups/1/runners",`
			`      "inherited": false,`
			`      "allows_public_repositories": false,`
			`      "restricted_to_workflows": false,`
			`      "selected_workflows": [],`
			`      "workflow_restrictions_read_only": false`
			`    },`
			`  ]`
			`}`
				`"allows_public_repositories" == false`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/self-hosted-runner-groups?apiVersion=2022-11-28#list-self-hosted-runner-groups-for-an-organization

6. Runner Group Should Be Limited to Selected Repositories	n/a	GET /orgs/{org}/actions/runner-groups	`{`
			`  "total_count": 1,`
			`  "runner_groups": [`
			`    {`
			`      "id": 1,`
			`      "name": "octo-runner-group",`
			`      "visibility": "selected",`
			`      "default": false,`
			`      "selected_repositories_url": "https://api.github.com/orgs/octo-org/actions/runner_groups/2/repositories",`
			`      "runners_url": "https://api.github.com/orgs/octo-org/actions/runner_groups/2/runners",`
			`      "inherited": true,`
			`      "allows_public_repositories": true,`
			`      "restricted_to_workflows": true,`
			`      "selected_workflows": [`
			`        "octo-org/octo-repo/.github/workflows/deploy.yaml@refs/heads/main"`
			`      ],`
			`      "workflow_restrictions_read_only": true`
			`    },`
			`  ]`
			`}`
				`"visibility" == "selected" && "selected_repositories_url != ""`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/self-hosted-runner-groups?apiVersion=2022-11-28#list-self-hosted-runner-groups-for-an-organization

Enterprise	**Vorbedingung**	**Get-Request**	**Response**	**Bedingung**	**Überprüfung möglich ja/nein**	**Anmerkung**	
1. Two-Factor Authentication Should Be Enforced For The Enterprise	n/a	n/a	n/a	n/a	n	Diese Konfiguration Einstellung lässt sich auf Enterprise-Ebene nicht per API überprüfen. Sie kann auf Organization-Ebene überprüft werden, was in einem folgenden Control (Organizational Management - 1.) relevant sein wird.	https://docs.github.com/en/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization

Members, Access Control and Permissions	Vorbedingung	Get-Request	Response	Bedingung	Überprüfung möglich ja/nein	Anmerkung	
2. Enterprise Should Not Allow Members To Change Repository Visibility	n/a	GET /orgs/{org}/repos?type=all	`[ { "id": 1296269, "node_id": "MDEwOlJlcG9zaXRvcnkxMjk2MjY5", "name": "Hello-World", "full_name": "octocat/Hello-World", [...] "visibility": "private", [...] } ]`	"visibility" == "private"	j	Eine Überprüfung ist je Repository für jede Organization möglich.	https://docs.github.com/en/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization
3. Enterprise Should Not Allow Members To Create public Repositories	n/a	n/a	n/a	n/a	n	Diese Konfiguration lässt sich auf Enterprise-Ebene nicht per API überprüfen. Sie kann auf Organization-Ebene überprüft werden, was in einem folgenden Control (Organizational Management - 3.) relevant sein wird.	
4. Enterprise Should Not Allow Members To Invite Outside Collaborators	n/a	GET /repos/{owner}/{repo}/collaborators	`[{ "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", [...] } { "login": "octo", "id": 2, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", [...] }]`	n/a		Die konkrete Einstellung kann nicht geprüft werden. Eine nachträgliche Überprüfung auf Repository-Ebene ist möglich: zunächst gilt es alle Collaborators eines Repositories zu erheben.	https://docs.github.com/en/rest/collaborators/collaborators?apiVersion=2022-11-28#list-repository-collaborators
	Es existieren Collaborators innerhalb eines Repositories	GET /orgs/{org}/members/{username/login}	Status 204 / Status 404	Response == Status 204	j	Die erhobenen Collaborators werden nun iterativ gegen eine Organization geprüft. Bei der Rückgabe des Status 204 ist der angegebene Collaborator Mitglied der Organisation und nicht extern eingeladen. Bei Rückgabe des Status 404 ist der angegebene Collaborator kein Mitglied der Organisation und ein externer Collaborator	https://docs.github.com/en/rest/orgs/members?apiVersion=2022-11-28#check-organization-membership-for-a-user
5. Enterprise Should Use Single-Sign-On	n/a	n/a	n/a	n/a	n	Diese Konfiguration Einstellung lässt sich auf Enterprise-Ebene nicht per API überprüfen.	
6. Enterprise Should Not Allow Members To Fork Internal And Private Repositories	n/a	GET /orgs/{org}	`{ "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", [...] "members_can_fork_private_repositories": false, [...] }`	"members_can_fork_private_repositories" == false	j	Eine Überprüfung ist auf Organization-Ebene möglich.	https://docs.github.com/en/enterprise-cloud@latest/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization

Members, Access Control and Permissions	Vorbedingung	Get-Request	Response	Bedingung	Überprüfung möglich ja/nein	Anmerkung	
1. Organization Should Have Fewer Than Three Owners	n/a	GET /orgs/{org}/members?role=admin	`[{ "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", [...] } { "login": "octo", "id": 2, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", [...] }]`	count(response[*].login) <= 3	j	Die Rückgabe beinhaltet die Anzahl an Mitgliedern einer Organisation mit Admin-Privilegien. Die Rückgabe darf nicht mehr als drei Mitglieder mit Admin-Privilegien beinhalten.	https://docs.github.com/en/enterprise-cloud@latest/rest/orgs/members?apiVersion=2022-11-28#list-organization-members
2. Organization Admins Should Have Activity In The Last 6 Months	n/a	n/a	n/a	n/a	n	Diese Überprüfung lässt sich nicht automatisieren. Eine manuelle Prüfung ist am zielführendsten.	
3. Organization Members Should Have Activity In The Last 6 Months	n/a	n/a	n/a	n/a	n	Diese Überprüfung lässt sich nicht automatisieren. Eine manuelle Prüfung ist am zielführendsten.	

Organizational Management	Vorbedingung	Get-Request	Response	Bedingung	Überprüfung möglich ja/nein	Anmerkung	
1. Two-Factor Authentication Should Be Enforced For The Organization	n/a	GET /orgs/{org}	`{ "login": "github", "id": 1, [...] "two_factor_requirement_enabled": true, [...] }`	"two_factor_requirement_enab...	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization

	Vorbedingung	Get-Request	Response	Bedingung	Überprüfung möglich ja/nein	Anmerkung	

2. Default Member Permissions Should Be Restricted	n/a	GET /orgs/{org}	{
			  "login": "github",
			  "id": 1,
			  "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=",
			  [...]
			  "default_repository_permission": "none",
			  [...]
			  "members_can_create_public_repositories": false,
			  [...]
			}
				"default_repository_permission" == "none"	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/enterprise-cloud@latest/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization

3. Only Admins Should Be Able To Create Public Repositories	n/a	GET /orgs/{org}	{
			  "login": "github",
			  "id": 1,
			  "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=",
			  [...]
			  "default_repository_permission": "none",
			  [...]
			  "members_can_create_public_repositories": false,
			  [...]
			}
				"members_can_create_public_repositories" == false	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/enterprise-cloud@latest/rest/orgs/orgs?apiVersion=2022-11-28#get-an-organization

4. Organization Should Use Single-Sign-On	n/a	n/a	n/a	n/a	n	Diese Konfiguration Einstellung lässt sich auf Organization-Ebene nicht per API überprüfen.	

5. Webhooks Should Be Configured To Use SSL	n/a	GET /orgs/{org}/hooks	"config": {
			  "content_type": "form",
			  "insecure_ssl": "0",
			  "secret": "********",
			  "url": "https://example.org"
			},
				"insecure_ssl" == "0"	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/orgs/webhooks?apiVersion=2022-11-28#list-organization-webhooks

6. Webhooks Should Be Configured With A Secret	n/a	GET /orgs/{org}/hooks	"config": {
			  "content_type": "form",
			  "insecure_ssl": "1",
			  "secret": "******",**
			  "url": "https://example.org"
			},
				"secret" != ""		Eine Überprüfung ist möglich. Ein Secret muss gesetzt sein.	https://docs.github.com/en/rest/orgs/webhooks?apiVersion=2022-11-28#list-organization-webhooks

Repository	**Vorbedingung**	**Get-Request**	**Response**	**Bedingung**	**Überprüfung möglich ja/nein**	**Anmerkung**	
1. Repository Should Be Updated At Least Quarterly	n/a	n/a	n/a	n/a	n	Diese Überprüfung lässt sich nicht automatisieren. Eine manuelle Prüfung ist am zielführensten.	
2. Workflows Should Not Be Allowed To Approve Pull Requests	n/a	n/a	n/a	n/a	j	Dopplung mit Continuous Integration / Continuous Deployment - 1.	

3. Default Branch Should Require Code Review	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "required_pull_request_reviews": {
			    "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_pull_request_reviews",
			    "dismissal_restrictions": {
			      [...]
			      "users": [
			        {
			          "id": 1,
			          [...]
			        }
			      ],
			      "teams": [
			        {
			          "id": 1,
			          [...]
			        }
			      ],
			      "apps": [
			        {
			          "id": 1,
			          [...]
			        }
			      ]
			    },
			    "dismiss_stale_reviews": true,
			    "require_code_owner_reviews": true,
				"required_pull_request_reviews" != "" && "required_approving_review_count" >= 1	j	Eine Überprüfung ist möglich. Es muss "required_pull_request_reviews" definiert sein und "approving_review_count" muss 1 oder größer sein.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

4. Default Branch Should Require Linear History	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "required_linear_history": {
			    "enabled": true
			  }
			  [...]
			}
				"required_linear_history"."enabled" == true	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

5. Default Workflow Token Permission Should Be Set To Read Only	n/a	GET /orgs/{org}/actions/permissions/workflow	{
			  "default_workflow_permissions": "read",
			  "can_approve_pull_request_reviews": true
			}
				"default_workflow_permissions" == "read"	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/actions/permissions?apiVersion=2022-11-28#get-default-workflow-permissions-for-an-organization

6. OSSF Scorecard Score Should Be Above 7	n/a	n/a	n/a	n/a	n	Eine automatisierte Überprüfung ist nicht möglich.	
7. Default Branch Should Require Code Review By At Least Two Reviewers	n/a	n/a	n/a	n/a	j	Der Control beschreibt in der zum Zeitpunkt der Verfassung dieser Arbeit die gleiche Handlungsanweisung wie unter Repository - 3.	

8. Default Branch Should Require All Checks To Pass Before Merge	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  "required_status_checks": {
			    "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_status_checks",
			    "contexts": [
			      "continuous-integration/travis-ci"
			    ],
			    "contexts_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_status_checks/contexts",
			    "enforcement_level": "non_admins"
			  },
			  [...]
			}
				"required_status_checks" != ""	j	Eine Überprüfung ist möglich. "required_status_checks" muss definiert sein.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

9. Default Branch Should Require Branches To Be Up To Date Before Merge	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection/required_status_checks	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_status_checks",
			  "strict": true,
			  "contexts": [
			    "continuous-integration/travis-ci"
			  ],
			  "contexts_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_status_checks/contexts"
			}
				"strict" == true	j	Eine Überprüfung ist möglich	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-status-checks-protection

10. Default Branch Should Not Allow Force Pushes	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "allow_force_pushes": {
			    "enabled": false
			  },
			  "allow_deletions": {
			    "enabled": true
			  },
			  [...]
			}
				"allow_force_pushes"."enabled" == false	j	Eine Überprüfung ist möglich	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

11. Default Branch Should Be Protected	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	Error 404 / Request-Output	reponse != null	j	Eine Überprüfung ist möglich: Wenn der Request fehlschlägt (404), ist der Branch nicht geschützt. Wenn Inhalt zurück kommt, dann ist er geschützt.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

12. Default Branch Deletion Protection Should Be Enabled	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "allow_force_pushes": {
			    "enabled": true
			  },
			  "allow_deletions": {
			    "enabled": false
			  },
			  [...]
			}
				"allow_deletions"."enabled" == false	j	Eine Überprüfung ist möglich	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

13. GitHub Advanced Security – Dependency Review Should Be Enabled For A Repository	n/a	GET /repos/{owner}/{repo}/code-security-configuration	{
			  "status": "attached",
			  "configuration": {
			    "id": 1325,
			    "target_type": "organization",
			    "name": "octo-org recommended settings",
			    "description": "This is a code security configuration for octo-org",
			    "advanced_security": "enabled",
			    "dependency_graph": "enabled",
			    "dependency_graph_autosubmit_action": "enabled",
			    "dependency_graph_autosubmit_action_options": {
			      "labeled_runners": false
			    },
				"dependency_graph" == "enabled"	j	Eine Überprüfung ist möglich. Ebenfalls ist eine Überprüfung auf Organization-Ebene denkbar und möglich.	https://docs.github.com/en/rest/code-security/configurations?apiVersion=2022-11-28#get-the-code-security-configuration-associated-with-a-repository

14. Vulnerability Alerts Should Be Enabled	n/a	GET /repos/{owner}/{repo}/code-security-configuration	{
			  "status": "attached",
			  "configuration": {
			    "id": 1325,
			    "target_type": "organization",
			    "name": "octo-org recommended settings",
			    "description": "This is a code security configuration for octo-org",
			    "advanced_security": "enabled",
			    "dependency_graph": "enabled",
			    "dependency_graph_autosubmit_action": "enabled",
			    "dependency_graph_autosubmit_action_options": {
			      "labeled_runners": false
			    },
			    "dependabot_alerts": "enabled",
			  [...]
			}
				"dependabot_alerts" == "enabled"	j	Eine Überprüfung ist möglich. Ebenfalls ist eine Überprüfung auf Organization-Ebene denkbar und möglich.	https://docs.github.com/en/rest/code-security/configurations?apiVersion=2022-11-28#get-the-code-security-configuration-associated-with-a-repository

15. Forking Should Not Be Allowed for This Repository	n/a	GET /repos/{owner}/{repo}	```json { "id": 1296269, "node_id": "MDEwOlJlcG9zaXRvcnkxMjk2MjY5", "name": "Hello-World", "full_name": "octocat/Hello-World", [...] "allow_forking": false, [...] } ```	"allow_forking" == false	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/repos/repos?apiVersion=2022-11-28#get-a-repository
16. Default Branch Should Require All Conversations To Be Resolved Before Merge	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection	```json { "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection", [...] "required_conversation_resolution": { "enabled": true }, [...] } ```	"required_conversation_resolution"."enabled" == true	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection
17. Webhooks Should Be Configured With A Secret	n/a	GET /repos/{owner}/{repo}/hooks/	```json [{ "type": "Repository", "id": 12345678, "name": "web", "active": true, "events": ["push", "pull_request"], [...] }] ```			Zunächst gilt es je Repository die Hook-ID zu erheben.	https://docs.github.com/en/rest/repos/webhooks?apiVersion=2022-11-28#list-repository-webhooks
	Es müssen Hooks definiert sein.	GET /repos/{owner}/{repo}/hooks/{hook_id}/config	```json { "content_type": "json", "insecure_ssl": "0", "secret": "********", "url": "https://example.com/webhook" } ```	"secret" != ""	j	Die zuvor erhobene Hook-ID muss dann dazu genutzt werden, um zu prüfen, ob ein Secret gesetzt ist. Eine Überprüfung ist demnach möglich.	https://docs.github.com/en/rest/repos/webhooks?apiVersion=2022-11-28#get-a-webhook-configuration-for-a-repository
18. Default Branch Should Require All Commits To Be Signed	n/a	GET /repos/{owner}/{repo}/branches/{default-branch}/protection/required_signatures	```json { "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_signatures", "enabled": true } ```	"enabled" == true	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-commit-signature-protection
19. Default Branch Should Require New Code Changes After Approval To Be Re-Approved	n/a	GET /repos/{owner}/{repo}/branches/{branch}/protection	```json { "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection", [...] "required_pull_request_reviews": { [...] }, "dismiss_stale_reviews": true, "require_code_owner_reviews": true, "required_approving_review_count": 2, "require_last_push_approval": true }, [...] } ```	"dismiss_stale_reviews" == true	j	Eine Überprüfung ist möglich	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection
20. Default Branch Should Restrict Who Can Push To It	n/a	GET /repos/{owner}/{repo}/branches/{branch}/protection	```json { "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection", [...] "required_pull_request_reviews": { "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_pull_request_reviews", "dismissal_restrictions": { [...] "users": [{ "login": "octocat", [...] }], "teams": [{ "id": 1, [...] }], "apps": [{ "id": 1, [...] }] }, [...] }, ```	"users" != "" || "teams" != "" || "apps" != ""	j	Eine Überprüfung ist möglich. Es müssen Users und/oder Teams und/oder Apps definiert sein.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

21. Repository Should Have Fewer Than Three Admins	n/a	`GET /repos/{owner}/{repo}/collaborators`	<pre>[
			  {
			    "login": "octocat",
			    [...]
			    "permissions": {
			      "pull": true,
			      "triage": true,
			      "push": true,
			      "maintain": false,
			      "admin": true
			    },
			    "role_name": "write"
			  }
			  {
			    "login": "octo",
			    [...]
			    "permissions": {
			      "pull": true,
			      "triage": true,
			      "push": true,
			      "maintain": false,
			      "admin": false
			    },
			    "role_name": "write"
			  }
			]</pre>
				`count(response[*].login) <= 3`	j	Eine Überprüfung ist möglich. Es dürfen nicht mehr als drei Admins existieren ("admin" = true)	https://docs.github.com/en/rest/collaborators/collaborators?apiVersion=2022-11-28#list-repository-collaborators

22. Default Branch Should Limit Code Review to Code-Owners	n/a	`GET /repos/{owner}/{repo}/branches/{branch}/protection`	<pre>{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "required_pull_request_reviews": {
			    "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_pull_request_reviews",
			    "dismissal_restrictions": {
			      "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions",
			      "users_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions/users",
			      "teams_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions/teams",
			      "users": [
			        {
			          "login": "octocat",
			          "id": 1,
			          [...]
			        }
			      ],
			      "teams": [
			        {
			          "id": 1,
			          "node_id": "MDQ6VGVhbTE=",
			          [...]
			        }
			      ],
			      "apps": [
			        {</pre>
				`"required_pull_request_reviews" != "" && "required_approving_review_count" >= 1`	j	Eine Überprüfung ist möglich. Neben "require_code_owner_reviews" = true müssen auch "required_pull_request_reviews" definiert sein.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

23. Default Branch Should Restrict Who Can Dismiss Reviews	n/a	`GET /repos/{owner}/{repo}/branches/{branch}/protection`	<pre>{
			  "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection",
			  [...]
			  "required_pull_request_reviews": {
			    "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/required_pull_request_reviews",
			    "dismissal_restrictions": {
			      "url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions",
			      "users_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions/users",
			      "teams_url": "https://api.github.com/repos/octocat/Hello-World/branches/master/protection/dismissal_restrictions/teams",
			      "users": [
			        {
			          "login": "octocat",
			          "id": 1,
			          [...]
			        }
			      ],
			      "teams": [
			        {
			          "id": 1,
			          "node_id": "MDQ6VGVhbTE=",
			          [...]
			        }
			      ],
			      "apps": [
			        {</pre>
				`"dismissal_restrictions"."users" != "" || "dismissal_restrictions"."teams" != ""`	j	Eine Überprüfung ist möglich. Es müssen "dismissal_restrictions" auf Basis von Users und/oder Teams definiert sein.	https://docs.github.com/en/rest/branches/branch-protection?apiVersion=2022-11-28#get-branch-protection

24. Webhooks Should Be Configured To Use SSL	n/a	`GET /repos/{owner}/{repo}/hooks`	`[`
			`  {`
			`    "type": "Repository",`
			`    [...]`
			`    "config": {`
			`      "content_type": "json",`
			`      "insecure_ssl": "0",`
			`      "url": "https://example.com/webhook"`
			`    },`
			`    [...]`
			`  }`
			`]`
				`"insecure_ssl" == "0"`	j	Eine Überprüfung ist möglich.	https://docs.github.com/en/rest/repos/webhooks?apiVersion=2022-11-28#list-repository-webhooks